SOBRE LA ESTRUCTURA DE LOS CUERPOS FINITOS

NATALIA ISABEL PÉREZ NIÑO

UNIVERSIDAD INDUSTRIAL DE SANTANDER
FACULTAD DE CIENCIAS
ESCUELA DE MATEMÁTICAS
BUCARAMANGA
2023

SOBRE LA ESTRUCTURA DE LOS CUERPOS FINITOS

NATALIA ISABEL PÉREZ NIÑO

Trabajo de grado para optar al título de
Matemática

Director
Héctor Edonis Pinedo Tapia
Doctor en Matemáticas

UNIVERSIDAD INDUSTRIAL DE SANTANDER
FACULTAD DE CIENCIAS
ESCUELA DE MATEMÁTICAS
BUCARAMANGA
2023

DEDICATORIA

A mis padres y mis hermanas.

AGRADECIMIENTOS

En primer lugar quiero agradecer a mi familia por sus consejos y apoyo en estos años. Al profesor Héctor Pinedo, por su colaboración y orientación durante mi pregrado, especialmente en este trabajo de grado. Además, quiero agradecer a todos los profesores quienes hicieron parte de mi formación como matemática. Tambien quiero agradecer a mis amigos quienes durante estos cuatro años me acompañaron en mis estudios, especialmente a Juan quien es un apoyo incondicional.

CONTENIDO

LISTA DE FIGURAS

pág.

LISTA DE TABLAS

pág.

RESUMEN

TÍTULO: SOBRE LA ESTRUCTURA DE LOS CUERPOS FINITOS [*]

AUTOR: NATALIA ISABEL PÉREZ NIÑO [**]

PALABRAS CLAVE: CUERPOS FINITOS, POLINOMIOS IRREDUCIBLES, TRANSFORMACIONES LINEALES, ÁLGEBRAS DE GRUPO, TEORÍA DE CÓDIGOS.

DESCRIPCIÓN:

En las últimas décadas, la teoría de los cuerpos finitos ha sido de gran interés por sus aplicaciones a la teoría de códigos y criptografía. Los enteros módulo p, siendo p un primo, son los primeros ejemplos de cuerpos finitos que surgen cuya teoría fue en gran parte desarrollada en los siglos XVII y XVIII. En general, los cuerpos finitos poseen diversas propiedades algebraicas que los hace un objeto de estudio de gran importancia. Este trabajo consiste en un estudio teórico de las propiedades estructurales de los cuerpos finitos y su aplicación a la teoría de códigos.

En el primer capítulo, recordaremos algunos conceptos y resultados del álgebra abstracta que usaremos a lo largo del desarrollo del escrito. En el capítulo siguiente presentaremos algunas propiedades que caracterizan a los cuerpos finitos, entre ellas su cardinalidad, la estructura cíclica de su grupo multiplicativo y la relación entre sus subcuerpos. Estudiaremos el comportamiento de los polinomios irreducibles sobre dichos cuerpos y caracterizaremos las transformaciones lineales y bases de los cuerpos finitos vistos como un espacio vectorial sobre algún subcuerpo. Para finalizar, en el último capítulo explicaremos en detalle como construir códigos cíclicos minimales de longitud n sobre cuerpos finitos usando idempotentes en álgebras de grupo, tomando como referencia el trabajo de Raul Ferraz y César Polcino [1].

---

[*] Trabajo de grado

[**] Facultad de Ciencias. Escuela de Matemáticas. Director: Héctor Edonis Pinedo Tapia, Doctor en Matemáticas.

[1] Cesar FERRAZ Raul y POLCINO. “Idempotents in group algebras and minimal abelian codes”. En: *Finite Field and Their Applications* 13.2 (2007), págs. 382-393.

ABSTRACT

TITLE: ON STRUCTURE OF FINITE FIELDS [*]

AUTHOR: NATALIA ISABEL PÉREZ NIÑO [**]

KEYWORDS: FINITE FIELDS, IRREDUCIBLE POLYNOMIALS, LINEAR TRANSFORMATIONS, GROUP ALGEBRAS, CODING THEORY.

DESCRIPTION: In recent decades, the theory of finite fields has been of great interest because of their applications to coding theory and cryptography. The integers modulo p, being p a prime, are the first examples of finite fields that arise whose theory was largely developed in the seventeenth and eighteenth centuries. In general, finite fields have various algebraic properties that make them an object of study of great importance. This work consists of a theoretical study of the structural properties of finite fields and their application to coding theory.

In the first chapter, we will remember some concepts and results of the abstract algebra that we will use throughout the text. In the next chapter we will present some properties that characterize the finite fields, including their cardinality, the cyclical structure of its multiplicative group and the relationship between its subfields. We will study the behavior of irreducible polynomials on these fields and characterize the linear transformations and bases of the finite fields seen as a vector space on some subfield. Finally, in the last chapter we will explain in detail how to build minimal cyclical codes of length n on finite fields using idempotents in group algebras, taking as reference the work of Raul Ferraz and César Polcino [1].

---

[*] Bachelor Thesis

[**] Facultad de Ciencias. Escuela de Matemáticas. Director: Héctor Edonis Pinedo Tapia, Doctor en Matemáticas.

Introducción

Durante los siglos XVII y XVIII, Pierre de Fermat, Leonhard Euler, Joseph-Louis Lagrange y Adrien-Marie Legendre desarrollan gran parte de la teoría fundamental de los enteros módulo p, siendo p un número primo; uno de los cuerpos finitos más conocidos. No obstante, los primeros resultados en la teoría de cuerpos finitos se dan en 1830 donde el famoso matemático francés Évariste Galois trabajando en la congruencia de polinomios irreducibles de grado n módulo p, $f(x) \equiv 0 \ (\text{mód}\ p)$, piensa en las raíces de dicha congruencia de manera similar en la que se utilizaba el símbolo $i = \sqrt{-1}$ para realizar distintos cálculos. De esta forma, establece que si α es una raíz de esta congruencia entonces las expresiones $a_1\alpha + a_2\alpha^2 + \cdots + a_n\alpha^n$, con $a_1, \ldots, a_n \in \mathbb{Z}_p$, forman un cuerpo finito de p^n elementos; razón por la cual los cuerpos finitos son llamados también cuerpos de Galois. Finalmente, en 1893 Eliakim Moore demuestra que existe salvo isomorfismo un único cuerpo finito de p^n elementos, terminando así la caracterización de la cardinalidad de los cuerpos finitos.

En este trabajo de grado nos interesa estudiar propiedades estructurales de cuerpos finitos donde veremos como la teoría de grupos, extensiones de cuerpos, álgebra lineal e incluso un poco de la teoría clásica de números se reúnen para dar una descripción detallada de esta estructura algebraica. De igual forma, la teoría de los cuerpos finitos ha sido fundamental en diversas áreas como en la criptografía y la teoría códigos, razón por la cual nos interesa ver la aplicación de los cuerpos finitos en la construción de códigos cíclicos minimales.

1. Preliminares

En este capítulo revisaremos algunos conceptos y resultados sobre extensiones de cuerpos, teoría de grupos y teoría clásica de números que serán de gran utilidad en el estudio de la estructura de un cuerpo finito.

1.1. Extensiones de Cuerpos

Definición 1.1.1. Un **cuerpo** es un anillo conmutativo $\mathbb{F}$ con unidad en el que todo elemento no nulo es invertible.

Sea $x \in \mathbb{F}$ y n un entero positivo. Denotamos $x + x + \cdots + x$ (n sumandos) por $n \cdot x$.

Definición 1.1.2. Sea $\mathbb{F}$ un cuerpo. Definimos la **característica** de $\mathbb{F}$ como el menor entero positivo n tal que $n \cdot x = 0$ para todo $x \in \mathbb{F}$. Si no existe tal entero, decimos que la característica de $\mathbb{F}$ es cero.

Ejemplo 1.1.3. $\mathbb{Q}$ es un cuerpo infinito con característica cero y $\mathbb{Z}_p$ es un cuerpo finito con caracterísitica p, donde p es primo.

Proposición 1.1.4. *Sea $\mathbb{F}$ un cuerpo, entonces la característica de $\mathbb{F}$ es cero o un número primo. En particular la característica de un cuerpo finito es un número primo.*

Demostración. Sea $\mathbb{F}$ un cuerpo, si el orden aditivo de la unidad es infinito, claramente la característica de $\mathbb{F}$ es cero. Ahora bien, si el orden aditivo de la unidad es n, probaremos que la característica de $\mathbb{F}$ es n. Sea $x \in \mathbb{F}$, entonces:

$$\begin{aligned} n \cdot x &= \underbrace{x + x + \cdots + x}_{n \text{ sumandos}} \\ &= \underbrace{1x + 1x + \cdots + 1x}_{n \text{ sumandos}} \\ &= \underbrace{(1 + 1 + \cdots + 1)}_{n \text{ sumandos}} x \\ &= (n \cdot 1)x = 0 \end{aligned}$$

Como n es el menor entero positivo que cumple que $n \cdot 1 = 0$, concluimos que n es la característica de $\mathbb{F}$. Por último, veamos que n es primo. Sean s, t enteros positivos tales

que $1 \leq s, t \leq n$ y $n = st$, entonces:

$$0 = n \cdot 1 = (st) \cdot 1 = (s \cdot 1)(t \cdot 1),$$

lo que implica que $s \cdot 1 = 0$ o $t \cdot 1 = 0$ y como n es el menor entero positivo tal que $n \cdot 1 = 0$, tenemos que $s = n$ o $t = n$; luego n es primo. En particular, la característica de un cuerpo finito es un número primo, puesto que el orden aditivo de la unidad es finito. □

Proposición 1.1.5. *Sea $\mathbb{F}$ un cuerpo finito con característica p, entonces $\mathbb{F}$ contiene un subcuerpo isomorfo a $\mathbb{Z}_p$.*

Demostración. Consideremos la aplicación $\phi : \mathbb{Z}_p \to \mathbb{F}$ tal que $\phi(x) = x \cdot 1$, para todo $x \in \{0, \ldots, p-1\}$. Sean $\alpha, \beta \in \mathbb{Z}_p$, entonces existen $q_1, q_2, r_1, r_2 \in \mathbb{Z}^+$ tales que $\alpha + \beta = pq_1 + r_1$ y $\alpha\beta = pq_2 + r_2$ con $0 \leq r_1, r_2 \leq p-1$. Así;

$$\phi(\alpha + \beta) = \phi(r_1) = r_1 \cdot 1 = (pq_1) \cdot 1 + r_1 \cdot 1 = (pq_1 + r_1) \cdot 1 = (\alpha + \beta) \cdot 1 = (\alpha \cdot 1) + (\beta \cdot 1)$$

$$\phi(\alpha\beta) = \phi(r_2) = r_2 \cdot 1 = (pq_2) \cdot 1 + r_2 \cdot 1 = (pq_2 + r_2) \cdot 1 = (\alpha\beta) \cdot 1 = (\alpha \cdot 1)(\beta \cdot 1)$$

Luego, ϕ es un homomorfismo. Finalmente, note que $\mathrm{Ker}(\phi) = \{0\}$ ya que p es el menor entero positivo tal que $p \cdot 1 = 0$. Por tanto, $\phi(\mathbb{Z}_p)$ es un subcuerpo de $\mathbb{F}$ isomorfo a $\mathbb{Z}_p$. □

Definición 1.1.6. Sean $\mathbb{F}$ y $\mathbb{K}$ cuerpos.

I) Decimos que $\mathbb{F}$ es una extensión de $\mathbb{K}$ si $\mathbb{K} \subseteq \mathbb{F}$, que es denotado por $\mathbb{F}/\mathbb{K}$. Además, dada una extensión $\mathbb{F}/\mathbb{K}$, un cuerpo **intermedio** es un cuerpo $\mathbb{L}$ tal que $\mathbb{K} \subseteq \mathbb{L} \subseteq \mathbb{F}$.

II) Sea $\mathbb{F}/\mathbb{K}$ una extensión de cuerpos y sea $X \subseteq \mathbb{F}$, denotamos por

$$\mathbb{K}(X) = \bigcap \{\mathbb{L} \subseteq \mathbb{F} : \mathbb{L} \text{ es un cuerpo intermedio y } X \subseteq \mathbb{L}\}.$$

Así, $\mathbb{K}(X)$ es un cuerpo intermedio y es el menor cuerpo intermedio que contiene a $\mathbb{K}$ y a X. Si $X = \{a_1, a_2, \ldots, a_n\}$ escribimos $\mathbb{K}(a_1, a_2, \ldots, a_n)$ en vez de $\mathbb{K}(\{a_1, a_2, \ldots, a_n\})$. Decimos que $\mathbb{F}/\mathbb{K}$ es una extensión **simple** si existe $\alpha \in \mathbb{F}$ tal que $\mathbb{F} = \mathbb{K}(\alpha)$.

Ejemplo 1.1.7. $\mathbb{C}$ es una extensión simple de $\mathbb{R}$, dado que $\mathbb{C} = \mathbb{R}(i)$.

Definición 1.1.8. Sean $\mathbb{F}/\mathbb{K}$ una extensión de cuerpos y $\alpha \in \mathbb{F}$. Decimos que α es **algebraico** sobre $\mathbb{K}$ si existe $p(x) \in \mathbb{K}[x]$ no nulo tal que $p(\alpha) = 0$. En caso contrario, α es llamado **trascendente**. Si para todo $\alpha \in \mathbb{F}$, α es algebraico sobre $\mathbb{K}$ decimos que $\mathbb{F}/\mathbb{K}$ es una **extensión algebraica**.

Ejemplo 1.1.9. $\sqrt{2}+\sqrt{3}$ es algebraico sobre $\mathbb{Q}$ pues es raíz del polinomio $x^4-10x^2+1 \in \mathbb{Q}[x]$.

Ejemplo 1.1.10. e y π son transcendentes sobre $\mathbb{Q}$.

Teorema 1.1.11. *Sean $\mathbb{F}/\mathbb{K}$ una extensión de cuerpos y $\alpha \in \mathbb{F}$ algebraico sobre $\mathbb{K}$. Entonces existe un polinomio $p(x)$ irreducible sobre $\mathbb{K}$ tal que $p(\alpha)=0$. Este polinomio es único salvo por un factor constante y tiene grado mínimo en el ideal $I_\alpha = \{p(x) \in \mathbb{K}[x] : p(\alpha)=0\}$. Además, si $q(\alpha)=0$ para $q(x) \in \mathbb{K}[x]$, entonces $p(x) \mid q(x)$.*

Demostración. Sea ϕ_α el homomorfismo de evaluación de $\mathbb{K}[x]$ en $\mathbb{F}$ dado por $\phi_\alpha(p(x)) = p(\alpha)$, para todo $p(x) \in \mathbb{K}[x]$. El ideal I_α, quien es el kernel de este homomorfismo, es un ideal en $\mathbb{K}[x]$, que es un dominio de ideales principales y por tanto existe $p(x) \in I_\alpha$ tal que $I_\alpha = \langle p(x) \rangle$. De lo que inmediatamente se sigue que si $q(x)$ es otro polinomio para el cual α es raíz, entonces $p(x) \mid q(x)$. Como α es algebraico, el kernel es distinto del nulo y por tanto $p(x)$ es un polinomio no nulo de grado mínimo en I_α.

Ahora bien, si suponemos que existen polinomios $q, h \in \mathbb{K}[x]$ de menor grado que p tal que $p(x) = q(x)\,h(x)$, entonces como $p(\alpha)=0$ tenemos que $q(\alpha)=0$ o $h(\alpha)=0$, lo que contradice la propiedad minimal de $p(x)$. Luego, $p(x)$ es irreducible. Por último, para ver la unicidad de $p(x)$, supongamos que $q(x)$ es un polinomio irreducible en $\mathbb{K}[x]$ tal que $q(\alpha)=0$, entonces $q(x) = p(x)\,h(x)$ pero como $q(x)$ es irreducible y $p(x)$ no es una constante, concluimos que $h(x)$ es un polinomio constante. □

De esta forma, el único polinomio mónico irreducible sobre $\mathbb{K}$ para el cual α es raíz es llamado **polinomio minimal** de α sobre $\mathbb{K}$. Denotamos por $m_\alpha(x)$ a dicho polinomio y por ∂m_α a su grado.

Ejemplo 1.1.12. Sean p un primo y n un entero positivo. Entonces $f(x) = x^n - p \in \mathbb{Q}[x]$ es irreducible, $f\left(\sqrt[n]{p}\right)=0$ y f es mónico. Por lo tanto, $m_{\sqrt[n]{p}}(x) = x^n - p$ y $\partial m_{\sqrt[n]{p}} = n$.

Sea $\mathbb{F}/\mathbb{K}$ una extensión de cuerpos, entonces $\mathbb{F}$ es un $\mathbb{K}$-espacio vectorial donde la suma de vectores es la suma usual en $\mathbb{F}$ y la multiplicación por un escalar es la multiplicación usual en $\mathbb{F}$. Denotamos por $[\mathbb{F} : \mathbb{K}]$ a la dimensión de $\mathbb{F}$ como $\mathbb{K}$-espacio vectorial. Si esta es finita, decimos que $\mathbb{F}/\mathbb{K}$ es una **extensión finita**.

Teorema 1.1.13. *Toda extensión finita de cuerpos es algebraica.*

Demostración. Sean $\mathbb{F}/\mathbb{K}$ una extensión de cuerpos de grado n y $\alpha \in \mathbb{F}$. Entonces los vectores $1, \alpha, \alpha^2, \ldots, \alpha^n$ son linealmente dependientes y así, existen escalares $c_0, c_1, c_2, \ldots, c_n \in \mathbb{K}$ no todos nulos tales que $c_n\alpha^n + \cdots + c_2\alpha^2 + c_1\alpha + c_0 = 0$, luego α es raíz del polinomio no nulo $c_n x^n + \cdots + c_2 x^2 + c_1 x + c_0 \in \mathbb{K}[x]$. □

Teorema 1.1.14. *Sean $\mathbb{F}/\mathbb{K}$ una extensión de cuerpos y $\alpha \in \mathbb{F}$. Si α es algebraico sobre $\mathbb{K}$, entonces $\mathbb{K}(\alpha)/\mathbb{K}$ es una extensión finita. De hecho, $[\mathbb{K}(\alpha) : \mathbb{K}] = \partial m_\alpha$ y $\left\{1, \alpha, \ldots, \alpha^{\partial m_\alpha - 1}\right\}$ es base de $\mathbb{K}(\alpha)$ como $\mathbb{K}$-espacio vectorial.*

Demostración. Sea $\phi_\alpha(\mathbb{K}[x])$ la imagen de $\mathbb{K}[x]$ bajo el homomorfismo de evaluación mencionado en el Teorema 1.1.11. Es claro que $\phi_\alpha(\mathbb{K}[x]) \subseteq \mathbb{K}(\alpha)$. Por el primer teorema de isomorfismos para anillos tenemos que $\mathbb{K}[x]/\langle m_\alpha(x)\rangle \cong \phi_\alpha(\mathbb{K}[x])$ y como m_α es irreducible se sigue que $\mathbb{K}[x]/\langle m_\alpha(x)\rangle$ es cuerpo, lo que implica que $\phi_\alpha(\mathbb{K}[x])$ sea un subcuerpo de $\mathbb{K}(\alpha)$ que contiene tanto a $\mathbb{K}$ como a α y por lo tanto $\phi_\alpha(\mathbb{K}[x]) = \mathbb{K}(\alpha)$.

Sea $p(x) \in \mathbb{K}[x]$, entonces existen $q(x), r(x) \in \mathbb{K}[x]$ tales que $p(x) = m_\alpha(x)q(x) + r(x)$ con $r(x) = 0$ o $\partial r(x) < n$. Si $r(x) = 0$ claramente $p(\alpha)$ es combinación lineal de $\left\{1, \alpha, \ldots, \alpha^{\partial m_\alpha - 1}\right\}$. En el caso contrario, note que $p(\alpha) = r(\alpha)$ y escribiendo a $r(x) = a_n x^{n-1} + \cdots + a_2 x^2 + a_1 x + a_0$ tenemos que

$$p(\alpha) = r(\alpha) = a_{n-1}\alpha^{n-1} + \cdots + a_2\alpha^2 + a_1\alpha + a_0.$$

Luego, todo elemento de $\mathbb{K}(\alpha)$ es combinación lineal de $\left\{1, \alpha, \alpha^2, \ldots, \alpha^{\partial m_\alpha - 1}\right\}$. Por último, sean $c_0, c_1, c_2, \ldots, c_{n-1} \in \mathbb{K}$ tales que $c_{n-1}\alpha^{n-1} + \cdots + c_2\alpha^2 + c_1\alpha + c_0 = 0$. Llamemos $h(x) = c_{n-1}x^{n-1} + \cdots + c_2x^2 + c_1x + c_0$, si algún escalar es distinto de cero, entonces $h(x) \in \mathbb{K}[x]$ es un polinomio no nulo de grado menor que n para el cual α es raíz, lo que contradice la propiedad minimal de $m_\alpha(x)$. □

Ejemplo 1.1.15. Considere el polinomio irreducible $f(x) = x^5 - 2 \in \mathbb{Q}[x]$. Como $\sqrt[5]{2}$ es un cero de $f(x)$, por el teorema anterior tenemos que $\left\{1, \sqrt[5]{2}, \sqrt[5]{4}, \sqrt[5]{8}, \sqrt[5]{16}\right\}$ es una base de $\mathbb{Q}(\sqrt[5]{2})$ como $\mathbb{Q}$-espacio vectorial.

Teorema 1.1.16. *Si $\mathbb{F}/\mathbb{K}$ es una extensión de cuerpos finita y $\mathbb{L}/\mathbb{F}$ es una extensión de cuerpos finita, entonces $\mathbb{L}/\mathbb{K}$ es una extensión finita y se cumple que:*

$$[\mathbb{L} : \mathbb{K}] = [\mathbb{L} : \mathbb{F}]\,[\mathbb{F} : \mathbb{K}]$$

Demostración. Sean $\{\alpha_i\}_{i=1}^n$ una base para $\mathbb{F}/\mathbb{K}$ y $\{\beta_j\}_{j=1}^m$ una base para $\mathbb{L}/\mathbb{F}$. Veamos que los mn elementos de la forma $\alpha_i\beta_j$ son una base para $\mathbb{L}$ como $\mathbb{K}$-espacio vectorial. Sea $x \in \mathbb{L}$, entonces existen $b_1, \ldots, b_m \in \mathbb{F}$ tales que $x = \sum_{j=1}^m b_j\beta_j$ y para cada $j \in \{1, \ldots, m\}$ existen $a_{1j}, \ldots, a_{nj} \in \mathbb{K}$ tales que $b_j = \sum_{i=1}^n a_{ij}\alpha_i$ por lo que

$$x = \sum_{j=1}^{m} \left(\sum_{i=1}^{n} a_{ij}\alpha_i \right) \beta_j = \sum_{\substack{1\leq i\leq n \\ 1\leq j\leq m}} a_{ij}(\alpha_i\beta_j).$$

Luego, los elementos de la forma $\alpha_i\beta_j$ generan a $\mathbb{L}$ como un $\mathbb{K}$-espacio vectorial. Nos falta ver que son linealmente independientes. Sean $c_{ij} \in \mathbb{K}$ tales que:

$$\sum_{\substack{1\leq i\leq n \\ 1\leq j\leq m}} c_{ij}(\alpha_i\beta_j) = 0 \Rightarrow \sum_{j=1}^{m} \left(\sum_{i=1}^{n} c_{ij}\alpha_i \right) \beta_j = 0.$$

Como los elementos β_j son linealmente independiente entonces para todo $j \in \{1, \ldots, m\}$ tenemos que $\sum_{i=1}^n c_{ij}\alpha_i = 0$ y como los elementos α_i son tambien linealmente independientes tenemos que $c_{ij} = 0$. □

Corolario 1.1.17. *Sean $\mathbb{F}/\mathbb{K}$ una extensión finita y $\mathbb{L}$ un cuerpo intermedio, entonces las extensiones $\mathbb{F}/\mathbb{L}$ y $\mathbb{L}/\mathbb{K}$ son finitas y tanto $[\mathbb{F} : \mathbb{L}]$ como $[\mathbb{L} : \mathbb{K}]$ dividen a $[\mathbb{F} : \mathbb{K}]$.*

Demostración. Sea $\mathfrak{B}$ una base para $\mathbb{F}$ como $\mathbb{K}$-espacio vectorial. Note que $\mathfrak{B}$ es un conjunto generador de $\mathbb{F}$ como $\mathbb{L}$-espacio vectorial y por lo tanto existe un subconjunto de $\mathfrak{B}$ que sea base para $\mathbb{F}$ como $\mathbb{L}$-espacio vectorial; luego $\mathbb{F}/\mathbb{L}$ es una extensión finita. Por otro lado, note que $\mathbb{L}$ es un subespacio vectorial de $\mathbb{F}$ y por lo tanto la dimensión de $\mathbb{L}$ como $\mathbb{K}$-espacio vectorial es finita. Del teorema anterior se sigue que tanto $[\mathbb{F} : \mathbb{L}]$ como $[\mathbb{L} : \mathbb{K}]$ dividen a $[\mathbb{F} : \mathbb{K}]$. □

Ejemplo 1.1.18. Hallemos la dimensión de $\mathbb{Q}(\sqrt[3]{2}, \sqrt[4]{3})$ como $\mathbb{Q}$-espacio vectorial. Del Teorema 1.1.16 tenemos que

$$\left[\mathbb{Q}(\sqrt[3]{2}, \sqrt[4]{3}) : \mathbb{Q}\right] = \left[\mathbb{Q}(\sqrt[3]{2}, \sqrt[4]{3}) : \mathbb{Q}(\sqrt[3]{2})\right] \left[\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}\right]$$

$$\left[\mathbb{Q}(\sqrt[3]{2}, \sqrt[4]{3}) : \mathbb{Q}\right] = \left[\mathbb{Q}(\sqrt[3]{2}, \sqrt[4]{3}) : \mathbb{Q}(\sqrt[4]{3})\right] \left[\mathbb{Q}(\sqrt[4]{3}) : \mathbb{Q}\right]$$

Como $\sqrt[3]{2}$ y $\sqrt[4]{3}$ son raíces de $x^3 - 2$ y $x^4 - 3$ respectivamente y estos polinomios son irreducibles sobre $\mathbb{Q}$ tenemos por el Teorema 1.1.14 que $\left[\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}\right] = 3$ y $\left[\mathbb{Q}(\sqrt[4]{3}) : \mathbb{Q}\right] =$

4. Por lo tanto 3 y 4 dividen a $\left[\mathbb{Q}(\sqrt[3]{2},\sqrt[4]{3}):\mathbb{Q}\right]$ y así $\left[\mathbb{Q}(\sqrt[3]{2},\sqrt[4]{3}):\mathbb{Q}\right]\geq 12$.
Por otro lado, como $\sqrt[4]{3}$ es raíz del polinomio $x^4-3\in\mathbb{Q}(\sqrt[3]{2})[x]$, tenemos por el Teorema 1.1.11 que $\partial m_{\sqrt[4]{3}}$ sobre $\mathbb{Q}(\sqrt[3]{2})$ es a lo sumo 4. Así;

$$\left[\mathbb{Q}(\sqrt[3]{2},\sqrt[4]{3}):\mathbb{Q}(\sqrt[3]{2})\right]\left[\mathbb{Q}(\sqrt[3]{2}):\mathbb{Q}\right]=\left[\left(\mathbb{Q}(\sqrt[3]{2})\right)\left(\sqrt[4]{3}\right):\mathbb{Q}(\sqrt[3]{2})\right]\left[\mathbb{Q}(\sqrt[3]{2}):\mathbb{Q}\right]\leq 12$$

Luego, $\left[\mathbb{Q}(\sqrt[3]{2},\sqrt[4]{3}):\mathbb{Q}\right]=12$.

Corolario 1.1.19. *Sean $\mathbb{F}/\mathbb{K}$ una extensión de cuerpos y $\alpha\in\mathbb{F}$. Si α es algebraico sobre $\mathbb{K}$ y $\beta\in\mathbb{K}(\alpha)$, entonces ∂m_β divide a ∂m_α.*

Demostración. Por el Teorema 1.1.14 tenemos que $\mathbb{K}/\mathbb{K}(\alpha)$ es una extensión finita y por tanto β es algebraico sobre $\mathbb{K}$ donde $\partial m_\beta=[\mathbb{K}(\beta):\mathbb{K}]$. Como $\mathbb{K}\subseteq\mathbb{K}(\beta)\subseteq\mathbb{K}(\alpha)$, tenemos por el Teorema 1.1.16

$$[\mathbb{K}(\alpha):\mathbb{K}]=[\mathbb{K}(\alpha):\mathbb{K}(\beta)]\,[\mathbb{K}(\beta):\mathbb{K}]\,.$$

De lo que sigue que ∂m_β divide a ∂m_α. □

Definición 1.1.20. Sea $\mathbb{F}$ un cuerpo. Decimos que $\mathbb{F}$ es **algebraicamente cerrado**, si para todo $p(x)\in\mathbb{F}[x]$ no constante, existe $\alpha\in\mathbb{F}$ tal que $p(\alpha)=0$.

Ejemplo 1.1.21. $\mathbb{C}$ es algebraicamente cerrado.

Ejemplo 1.1.22. Ningún cuerpo finito es algebraicamente cerrado. En efecto, sea $\mathbb{F}=\{a_1,\ldots,a_n\}$ un cuerpo finito con n elementos, entonces $p(x)=(x-a_1)\cdots(x-a_n)+1$ no tiene raíces en $\mathbb{F}$.

Finalizamos esta sección con la siguiente definición.

Definición 1.1.23. Sea $\mathbb{F}$ un cuerpo. La **clausura algebraica** de $\mathbb{F}$ denotada por $\overline{\mathbb{F}}$ es una extensión $\mathbb{K}$ de $\mathbb{F}$ tal que:

i) $\mathbb{K}$ es algebraicamente cerrado.

ii) $\mathbb{K}$ es minimal respecto a i), es decir, si $\mathbb{L}$ es un cuerpo intermedio y es algebraicamente cerrado, entonces $\mathbb{L}=\mathbb{K}$.

Ejemplo 1.1.24. $\mathbb{C}=\overline{\mathbb{R}}$ puesto que $\mathbb{C}$ es algebraicamente cerrado y como $[\mathbb{C}:\mathbb{R}]=2$, no existen cuerpos intermedios.

Teorema 1.1.25. *Sean $\mathbb{F}$ un cuerpo y $\mathbb{K}$ una extensión de $\mathbb{F}$, entonces*

I) *$\mathbb{K}$ es la clausura algebraica de $\mathbb{F}$ si, y solo si, $\mathbb{K}$ es algebraicamente cerrado y una extensión algebraica de $\mathbb{F}$.*

II) *$\mathbb{F}$ tiene una clausura algebraica y es única salvo isomorfismo.*

Demostración. I) Ver [1], página 253.

II) Ver [2], página 290.

□

1.2. Teoría de Grupos

En esta sección recordaremos algunos conceptos y resultados conocidos de la teoría de grupos que utilizaremos en capítulos posteriores cuando estudiemos el grupo multiplicativo de un cuerpo finito.

Definición 1.2.1. Sean G un grupo y $a \in G$. Definimos el **orden** de a como el menor entero positivo n tal que $a^n = e$, donde e es el elemento identidad del grupo. Si tal entero no existe, decimos que a tiene orden infinito. El orden de a es denotado por $o(a)$.

Para cualquier elemento a de G, denotamos por $\langle a \rangle$ al conjunto $\{a^n \mid n \in \mathbb{Z}\}$. Decimos que un grupo G es **cíclico** si existe $a \in G$ tal que $G = \langle a \rangle$. Dicho elemento es llamado un **generador** de G.

Ejemplo 1.2.2. Sea n un entero positivo. Considere $U(n)$ el conjunto de todos los enteros positivos menores que n y primos relativos con n, entonces $U(n)$ es un grupo con la multiplicación módulo n. En particular, tenemos que $U(10)$ es un grupo cíclico generado por el número 3.

Teorema 1.2.3. *Sean G un grupo y $a \in G$. Si $o(a)$=n, entonces $\langle a \rangle = \{e, a, a^2, \ldots, a^{n-1}\}$ y $a^i = a^j$ si, y solo si, n divide $i - j$.*

---

[1] Karlheinz SPINDLER. *Abstract Algebra with Applications. Volume 2: Rings and Fiels*. Chapman, Hall/CRC Pure y Applied Mathematics, 1993.

[2] Jhon FRALEIGH. *A First Course in Abstract Algebra*. Addison-Wesley, 2003.

Demostración. Es claro que $\{e, a, a^2, \ldots, a^{n-1}\} \subseteq \langle a \rangle$. Ahora sea $a^k \in \langle a \rangle$, por el algoritmo de la división existen enteros q, r tales que $k = qn + r$ con $0 \leq r < n$, por lo que

$$a^k = a^{qn+r} = a^{qn}a^r = (a^n)^q a^r = a^r$$

y así $\langle a \rangle = \{e, a, a^2, \ldots, a^{n-1}\}$. Supongamos que $a^i = a^j$, entonces $a^{i-j} = e$. Por el algoritmo de la división, existen enteros q, r tales que $i - j = qn + r$ con $0 \leq r < n$ y así $e = a^{i-j} = a^r$. Como n es el menor entero positivo tal que $a^n = e$ tenemos que $r = 0$ lo que implica que n divide a $i - j$. Recíprocamente, si n divide a $i - j$ entonces existe un entero t tal que $i - j = nt$. Luego, $a^{i-j} = a^{nt} = (a^n)^t = e$ y por lo tanto $a^i = a^j$. □

Del teorema anterior, tenemos que $|\langle a \rangle| = o(a)$.

Corolario 1.2.4. *Sean G un grupo y $a \in G$. Si $o(a) = n$ y k es un entero positivo tal que $a^k = e$, entonces $n|k$.*

Demostración. Como $a^k = a^0 = e$ tenemos por el teorema anterior que n divide a k. □

Teorema 1.2.5. *Sean a un elemento de orden n en un grupo y k un entero positivo. Entonces:*

$$o(a^k) = \frac{n}{mcd(n, k)}$$

Demostración. Llamemos $d = mcd(n, k)$, entonces $k = dr$ con $r \in \mathbb{Z}$. Veamos que $\langle a^k \rangle = \langle a^d \rangle$. Como $a^k = (a^d)^r$ tenemos que $a^k \in \langle a^d \rangle$, lo que implica que $\langle a^k \rangle \subseteq \langle a^d \rangle$. Dado que d es el máximo común divisor entre n y k existen enteros s, t tal que $d = ns + kt$ por lo que $a^d = a^{ns+kt} = a^{ns}a^{kt} = a^{kt} = (a^k)^t$ y así $\langle a^d \rangle \subseteq \langle a^k \rangle$; luego $\langle a^k \rangle = \langle a^d \rangle$. Por lo anterior, basta probar que $o(a^d) = n/d$. Es claro que $(a^d)^{n/d} = e$. Si i es un entero positivo menor que n/d tal que $(a^d)^i = e$, entonces dado que $di < n$, la igualdad anterior contradice que n es el orden de a, por lo tanto $(a^d)^i \neq e$ que implica que $o(a^d) = n/d$. □

Es inmediato del teorema anterior que si $o(a) = n$, entonces a^k es generador de $\langle a \rangle$ si, y solo si, $mcd(n, k) = 1$.

Teorema 1.2.6. *(Teorema Fundamental de Grupos Cíclicos). Todo subgrupo de un grupo cíclico es cíclico. Además si $o(a) = n$, entonces la cardinalidad de cualquier subgrupo de $\langle a \rangle$ es divisor de n y para cada divisor positivo k de n, el subgrupo $\langle a^{n/k} \rangle$ es el único subgrupo de $\langle a \rangle$ con k elementos.*

Demostración. Sean $G = \langle a \rangle$ y H un subgrupo de G. Si $H = \{e\}$, es claro que H es cíclico. En caso contrario, considere d el menor entero positivo tal que $a^d \in H$. Afirmamos que $\langle a^d \rangle = H$. Es claro que $\langle a^d \rangle \subseteq H$. Ahora, sea $x \in H$, entonces existe $t \in \mathbb{Z}$ tal que $a^t = x$. Por el algoritmo de la división, existen $q, r \in \mathbb{Z}$ tales que $t = qd + r$ con $0 \leq r < d$. Como a^t y a^{qd} pertenencen a H tenemos que $a^r \in H$ y además, dado que d es el menor entero positivo tal que $a^d \in H$ tenemos que $r = 0$. Lo que muestra que $H \subseteq \langle a^d \rangle$.

Supongamos que $o(a) = n$ y sea $H = \langle a^s \rangle$, entonces por el teorema anterior tenemos que $o(a^s)|n$ y por lo tanto $|H||n$. Finalmente, sea k un divisor de n, entonces por el teorema anterior tenemos que $o(a^{n/k}) = \frac{n}{n/k} = k$ y así $\langle a^{n/k} \rangle$ es un subgrupo de $\langle a \rangle$ de k elementos. Además, si H es un subgrupo de $\langle a \rangle$ con k elementos, entonces como mostramos al principio de la prueba $H = \langle a^d \rangle$ y tomando $t = n$ vemos que $d|n$, luego $k = o(a^d) = \frac{n}{mcd(n,d)} = n/d$ que implica que $d = n/k$. □

Teorema 1.2.7. *(Teorema de Lagrange). Si G es un grupo finito y H es un subgrupo de G, entonces $|H|$ divide a $|G|$.*

Demostración. Ver [3], Capítulo 7. □

Si $a \in G$, entonces $\langle a \rangle$ es subgrupo de G y por consiguiente $o(a) = |\langle a \rangle|$ divide a $|G|$. De esta forma, si G tiene n elementos entonces $a^n = e$.

Finalizamos esta sección, mencionando dos teoremas importantes sobre la estructura de grupos abelianos finitos.

Teorema 1.2.8. *(Teorema de Cauchy para Grupos Abelianos) Sea G un grupo abeliano de n elementos y p un primo que divide a n. Entonces G tiene un elemento de orden p.*

Demostración. Ver [3], página 195. □

Teorema 1.2.9. *(Teorema Fundamental de Grupos Abelianos Finitos) Todo grupo abeliano finito es isomorfo a $\mathbb{Z}_{p_1^{n_1}} \times \mathbb{Z}_{p_2^{n_2}} \times \cdots \times \mathbb{Z}_{p_k^{n_k}}$ donde $p_1, \ldots, p_k$ son números primos, no necesariamente distintos y $n_1, \ldots, n_k \in \mathbb{N}$. Además, las potencias $p_1^{n_1}, \ldots, p_k^{n_k}$ son únicas salvo por el orden.*

Demostración. Ver [3], Capítulo 11. □

---

[3] Joseph GALLIAN. *Contemporary Abstract Algebra*. 8.ª ed. Brooks/Cole, Cengage Learning.

1.3. Teoría de Números

En esta sección mencionaremos algunas propiedades de dos funciones aritméticas muy importantes y recordaremos algunos resultados muy conocidos de los enteros módulo p, siendo p un primo.

Definición 1.3.1. Una función aritmética es una función f cuyo dominio es el conjunto de los enteros positivos y contradominio es el conjunto de los números complejos.

Para cada entero positivo n, definimos la función ϕ de Euler en n como el número de enteros positivos menores o iguales que n y primos relativos con n.

Ejemplo 1.3.2. Si p es un número primo, entonces todos los enteros positivos menores que p son primos relativos con p, por lo tanto $\phi(p) = p - 1$.

Presentamos algunas propiedades de la función ϕ de Euler.

Proposición 1.3.3. *Si p es un primo y k un entero positivo, entonces $\phi(p^k) = p^k - p^{k-1}$.*

Demostración. Los enteros positivos menores o iguales que p^k que no son primos relativos con p^k son $p, 2p, 3p, \ldots, p^{k-1}p$, por lo tanto $\phi(p^k) = p^k - p^{k-1}$. □

Proposición 1.3.4. *Si m y n son primos relativos, entonces $\phi(mn) = \phi(m)\phi(n)$.*

Demostración. Ver [4], página 79. □

Teorema 1.3.5. *Si $n = p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}$ es la descomposición canónica de un entero positivo n, entonces*

$$\phi(n) = \prod_{i=1}^{k} (p_i^{e_i} - p_i^{e_{i-1}}).$$

Demostración. Por las Proposiciones 1.3.3 y 1.3.4 tenemos que

$$\phi(n) = \phi(p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}) = \prod_{i=1}^{k} \phi(p_i^{e_i}) = \prod_{i=1}^{k} (p_i^{e_i} - p_i^{e_{i-1}}).$$

□

[4] GORDILLO Jorge y RUBIANO Gustavo JIMENEZ Luis. *Teoría de números [para principiantes]*. Facultad de Ciencias, Universidad Nacional de Colombia, Sede Bogotá, 2004.

Teorema 1.3.6. *Sea n un entero positivo, entonces $\sum_{d|n} \phi(d) = n$.*

Demostración. Es claro que la igualdad vale para $n = 1$. Veamos que la igualdad vale para el caso $n = p^k$. Como los divisores de p^k son $1, p, p^2, \ldots, p^k$ tenemos por la Proposición 1.3.3:

$$\sum_{d|p^k} \phi(d) = \phi(1)+\phi(p)+\phi(p^2)+\cdots+\phi(p^k) = 1+(p-1)+(p^2-p)+\cdots+(p^{k-1}-p^{k-2})+(p^k-p^{k-1}) = p^k.$$

En el caso general, si $n = p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}$ es la descomposición canónica de un entero positivo $n > 1$, entonces reemplazando cada $p_i^{e_i}$ por la ecuación anterior obtenemos que

$$n = \prod_{i=1}^{k} \left(1 + \phi(p_i) + \phi(p_i^2) + \cdots + \phi(p_i^{e_i})\right).$$

Realizando las distributivas de la productoria, vemos que todos los sumandos son de la forma:

$$\phi(p_1^{t_1})\phi(p_2^{t_2}) \cdots \phi(p_k^{t_k}) = \phi(p_1^{t_1} p_2^{t_2} \cdots p_k^{t_k}) \text{ con } 1 \leq t_i \leq e_i,$$

los cuales son todos los posibles divisores de n y por lo tanto $\sum_{d|n} \phi(d) = n$. □

Para cada entero positivo n, definimos la función de Möbius $\mu : \mathbb{Z}^+ \to \mathbb{Z}$ por:

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

Ejemplo 1.3.7. Si p es un primo, entonces $\mu(p) = -1$.

Note que $\mu(n) \neq 0$ si, y solo si, $n = 1$ o n es el producto de primos distintos.

Teorema 1.3.8. *Para todo entero positivo n, se tiene que*

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

Demostración. Si $n = 1$ es claro que $\sum_{d|1} \mu(d) = 1$. Sea $n > 1$ y $p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}$ su descomposición canónica. Los únicos términos de la sumatoria no nulos ocurrren cuando

$d = 1$ o cuando d es el producto de primos distintos. Luego,

$$\begin{aligned}\sum_{d|n} \mu(d) &= \mu(1) + \mu(p_1) + \mu(p_2) + \cdots + \mu(p_k) + \mu(p_1p_2) + \cdots + \mu(p_{k-1}p_k) + \cdots + \mu(p_1p_2 \ldots p_k) \\ &= 1 + \binom{k}{1}(-1) + \binom{k}{2}(-1)^2 + \cdots + \binom{k}{k}(-1)^k \\ &= (1-1)^k = 0.\end{aligned}$$

□

Teorema 1.3.9. *(Fórmula de Inversión de Möbius) Si f es un función aritmética y $F(n) = \sum_{d|n} f(d)$ para todo entero positivo n, entonces:*

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

Demostración. Como $F(n) = \sum_{d|n} f(d)$, tenemos que $F\left(\frac{n}{d}\right) = \sum_{b|\frac{n}{d}} f(b)$ y así

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

Si x es un término de $\sum_{d|n} \sum_{b|\frac{n}{d}} \mu(d)f(b)$, entonces $x = \mu(d)f(b)$ donde $d|n$ y $b|\frac{n}{d}$. Como $d|n$, $\frac{n}{d}|n$ y por tanto $b|n$. Asimismo como $b|\frac{n}{d}$ tenemos que $d|\frac{n}{b}$ y por consiguiente x es un término de $\sum_{b|n} \sum_{d|\frac{n}{b}} \mu(d)f(b)$. Análogamente se muestra que todo término de $\sum_{b|n} \sum_{d|\frac{n}{b}} \mu(d)f(b)$ es un término de $\sum_{d|n} \sum_{b|\frac{n}{d}} \mu(d)f(b)$. De este modo, tenemos:

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

Si $b \neq n$ por el teorema anterior tenemos que $\sum_{d|\frac{n}{b}} \mu(d) = 0$ y por tanto $f(n) = \sum_{d|n} \mu(d) F\left(\frac{n}{d}\right)$. □

Para finalizar esta sección recordaremos algunos resultados importantes en $\mathbb{Z}_p$, siendo p un primo. Más adelante generalizaremos estos resultados para cuerpos finitos.

Teorema 1.3.10. *Sea p un primo. Entonces:*

I) *(Pequeño Teorema de Fermat) $a^p \equiv a \,(\text{mód}\, p)$, para todo $a \in \mathbb{Z}$.*

II) *(Teorema de Wilson)* $(p-1)! \equiv -1$ (*mód* p).

III) *Si* p *es impar, entonces* $1 + 2 + \cdots + (p-1) \equiv 0$ (*mód* p).

Definición 1.3.11. Sea $\alpha \in \mathbb{Z}_p$, decimos que α es **residuo cuadrático** módulo p, si existe $\beta \in \mathbb{Z}_p$ tal que $\beta^2 \equiv \alpha$ (mód p).

Teorema 1.3.12. *(Criterio de Euler) Sean p un primo impar y* $\alpha \in \mathbb{Z}_p$ *con* $\alpha \neq 0$*, entonces* α *es residuo cuadrático módulo* p *si, y solo si,* $\alpha^{\frac{p-1}{2}} \equiv 1$ (*mód* p).

2. Sobre la estructura de los cuerpos finitos

En este capítulo mostraremos los aspectos más importantes de la estructura de los cuerpos finitos. Usaremos como referencia general los libros [5], [6] y [7] .Empezaremos caracterizando la cardinalidad de dichos cuerpos, estudiaremos la estructura cíclica de su grupo multiplicativo, propiedades de los polinomios irreducibles y mencionaremos otras características básicas que serán de gran utilidad en la aplicación que veremos en el Capítulo 4. Además, finalizaremos este capítulo estudiando las extensiones de cuerpos finitos como espacios vectoriales.

2.1. Caracterización de un cuerpo finito

A continuación mostramos que la cardinalidad de un cuerpo finito es la potencia de un número primo.

Teorema 2.1.1. *Sea $\mathbb{F}/\mathbb{K}$ una extensión finita de grado n. Entonces:*

I) *Si $\mathbb{K}$ tiene q elementos, entonces $\mathbb{F}$ tiene q^n elementos.*

II) *Si $\mathbb{F}$ es un cuerpo finito de característica p, entonces existe algún entero positivo m tal que $\mathbb{F}$ tiene p^m elementos.*

Demostración. Probaremos cada una de las afirmaciones.

I) Sea $\{\alpha_1, \alpha_2, \ldots, \alpha_n\}$ una base para $\mathbb{F}$ como $\mathbb{K}$-espacio vectorial. Consideremos la función $\phi : \mathbb{K}^n \to \mathbb{F}$ dada por $\phi(a_1, a_2, \ldots, a_n) = a_1\alpha_1 + a_2\alpha_2 + \cdots + a_n\alpha_n$. Teniendo en cuenta que cada elemento de $\mathbb{F}$ se puede escribir de manera única como combinación lineal de $\alpha_1, \alpha_2, \ldots, \alpha_n$ tenemos que ϕ es una función biyectiva y por lo tanto $q^n = |\mathbb{K}|^n = |\mathbb{F}|$.

---

[5] Harald LIDL Rudolf y NIEDERREITER. *Introduction to finite fields and their applications*. New York Cambridge University Press, 2002.

[6] Dieter HACHENBERGER Dirk y JUNGNICKEL. *Topics in Galois Fields*. Algoritms y Computation in Mathematics, Springer, 2020.

[7] James BELK. *Classification of Finite Fields*. URL: `https://e.math.cornell.edu/people/belk`.

II) Como $\mathbb{F}$ es un cuerpo finito con caracterísitica p, existe un subcuerpo $\mathbb{L}$ de $\mathbb{F}$ isomorfo a $\mathbb{Z}_p$ y por tanto $\mathbb{F}/\mathbb{L}$ es una extensión finita. Sea m el grado de la extensión $\mathbb{F}/\mathbb{L}$, se sigue del ítem anterior que $\mathbb{F}$ tiene p^m elementos.

Presentamos otra demostración de esta afirmación usando el Teorema de Cauchy para Grupos Abelianos. Si $\mathbb{F}$ es un cuerpo finito con característica p, entonces el orden aditivo de la unidad es p y por tanto el de cualquier elemento no nulo de $\mathbb{F}$. Afirmamos que $\mathbb{F}$ tiene p^m elementos para algún $m \in \mathbb{Z}^+$. Supongamos por absurdo que existe un primo $q \neq p$ tal que q divide al orden del cuerpo. Por el Teorema de Cauchy para Grupos Abelianos existiría un elemento en $\mathbb{F}$ cuyo orden aditivo es q, que claramente es una contradicción.

□

Ahora demostraremos la existencia de un cuerpo finito de p^n elementos para todo p primo y $n \in \mathbb{Z}^+$. Usaremos un par de lemas.

Lema 2.1.2. *Si $\mathbb{F}$ es un cuerpo con característica p, entonces $x^{p^n} - x$ tiene p^n raíces distintas en su clausura algebraica $\overline{\mathbb{F}}$.*

Demostración. Como $\overline{\mathbb{F}}$ es algebraicamente cerrado, $\overline{\mathbb{F}}$ contiene todas las raíces del polinomio $f(x) = x^{p^n} - x$, por lo que debemos mostrar que cada raíz de $f(x)$ en $\overline{\mathbb{F}}$ es simple. Es claro que 0 es una raíz simple de $f(x)$. Supongamos que $\alpha \neq 0$ es una raíz de $f(x)$. Entonces α es un cero de $x^{p^n-1} - 1$ y así, $x - \alpha$ es un factor de $x^{p^n-1} - 1$ en $\overline{\mathbb{F}}[x]$. Si realizamos la división entre polinomios $q(x) = \dfrac{x^{p^n-1} - 1}{x - \alpha}$, obtenemos que $q(x) = x^{p^n-2} + \alpha x^{p^n-3} + \alpha^2 x^{p^n-4} + \cdots + \alpha^{p^n-3} x + \alpha^{p^n-2}$. Evaluando α en $q(x)$ vemos que cada sumando de $q(\alpha)$ es $\alpha^{p^n-2} = \alpha^{p^n-1}\alpha^{-1}$ y como α es raíz del polinomio $x^{p^n-1} - 1$, tenemos que $\alpha^{p^n-2} = \alpha^{-1}$. Puesto que $q(x)$ tiene $p^n - 1$ sumandos, $q(\alpha) = (p^n - 1)\alpha^{-1} = p^n\alpha^{-1} - \alpha^{-1}$ y como la característica de $\mathbb{F}$ es p, se tiene que $p^n\alpha^{-1} = 0$. De lo que se sigue que $q(\alpha) = -\alpha^{-1} \neq 0$ y por tanto α es un cero de simple de $p(x)$. □

Lema 2.1.3. *Si $\mathbb{F}$ es un cuerpo con característica p, entonces $(\alpha + \beta)^{p^n} = \alpha^{p^n} + \beta^{p^n}$ para todo $\alpha, \beta \in \mathbb{F}$ y todo entero positivo n.*

Demostración. Sean $\alpha, \beta \in \mathbb{F}$. Haremos esta prueba por inducción en n. Si $n = 1$, por el teorema del binomio tenemos:

$$(\alpha + \beta)^p = \sum_{k=0}^{p} \binom{p}{k} \alpha^{p-k}\beta^k$$

Como p es primo, tenemos que p divide a $\begin{pmatrix} p \\ k \end{pmatrix}$ con $1 \leq k \leq p-1$ y así, $(\alpha+\beta)^p = \alpha^p+\beta^p$. Ahora, sea k un entero positivo y supongamos que el resultado es verdadero para k, es decir, $(\alpha+\beta)^{p^k} = \alpha^{p^k}+\beta^{p^k}$. Entonces, $(\alpha+\beta)^{p^{k+1}} = \left[(\alpha+\beta)^{p^k}\right]^p = \left[\alpha^{p^k}+\beta^{p^k}\right]^p = \alpha^{p^{k+1}}+\beta^{p^{k+1}}$. Por el principio de inducción matemática, tenemos que $(\alpha+\beta)^{p^n} = \alpha^{p^n}+\beta^{p^n}$ para todo entero positivo n. □

Teorema 2.1.4. *Sean p un primo y n un entero positivo, entonces existe un cuerpo finito con p^n elementos.*

Demostración. Sean $\overline{\mathbb{Z}_p}$ la clausura algebraica de $\mathbb{Z}_p$ y $\mathbb{K} = \left\{\alpha \in \overline{\mathbb{Z}_p} \mid \alpha \text{ es raíz de } x^{p^n}-x\right\}$. Veamos que $\mathbb{K}$ es un subcuerpo de $\overline{\mathbb{Z}_p}$. Claramente tanto 0 como 1 pertenecen a $\mathbb{K}$. Sean $\alpha, \beta \in \mathbb{K}$, entonces $\alpha^{p^n} = \alpha$ y $\beta^{p^n} = \beta$. Note que si p es un primo distinto de 2, $(-1)^{p^n} = -1$ y si $p = 2$, $(-1)^{p^n} = 1 = -1$. Usando el Lema 2.1.3 obtenemos:

$$(\alpha-\beta)^{p^n} = (\alpha+(-\beta))^{p^n} = \alpha^{p^n}+(-\beta)^{p^n} = \alpha^{p^n}+(-1)^{p^n}\beta^{p^n} = \alpha^{p^n}-\beta^{p^n} = \alpha-\beta$$

Supongamos que $\beta \neq 0$, entonces $(\alpha\beta^{-1})^{p^n} = \alpha^{p^n}(\beta^{-1})^{p^n} = \alpha^{p^n}\left(\beta^{p^n}\right)^{-1} = \alpha\beta^{-1}$. De esta forma hemos mostrado que $\alpha-\beta \in \mathbb{K}$ y $\alpha\beta^{-1} \in \mathbb{K}$ por lo que concluimos que $\mathbb{K}$ es un subcuerpo de $\overline{\mathbb{Z}_p}$ y por el Lema 2.1.2 tenemos que $\mathbb{K}$ es un cuerpo de p^n elementos. □

El teorema anterior nos garantiza la existencia de un cuerpo finito de p^n elementos, sin embargo no nos proporciona un método sencillo para construir dichos cuerpos. A continuación mostraremos una forma de construir un cuerpo finito de 4 elementos usando anillos cocientes.

Ejemplo 2.1.5. Para construir un cuerpo finito de 4 elementos, consideremos:

$$\mathbb{F} = \mathbb{Z}_2[x] / \left\langle x^2+x+1\right\rangle = \left\{p(x)+\left\langle x^2+x+1\right\rangle \mid p(x) \in \mathbb{Z}_2[x]\right\}$$

Dado que x^2+x+1 es irreducible sobre $\mathbb{Z}_2$, tenemos que $\mathbb{F}$ es un cuerpo. Para ver que es un cuerpo de 4 elementos, note que si $p(x) \in \mathbb{Z}_2[x]$ entonces por el algoritmo de la división $p(x) = q(x)(x^2+x+1)+r(x)$ donde $r(x) = 0$ o el grado de $r(x)$ es menor que 2. De esta forma, $p(x)+\langle x^2+x+1\rangle = q(x)(x^2+x+1)+r(x)+\langle x^2+x+1\rangle = r(x)+\langle x^2+x+1\rangle$.

Por lo que podemos ver $\mathbb{F} = \{ax+b \mid a, b \in \mathbb{Z}_2\}$, que efectivamente tiene 4 elementos,

donde la suma y multiplicación se realiza en módulo $x^2 + x + 1$. Por ejemplo, $x(x+1) = x^2 + x = 1$ puesto que el residuo que deja $x^2 + x$ al dividirse por $x^2 + x + 1$ es 1. En las Tablas 2.1 y 2.2 se encuentran la suma y la multiplicación entre los elementos de $\mathbb{F}$.

$+$	0	1	x	$x+1$
0	0	1	x	$x+1$
1	1	0	$x+1$	x
x	x	$x+1$	0	1
$x+1$	$x+1$	x	1	0

Tabla 2.1: Suma en $\mathbb{F}$.

$\cdot$	0	1	x	$x+1$
0	0	0	0	0
1	0	1	x	$x+1$
x	0	x	$x+1$	1
$x+1$	0	$x+1$	1	x

Tabla 2.2: Multiplicación en $\mathbb{F}$.

En general, si $f(x)$ es un polinomio irreducible de grado n sobre $\mathbb{Z}_p$, entonces $\mathbb{Z}_p / \langle f(x) \rangle$ es un cuerpo finito con p^n elementos.

Finalizamos la caracterización sobre la cardinalidad de los cuerpos finitos, demostrando la unicidad de dichos cuerpos. Empezaremos mostrando que el grupo multiplicativo de un cuerpo finito es cíclico y posteriormente mencionaremos algunas proposiciones que usaremos en la prueba.

Lema 2.1.6. *Sea G un grupo finito con n elementos. Si para todo $d \mid n$ se tiene que la cardinalidad de $\{x \in G \mid x^d = 1\}$ es menor o igual que d, entonces G es cíclico.*

Demostración. Sean $d \mid n$ y G_d el conjunto de todos los elementos de G cuyo orden es d. Supongamos que G_d es distinto de vacío y fijemos $y \in G_d$. Entonces, $\langle y \rangle \subseteq \{x \in G \mid x^d = 1\}$ pero el subgrupo $\langle y \rangle$ tiene d elementos, así que por hipotesis $\langle y \rangle = \{x \in G \mid x^d = 1\}$. De lo anterior, es claro que G_d es el conjunto de los generadores del grupo ciclíco $\langle y \rangle$ y como la cantidad de generadores del grupo cíclico $\langle y \rangle$ es $\phi(d)$, hemos probado que G_d es vacío o tiene $\phi(d)$ elementos, para todo $d \mid n$. Ahora bien, puesto que

los G_d forman una partición de G, tenemos que:

$$n = |G| = \sum_{d|n} |G_d| \leq \sum_{d|n} \phi(d) = n,$$

donde la última igualdad se sigue del Teorema 1.3.6 y por lo tanto, $|G_d| = \phi(d)$ para todo $d|n$. En particular G_n es no vacío; luego G es cíclico. □

Si G es un subgrupo finito del grupo multiplicativo de un cuerpo $\mathbb{F}$, sabemos que el polinomio $x^d - 1$ tiene a lo sumo d raíces en $\mathbb{F}$ y por tanto en G. Así que siguiente teorema es una consecuencia inmediata del Lema 2.1.6.

Teorema 2.1.7. *Sea $\mathbb{F}$ un cuerpo. Si G es un subgrupo finito del grupo multiplicativo $\mathbb{F}^*$, entonces G es cíclico. En particular, el grupo multiplicativo de todos los elementos no nulos de un cuerpo finito es cíclico.*

La siguiente proposición es un resultado clásico de la teoría de grupos.

Proposición 2.1.8. *Sean $n_1, n_2, \ldots, n_r \in \mathbb{Z}^+$. Si n_i y n_j son primos relativos cuando $i \neq j$, entonces $\mathbb{Z}_{n_1} \times \mathbb{Z}_{n_2} \times \cdots \times \mathbb{Z}_{n_r}$ es cíclico.*

Demostración. Afirmamos que $o(1, 1, \ldots, 1) = n_1 n_2 \cdots n_r$. En efecto, tenemos que:

$$n_1 n_2 \cdots n_r (1, 1, \ldots, 1) = (n_1 n_2 \cdots n_r, n_1 n_2 \cdots n_r, \ldots, n_1 n_2 \cdots n_r) = (0, 0, \ldots, 0).$$

Sea x un entero positivo tal que $x(1, 1, \ldots, 1) = (0, 0, \ldots, 0)$ entonces $x \equiv 0 \pmod{n_i}$ para todo $i \in \{1, \ldots, r\}$ lo que implica que n_i divide a x y por lo tanto $mcm(n_1, n_2, \ldots, n_r)|x$. Como los n_i son primos relativos dos a dos tenemos que $mcm(n_1, n_2, \ldots, n_r) = n_1 n_2 \cdots n_r$ y así $n_1 n_2 \cdots n_r \leq x$. Luego, $\mathbb{Z}_{n_1} \times \mathbb{Z}_{n_2} \times \cdots \times \mathbb{Z}_{n_r}$ es generado por $(1, 1, \ldots, 1)$. □

Con ayuda de la proposición anterior, damos otra demostración del Teorema 2.1.7 usando el Teorema Fundamental de Grupos Abelianos Finitos, sin recurrir a la función aritmética ϕ.

Demostración. Por el Teorema Fundamental de Grupos Abelianos Finitos, tenemos que G es isomorfo a $\mathbb{Z}_{n_1} \times \mathbb{Z}_{n_2} \times \cdots \times \mathbb{Z}_{n_r}$ donde cada n_i es la potencia de un primo. Sea m el mínimo común multiplo de $n_1, n_2, \ldots, n_r$. Entonces $m \leq n_1 n_2 \cdots n_r$. Veamos que todo elemento de G es raíz del polinomio $x^m - 1$. Fijemos $f : G \to \mathbb{Z}_{n_1} \times \mathbb{Z}_{n_2} \times \cdots \times \mathbb{Z}_{n_r}$ un isomorfismo y sea $\alpha \in G$. Note que si $a_i \in \mathbb{Z}_{n_i}$, entonces $n_i \cdot a_i = 0$ lo que implica

que $m \cdot a_i = 0$ puesto que $n_i \mid m$. De esta forma, si $f(\alpha) = (a_1, a_2, \ldots, a_r)$ entonces $f(\alpha^m) = (m \cdot a_1, m \cdot a_2, \ldots, m \cdot a_r) = (0, 0, \ldots, 0)$. Como f es un homomorfismo sabemos que $f(1) = (0, 0, \ldots, 0)$ y por la inyectividad de f concluimos que $\alpha^m = 1$. Ahora bien, dado que $x^m - 1$ puede tener a lo sumo m raíces en $\mathbb{F}$ tenemos que $m \geq n_1 n_2 \cdots n_r$ y por tanto $m = n_1 n_2 \cdots n_r$. Así, n_i y n_j son primos relativos cuando $i \neq j$ y podemos concluir a partir de la Proposición 2.1.8 que G es isomorfo al grupo cíclico $\mathbb{Z}_{n_1} \times \mathbb{Z}_{n_2} \times \cdots \times \mathbb{Z}_{n_r}$. □

Definición 2.1.9. Sea $\mathbb{F}$ un cuerpo. Un generador del grupo cíclico $\mathbb{F}^*$ es llamado un **elemento primitivo** de $\mathbb{F}$.

Ejemplo 2.1.10. Consideremos $\mathbb{F}$ como en el Ejemplo 2.1.5, como $\mathbb{F}^*$ tiene 3 elementos, sabemos que cualquier elemento no nulo tiene orden 1 o 3 en el grupo multiplicativo $\mathbb{F}^*$. Por lo que concluimos que x y $x + 1$ son elementos primitivos de $\mathbb{F}$.

Corolario 2.1.11. *Si $\mathbb{F}$ una extensión finita de un cuerpo finito $\mathbb{K}$, entonces $\mathbb{F}$ es una extensión simple de $\mathbb{K}$.*

Demostración. Sea α un elemento primitivo de $\mathbb{F}$. Afirmamos que $\mathbb{F} = \mathbb{K}(\alpha)$. De la definición de $\mathbb{K}(\alpha)$ es inmediato que $\mathbb{K}(\alpha) \subseteq \mathbb{F}$. Por otro lado, como $\mathbb{K}(\alpha)$ es un cuerpo que contiene a $\mathbb{K}$ y α, debe contener al 0 y a todas las potencias de α. Lo que implica que $\mathbb{F} \subseteq \mathbb{K}(\alpha)$. □

En la demostración anterior vimos que si $\mathbb{K}$ es un cuerpo finito y $\mathbb{F}$ es una extensión finita de $\mathbb{K}$ cuyo elemento primitivo es α, entonces $\mathbb{F} = \mathbb{K}(\alpha)$. Sin embargo, la recíproca de esta implicación no es cierta. Consideremos $\mathbb{F} = \mathbb{Z}_3[x]/\langle x^3 + 2x + 2\rangle$. Por el Teorema de Kronecker sabemos que $\alpha = \overline{x}$ es raíz de $x^3 + 2x + 2$ en $\mathbb{F}[x]$. Por lo tanto $\alpha^3 = \alpha + 1$, lo que implica que $\alpha^4 = \alpha^2 + \alpha$ y $\alpha^9 = \alpha^3 + 1$. De este modo, $\alpha^{13} = (\alpha^2 + \alpha)(\alpha^3 + 1) = \alpha^5 + \alpha^2 + \alpha^4 + \alpha = \alpha^2 + \alpha + 1 + \alpha^2 + \alpha^2 + \alpha + \alpha = 3\alpha^2 + 3\alpha + 1 = 1$. Lo que muestra que $\mathbb{F} = \mathbb{Z}_3(\alpha)$ pero α no es generador de $\mathbb{F}^*$.

Hasta este momento hemos visto que el grupo multiplicativo de un cuerpo finito es cíclico. Es natural preguntarse si existe algún cuerpo infinito cuyo grupo multiplicativo sea cíclico, la respuesta es no.

Teorema 2.1.12. *Sea $\mathbb{F}$ un cuerpo. Si $\mathbb{F}^*$ es cíclico, entonces $\mathbb{F}$ es finito.*

Demostración. Como $\mathbb{F}$ es cuerpo, la característica de $\mathbb{F}$ es cero o un número primo. Si $\mathbb{F}$ tiene característica cero, entonces $\mathbb{F}$ contiene un subanillo isomorfo a $\mathbb{Z}$ y por tanto un

subcuerpo isomorfo a $\mathbb{Q}$. Luego, $\mathbb{Q}^*$ es isomorfo a un grupo multiplicativo cíclico, lo que es un absurdo. Esto implica que la característica de $\mathbb{F}$ es un número primo y por tanto podemos ver a $\mathbb{Z}_p$ como un subcuerpo de $\mathbb{F}$. Sea α un generador del grupo cíclico $\mathbb{F}^*$ y supongamos que p es un primo impar, entonces existe $n \in \mathbb{Z}$ no nulo tal que $\alpha^n = -1$. Si n es un entero positivo, α es raíz del polinomio $x^n + 1 \in \mathbb{Z}_p[x]$, caso contrario, α^{-1} es raíz del polinomio $x^{-n} + 1 \in \mathbb{Z}_p[x]$.

Para el caso donde $p = 2$, note que si $\alpha = 1$, entonces $\mathbb{F} = \mathbb{Z}_2$. Ahora si $\alpha \neq 1$ tenemos que $1 + \alpha \neq 0$ y por lo tanto existe entonces existe $n \in \mathbb{Z}$ no nulo tal que $\alpha^n = 1 + \alpha$. Si n es un entero positivo, α es raíz del polinomio $x^n + x + 1 \in \mathbb{Z}_p[x]$, caso contrario, α^{-1} es raíz de $x^{-n+1} + x + 1 \in \mathbb{Z}_p[x]$. Por lo que hemos mostrado que α o α^{-1} es algebraico sobre $\mathbb{Z}_p$ y teniendo en cuenta que $\mathbb{F} = \mathbb{Z}_p(\alpha) = \mathbb{Z}_p(\alpha^{-1})$, concluimos que $\mathbb{Z}_p(\alpha)$ es una extensión finita de $\mathbb{Z}_p$ y por el Teorema 2.1.1, $\mathbb{F}$ es finito.

□

Proposición 2.1.13. *Sea $\mathbb{F}$ un cuerpo de p^n elementos. Entonces existe un polinomio irreducible $f(x) \in \mathbb{Z}_p[x]$ tal que $\mathbb{F} \cong \mathbb{Z}_p[x]/\langle f(x)\rangle$. Cada polinomio $f(x)$ irreducible con esta propiedad tiene grado n.*

Demostración. Como $\mathbb{F}$ es un cuerpo de p^n elementos, podemos ver a $\mathbb{Z}_p$ como un subcuerpo de $\mathbb{F}$ y así $\mathbb{F}/\mathbb{Z}_p$ es una extensión finita. Por el Corolario 2.1.11 tenemos que existe $\alpha \in \mathbb{F}$ tal que $\mathbb{F} = \mathbb{Z}_p(\alpha)$. Debido a que toda extensión finita es algebraica, concluimos que $\mathbb{F} = \mathbb{Z}_p(\alpha) \cong \mathbb{Z}_p[x]/\langle f(x)\rangle$ donde $f(x)$ es el polinomio minimal de α sobre $\mathbb{Z}_p$.

Adicionalmente, si $f(x)$ es un polinomio irreducible sobre $\mathbb{Z}_p$ tal que $\mathbb{F} \cong \mathbb{Z}_p[x]/\langle f(x)\rangle$, entonces $\mathbb{F} \cong \mathbb{Z}_p[x]/\langle f(x)\rangle \cong \mathbb{Z}_p(\beta)$ donde $\beta \in \overline{\mathbb{Z}_p}$ y $f(\beta) = 0$. Sea m el grado de $f(x)$, sabemos que $\mathbb{Z}_p(\beta)$ tiene p^m elementos y como es isomorfo a $\mathbb{F}$, un cuerpo de p^n elementos, concluimos que m el grado del polinomio $f(x)$ es igual a n. □

Proposición 2.1.14. *Sea $\mathbb{F}$ un cuerpo finito con p^n elementos. Entonces todo elemento de $\mathbb{F}$ es una raíz de $x^{p^n} - x$ y por lo tanto:*

$$x^{p^n} - x = \prod_{\alpha \in \mathbb{F}} (x - \alpha).$$

Demostración. Sea $\alpha \in \mathbb{F}^*$, el grupo multiplicativo de $\mathbb{F}$ cuya cardinalidad es $p^n - 1$. Por el Teorema de Lagrange tenemos que $\alpha^{p^n-1} = 1$ y por consiguiente $\alpha^{p^n} = \alpha$. Asimismo, 0 es claramente raíz de $x^{p^n} - x$ y por tanto todo elemento de $\mathbb{F}$ es raíz de $x^{p^n} - x$. Teniendo en cuenta que $x^{p^n} - x$ tiene a lo sumo p^n raíces en $\mathbb{F}$, vemos que $x^{p^n} - x$ contiene todas sus raíces en $\mathbb{F}$ y la factorización dada se sigue. □

Proposición 2.1.15. *Sea $\mathbb{F}$ un cuerpo finito con p^n elementos, y sea*

$$x^{p^n} - x = m_1(x)m_2(x)\dots m_r(x)$$

la factorización de $x^{p^n} - x$ en polinomios mónicos irreducibles de $\mathbb{Z}_p[x]$. Entonces:

I) *El polinomio minimal para cada $\alpha \in \mathbb{F}$ es uno de los polinomios $m_1(x), m_2(x), \dots, m_r(x)$.*

II) *Para cada i, el número de elementos de $\mathbb{F}$ con polinomio minimal $m_i(x)$ es igual al grado de $m_i(x)$.*

Demostración. Sea $\alpha \in \mathbb{F}$. Por la proposición anterior, tenemos que α es raíz de $x^{p^n} - x$ que implica que α sea raíz de $m_i(x)$ para algún $i \in \{1, \dots, r\}$ y como $m_i(x)$ es irreducible y mónico, debe ser el polinomio minimal de α. Por último, sea $i \in \{1, \dots, r\}$. Como $x^{p^n} - x$ tiene todas sus raíces en $\mathbb{F}$, $m_i(x)$ también las tiene en $\mathbb{F}$, por lo que el número de raíces de este polinomio en $\mathbb{F}$ es igual a su grado y debido a que es irreducible y mónico tenemos que $m_i(x)$ es el polinomio minimal para cada una de estas raíces. □

Ejemplo 2.1.16. De la Proposición 2.1.14 tenemos que tanto x como $x - 1$ son factores irreducibles del polinomio $x^4 - x$ sobre $\mathbb{Z}_2$. Si dividimos $x^4 - x$ entre $x^2 - x$, tenemos que $x^2 + x + 1$ es un factor irreducible de dicho polinomio puesto que es un polinomio de grado 2 que no tiene raíces en $\mathbb{Z}_2$. Así, la factorización del polinomio $x^4 - x$ en polinomios irreducibles sobre $\mathbb{Z}_2$ es:

$$x^4 - x = x(x - 1)(x^2 + x + 1).$$

Por lo que cualquier cuerpo finito con 4 elementos debe contener al 0, 1 y dos raíces del polinomio $x^2 + x + 1$.

Teorema 2.1.17. *(Unicidad de los cuerpos finitos). Si $\mathbb{F}$ y $\mathbb{K}$ son cuerpos finitos con p^n elementos entonces $\mathbb{F} \cong \mathbb{K}$.*

Demostración. De la Proposición 2.1.13 tenemos que existen $\alpha \in \mathbb{F}$ y un polinomio irreducible $f \in \mathbb{Z}_p[x]$ de grado n tal que $\mathbb{F} = \mathbb{Z}_p(\alpha) \cong \mathbb{Z}_p[x]/\langle f(x)\rangle$. Como $f(x)$ es el polinomio minimal de α se concluye por la Proposición 2.1.15 que $f(x)$ es un factor irreducible de $x^{p^n} - x$. De igual forma, por la Proposición 2.1.15 sabemos que existe $\beta \in \mathbb{K}$ tal que su polinomio minimal sea $f(x)$. Por lo cual $\mathbb{Z}_p(\beta) \cong \mathbb{Z}_p[x]/\langle f(x)\rangle$ y así $\mathbb{Z}_p(\beta)$ es un subcuerpo de $\mathbb{K}$ con p^n elementos. De lo anterior, se concluye que $\mathbb{K} = \mathbb{Z}_p(\beta) \cong \mathbb{Z}_p[x]/\langle f(x)\rangle \cong \mathbb{F}$. □

Como existe un único cuerpo con q elementos, denotamos a dicho cuerpo por $\mathbb{F}_q$ donde se entiende que q es la potencia de algún primo. Algunos autores denotan este cuerpo por $GF(q)$, en honor a Évariste Galois y lo llaman "*cuerpo de Galois de orden* q", (Galois Field en inglés).

Teorema 2.1.18. *(Criterio de Subcuerpo). Sea $\mathbb{F}_q$ el cuerpo finito con $q = p^n$ elementos. Si $\mathbb{K}$ es un subcuerpo de $\mathbb{F}_q$, entonces $\mathbb{K}$ tiene p^m elementos donde $m \mid n$. Recíprocamente, para cada divisor m de n, $\mathbb{K} = \left\{x \in \mathbb{F}_q \mid x^{p^m} = x\right\}$ es el único subcuerpo de $\mathbb{F}_q$ con p^m elementos.*

Demostración. Sea $\mathbb{K}$ un subcuerpo de $\mathbb{F}_q$. Si vemos a $\mathbb{K}$ como un subgrupo del grupo aditivo $\mathbb{F}_q$ concluimos por el Teorema de Lagrange que $|\mathbb{K}| = p^m$ con $m \leq n$. Sea t el grado de la extensión $\mathbb{F}_q/\mathbb{K}$, entonces $|\mathbb{F}_q| = (p^m)^t = p^n$ por lo que $mt = n$ y así $m \mid n$.

Recíprocamente, supongamos que $m \mid n$. Entonces, dado que

$$p^n - 1 = (p^m - 1)(p^{n-m} + p^{n-2m} + \cdots + p^m + 1), \tag{2.1}$$

vemos que $p^m - 1 \,|\, p^n - 1$. Ahora, como $p^m - 1 \,|\, p^n - 1$ podemos reemplazar en la ecuación 2.1 a p por x, m por $p^m - 1$ y n por $p^n - 1$ para obtener que $x^{p^m-1} - 1$ es un factor de $x^{p^n-1} - 1$ en $\mathbb{F}_q[x]$ y multiplicando por x vemos que $x^{p^m} - x$ es un factor de $x^{p^n} - x$ en $\mathbb{F}_q[x]$. De la Proposición 2.1.14 sabemos que $x^{p^n} - x$ contiene todas sus raíces en $\mathbb{F}_q$ que implica $x^{p^m} - x$ contiene todas sus raíces en $\mathbb{F}_q$.

Adicionalmente, en la demostración del Teorema 2.1.4 vimos que si un cuerpo con característica p contiene todas las raíces de $x^{p^m} - x$, entonces dichas raíces forman un cuerpo de p^m elementos. Lo que nos permite concluir que $\mathbb{K} = \left\{x \in \mathbb{F}_q \mid x^{p^m} = x\right\}$ es un subcuerpo de $\mathbb{F}_q$ con p^m elementos. Para finalizar, si suponemos que existen dos

subcuerpos distintos de $\mathbb{F}_q$ con p^m elementos, obtendriamos que el polinomio $x^{p^m} - x$ tiene mas de p^m raíces en $\mathbb{F}_q$, lo que claramente es un absurdo. □

Observación 2.1.19. Las proposiciones 2.1.13, 2.1.14 y 2.1.15 también se valen si tomamos $p = q$ y $\mathbb{F}_q$ en vez de $\mathbb{Z}_p$.

Ejemplo 2.1.20. Gracias al Teorema 2.1.18 los subcuerpos del cuerpo finito $\mathbb{F}_{3^{18}}$ se obtienen a partir de los divisores positivos de 18. En la Figura 2.1 se encuentran las relaciones de contenencia entre los distintos subcuerpos de $\mathbb{F}_{3^{18}}$.

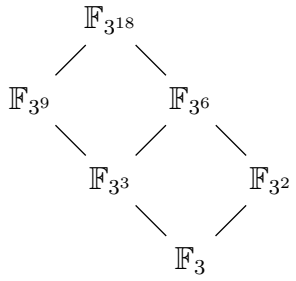

Figura 2.1: Subcuerpos de $\mathbb{F}_{3^{18}}$.

Definición 2.1.21. Sean $\mathbb{F}/\mathbb{K}$ una extensión de cuerpos, $\mathbb{L}$ y $\mathbb{T}$ cuerpos intermedios de $\mathbb{F}/\mathbb{K}$. Entonces el menor cuerpo intermedio de $\mathbb{F}/\mathbb{K}$ que contiene a $\mathbb{L}$ y $\mathbb{T}$ (esto es la intersección de todos los cuerpos intermedios que contienen a $\mathbb{L}$ y $\mathbb{T}$) es denotado por $\mathbb{LT}$.

Teorema 2.1.22. *Sean $\mathbb{F}_{q^n}/\mathbb{F}_q$ una extensión de cuerpos, m y l divisores de n. Entonces $\mathbb{F}_{q^m}$ y $\mathbb{F}_{q^l}$ son cuerpos intermedios de $\mathbb{F}_{q^n}/\mathbb{F}_q$. Además, se vale que $\mathbb{F}_{q^m} \cap \mathbb{F}_{q^l} = \mathbb{F}_{q^d}$ y $\mathbb{F}_{q^m}\mathbb{F}_{q^l} = \mathbb{F}_{q^k}$ donde $d = mcd(l, m)$ y $k = mcm(l, m)$.*

Demostración. Por el Teorema 2.1.18 tenemos que $\mathbb{F}_{q^m}$ y $\mathbb{F}_{q^l}$ son subcuerpos de $\mathbb{F}_{q^n}$ que contienen a $\mathbb{F}_q$. Como la intersección de subcuerpos es subcuerpo tenemos que $\mathbb{F}_{q^m} \cap \mathbb{F}_{q^l}$ es un subcuerpo de $\mathbb{F}_{q^n}$ que a su vez contiene a $\mathbb{F}_q$ por lo que esta intersección es un cuerpo intermedio de $\mathbb{F}_{q^n}/\mathbb{F}_q$. Por el Corolario 1.1.17, tenemos que $[\mathbb{F}_{q^m} \cap \mathbb{F}_{q^l} : \mathbb{F}_q] = t$ con $t|n$; luego $\mathbb{F}_{q^m} \cap \mathbb{F}_{q^l} = \mathbb{F}_{q^t}$. Note que como $\mathbb{F}_{q^t} \subseteq \mathbb{F}_{q^m}$ y $\mathbb{F}_{q^t} \subseteq \mathbb{F}_{q^l}$ tenemos que t es un divisor en común entre m y l, así que $t|d$. Por otro lado $\mathbb{F}_{q^d} \subseteq \mathbb{F}_{q^m} \cap \mathbb{F}_{q^l}$ que implica que $d|t$ y por lo tanto $t = d$.

Ahora bien, como n es un multiplo en común de m y l tenemos que $k|n$ y por lo tanto $\mathbb{F}_{q^k}$ es un cuerpo intermedio de $\mathbb{F}_{q^n}/\mathbb{F}_q$ que contiene tanto a $\mathbb{F}_{q^m}$ como a $\mathbb{F}_{q^l}$. Para finalizar, sea $\mathbb{L}$ un cuerpo intermedio de $\mathbb{F}_{q^n}/\mathbb{F}_q$ que contiene tanto $\mathbb{F}_{q^m}$ como a $\mathbb{F}_{q^l}$, una vez más por el Corolario 1.1.17 tenemos que $\mathbb{L} = \mathbb{F}_{q^t}$ donde t es un múltiplo de m y l luego $k|t$ y así $\mathbb{F}_{q^k} \subseteq \mathbb{L}$. Lo que implica que $\mathbb{F}_{q^m}\mathbb{F}_{q^l} = \mathbb{F}_{q^k}$. □

En el caso particular donde $mcd(m, l) = 1$ y $n = lm$ tenemos que $\mathbb{F}_{q^m} \cap \mathbb{F}_{q^l} = \mathbb{F}_q$ y $\mathbb{F}_{q^m}\mathbb{F}_{q^l} = \mathbb{F}_{q^n}$.

Ahora mostaremos que algunos resultados de los enteros módulo p, siendo p un primo, se generalizan a todo cuerpo finito. Empezaremos mostrando la generalización del ítem III) del Teorema 1.3.10.

Teorema 2.1.23. *Sea $\mathbb{F}_q$ un cuerpo finito distinto de $\mathbb{F}_2$, entonces $\sum_{x\in\mathbb{F}_q} x = 0$.*

Demostración. Sea α un elemento primitivo de $\mathbb{F}_q$, como $\mathbb{F}_q$ es distinto de $\mathbb{F}_2$, entonces $\alpha \neq 1$ y así

$$\frac{\alpha^q - 1}{\alpha - 1} = 1 + \alpha + \alpha^2 + \cdots + \alpha^{q-1}.$$

Como α genera $\mathbb{F}_q^*$ entonces $\sum_{x\in\mathbb{F}} x = \sum_{i=1}^{q-1} \alpha^i$ y por lo tanto

$$\sum_{x\in\mathbb{F}} x = \frac{\alpha^q - 1}{\alpha - 1} - 1 = \frac{\alpha - 1}{\alpha - 1} - 1 = 0.$$

□

Veamos la generalización del Teorema de Wilson.

Teorema 2.1.24. *Sea $\mathbb{F}$ un cuerpo finito, entonces $\prod_{x\in\mathbb{F}^*} x = -1$.*

Demostración. Si la característica de $\mathbb{F}$ es un primo impar, entonces el polinomio $x^2 - 1$ tiene exactamente dos raíces en $\mathbb{F}$, 1 y -1, las cuales son distintas. Esto implica que 1 y -1 son los únicos elementos de $\mathbb{F}^*$ que son su propio inverso, luego al realizar la multiplicación de todos los elementos de $\mathbb{F}^*$, podemos agrupar de a parejas, cada elemento distinto de estos con su inverso y obtener lo deseado. Por otro lado, si la característica de $\mathbb{F}$ es 2, entonces el polinomio $x^2 - 1$ se puede factorizar en $\mathbb{F}$ como $(x-1)(x-1)$ y así 1 es la única raíz en $\mathbb{F}$. Es decir, el 1 es el único elemento cuyo inverso es si mismo . Al igual que en el caso anterior, agrupando de a parejas, obtenemos que $\prod_{x\in\mathbb{F}^*} x = 1$ pero como $1 = -1$ concluimos lo deseado. □

Finalmente, presentamos el criterio de Euler para cuerpos finitos.

Teorema 2.1.25. *Sea $\mathbb{F}_{p^n}$ el cuerpo finito de p^n elementos con p un primo impar y sea $\alpha \neq 0$ en $\mathbb{F}_{p^n}$, entonces:*

I) *α es un cuadrado en $\mathbb{F}_{p^n}$ si, y solo si, $\alpha^{\frac{p^n-1}{2}} = 1$*

II) *α no es cuadrado en $\mathbb{F}_{p^n}$ si, y solo si, $\alpha^{\frac{p^n-1}{2}} = -1$.*

III) *Los cuadrados no nulos de $\mathbb{F}_{p^n}$ forman un subgrupo de $\mathbb{F}_{p^n}^*$ de índice 2 y por lo tanto hay exactamente $\frac{p^n+1}{2}$ cuadrados en $\mathbb{F}_{p^n}$.*

Demostración. Probaremos cada una de las afirmaciones.

I) Supongamos que existe $\beta \neq 0$ en $\mathbb{F}_{p^n}$ tal que $\beta^2 = \alpha$, entonces $\alpha^{\frac{p^n-1}{2}} = \beta^{p^n-1} = 1$. Recíprocamente, supongamos que $\alpha^{\frac{p^n-1}{2}} = 1$ y sea $\mathbb{L}$ una extensión de $\mathbb{F}_{p^n}$ que contiene a un elemento β tal que $\beta^2 = \alpha$, entonces $\beta^{p^n-1} = 1$ y por lo tanto $\beta \in \mathbb{F}_{p^n}$ lo que implica que α es un cuadrado en $\mathbb{F}_{p^n}$.

II) Supongamos que α no es cuadrado en $\mathbb{F}_{p^n}$. Note que $\alpha^{\frac{p^n-1}{2}}$ es raíz del polinomo x^2-1, luego $\alpha^{\frac{p^n-1}{2}} = 1$ o $\alpha^{\frac{p^n-1}{2}} = -1$ pero como α no es cuadrado por el ítem anterior concluimos que $\alpha^{\frac{p^n-1}{2}} = -1$. Para la recíproca, note que si α es un cuadrado en $\mathbb{F}_{p^n}$ por el ítem anterior tenemos que $\alpha^{\frac{p^n-1}{2}} = 1$ y como el primo es impar tenemos que $1 \neq -1$, luego $\alpha^{\frac{p^n-1}{2}} \neq -1$.

III) Sea $H = \left\{\alpha \in \mathbb{F}_{p^n}^* \mid \alpha \text{ es un cuadrado en } \mathbb{F}_{p^n}\right\}$ y sean $\alpha, \beta \in \mathbb{F}_{p^n}$, entonces

$$\left(\alpha\beta^{-1}\right)^{\frac{p^n-1}{2}} = \alpha^{\frac{p^n-1}{2}}(\beta^{-1})^{\frac{p^n-1}{2}} = 1.$$

Luego, $\alpha\beta^{-1} \in H$. Ahora, para ver que el índice de H es 2, sean α y β en $\mathbb{F}_{p^n}$ que no sean cuadrados entonces

$$\left(\alpha\beta^{-1}\right)^{\frac{p^n-1}{2}} = \alpha^{\frac{p^n-1}{2}}(\beta^{-1})^{\frac{p^n-1}{2}} = (-1)(-1) = 1.$$

Luego, $\alpha\beta^{-1} \in H$, lo que implica que las clases laterales αH y βH sean iguales y así solo existen dos clases laterales distintas de H en $\mathbb{F}_{p^n}^*$. Finalmente del Teorema de Lagrange tenemos que $|H| = \frac{p^n-1}{2}$ pero como 0 también es un cuadrado tenemos que hay exactamente $\frac{p^n+1}{2}$ cuadrados en $\mathbb{F}_{p^n}$.

□

Como mencionamos en la Sección 2.1, todo cuerpo tiene una clausura algebraica. En general no hay un método para determinar la clausura algebraica de un cuerpo, sin embargo en el caso de $\mathbb{Z}_p$ siendo p un primo es posible construirla usando algunas herramientas de la teoría algebraica de números.

Definición 2.1.26. Sean $R \subseteq S$ anillos y $\alpha \in S$. Decimos que α es un **entero** sobre R si existe $f(x) \in R[X]$ mónico tal que $f(\alpha) = 0$.

El conjunto formado por todos los elementos de S que son enteros sobre R es llamado la **clausura entera** de R en S.

Definición 2.1.27. Sean $R \subseteq S$ anillos y $X \subseteq S$, denotamos por $R[X]$ a la intersección de todos los subanillos de S que contienen tanto a R como a X. Si $X = \{a_1, a_2, \ldots, a_n\}$ escribimos $R[a_1, a_2, \ldots, a_n]$ en vez de $R[\{a_1, a_2, \ldots, a_n\}]$.

Usaremos un par de resultados sobre enteros algebraicos.

Teorema 2.1.28. *Sean S un anillo conmutativo con unidad 1 y R un subanillo de S con $1 \in R$. Entonces*

I) *$\alpha \in S$ es entero sobre R si, y solo si, $R[\alpha]$ es finitamente generado como R-módulo.*

II) *Si los elementos $\alpha_1, \ldots, \alpha_n \in S$ son enteros sobre R, entonces el anillo $R[\alpha_1, \ldots, \alpha_n]$ es finitamente generado como R-módulo.*

III) *Si S es finitamente generado como R-módulo, entonces todo elemento de S es entero sobre R.*

IV) *La clausura entera de R en S es un subanillo de S.*

Demostración. Ver [1], Sección 10. □

Teorema 2.1.29. *Sean $R \leq S \leq T$ anillos conmutativos con la misma unidad $1 \in R$. Si S es finitamente generado como R-módulo y T es finitamente generado como S-módulo, entonces T es finitamente generado como R-módulo.*

Demostración. Ver [1], página 194. □

Lema 2.1.30. *Sean p un primo y R la clausura entera de $\mathbb{Z}$ en $\mathbb{C}$. Entonces*

I) *Existe un ideal maximal P de R con $p \in P$ y por tanto R/P es un cuerpo.*

II) *$\mathbb{Z}_p$ es isomorfo a un subcuerpo de R/P.*

Demostración. Probaremos cada una de las afirmaciones.

I) Del ítem I) del teorema anterior tenemos que R es un anillo con unidad. Si consideramos $I = pR$ tenemos que I es un ideal de R distinto de R puesto que si $p(a+bi) = 1$ entonces $a = 1/p$ y $b = 0$ lo que significa que $1/p$ es un entero sobre $\mathbb{Z}$. Esto es un absurdo ya que si existen $a_0, a_1, \ldots, a_{n-1} \in \mathbb{Z}$ tales que

$$\frac{1}{p^n} + a_{n-1}\frac{1}{p^{n-1}} + \cdots + a_1\frac{1}{p} + a_0 = 0.$$

Multiplicando por p^n obtenemos:

$$1 + a_{n-1}p + \cdots + a_1p^{n-1} + a_0p^n = 0.$$

Lo que implica que $p \mid 1$. Así, por el Lema de Zorn se puede garantizar la existencia de un ideal maximal P de R tal que $pR \subseteq P$ y por lo tanto $p \in P$.

II) Primero veamos que $P \cap \mathbb{Z} = p\mathbb{Z}$. Es fácil ver que $P \cap \mathbb{Z}$ es un ideal de $\mathbb{Z}$ y que $p\mathbb{Z} \subseteq P \cap \mathbb{Z}$. Ahora si $P \cap \mathbb{Z} = \mathbb{Z}$, entonces $1 \in P$ y por tanto $P = R$, lo que es un absurdo; luego $P \cap \mathbb{Z} \neq \mathbb{Z}$. Como $p\mathbb{Z}$ es un ideal maximal de $\mathbb{Z}$ tenemos que $P \cap \mathbb{Z} = p\mathbb{Z}$.

Es claro que $\mathbb{Z} + P$ es un subanillo de R que contiene a P. Como P es un ideal de R también es un ideal de $\mathbb{Z} + P$ y por tanto podemos considerar el anillo cociente $(\mathbb{Z}+P)/P$. Veamos que $\mathbb{Z}/(P \cap \mathbb{Z}) \cong (\mathbb{Z}+P)/P$. Consideremos la función $f : \mathbb{Z}/(P \cap \mathbb{Z}) \to (\mathbb{Z}+P)/P$ tal que $f(\alpha + (P \cap \mathbb{Z})) = \alpha + P$. Supongamos que $\alpha, \beta \in \mathbb{Z}$ y $\alpha + (P \cap \mathbb{Z}) = \beta + (P \cap \mathbb{Z})$ entonces $\alpha - \beta \in P \cap \mathbb{Z}$ y así $\alpha - \beta \in P$ que implica que $\alpha + P = \beta + P$; luego f está bien definida. Para ver que f es inyectiva supongamos que $\alpha + P = \beta + P$, entonces $\alpha - \beta \in P$ pero como $\alpha, \beta \in \mathbb{Z}$ tenemos que $\alpha - \beta \in P \cap \mathbb{Z}$ y por lo tanto $\alpha + (P \cap \mathbb{Z}) = \beta + (P \cap \mathbb{Z})$.

Por otro lado, sea $(\alpha+p_1)+P \in (\mathbb{Z}+P)/P$, entonces $(\alpha+p_1)+P = (\alpha+P)+(p_1+P) = \alpha + P$; luego $f(\alpha) = (\alpha + p_1) + P$ y así f es sobreyectiva. No es difícil ver que f es un homomorfismo de anillos y por tanto f es un isomorfismo. Finalmente, dado que

$\mathbb{Z}_p = \mathbb{Z}/p\mathbb{Z} = \mathbb{Z}/(P \cap \mathbb{Z}) \cong (\mathbb{Z} + P)/P$, concluimos que $(\mathbb{Z} + P)/P$ es un subcuerpo de R/P isomorfo a $\mathbb{Z}_p$.

□

Teorema 2.1.31. *R/P es la clausura algebraica de $\mathbb{Z}_p$.*

Demostración. Por el Teorema 1.1.25 basta mostrar que R/P es algebraicamente cerrado y una extensión algebraica de $\mathbb{Z}_p$. Veamos que R/P es algebraicamente cerrado. Sea $f(x) \in (R/P)[x]$, como R/P es cuerpo podemos escribir a $f(x) = ah(x)$ donde a es el coeficiente principal de f y $h(x) \in (R/P)[x]$. Así, $h(x)$ es mónico y $h(x) = g(x) + P$ donde $g(x) \in R[x]$. Escribamos $g(x) = x^n + \cdots + a_1x + a_0$, como $g(x) \in \mathbb{C}[x]$ y $\mathbb{C}$ es algebraicamente cerrado existe $\alpha \in \mathbb{C}$ tal que $g(\alpha) = 0$. Note que $g(x) \in M$, siendo $M = \mathbb{Z}[a_0, a_1, \ldots, a_{n-1}]$ y α es entero sobre M; luego por el ítem I) del Teorema 2.1.28, $M[\alpha]$ es un M-módulo finitamente generado.

Como cada a_i es entero sobre $\mathbb{Z}$ tenemos por el ítem II) del Teorema 2.1.28 que M es un $\mathbb{Z}$-módulo finitamente generado y así $M[\alpha]$ es un $\mathbb{Z}$-módulo finitamente generado por el Teorema 2.1.29. De esta forma concluimos que α es un entero sobre $\mathbb{Z}$ por el ítem III) del Teorema 2.1.28; es decir, $\alpha \in R$ y llamando $\overline{\alpha} = \alpha + P$ tenemos que $f(\overline{\alpha}) = a(h(\overline{\alpha})) = a(g(\alpha) + P) = P$ y así f tiene una raíz en R/P; luego R/P es algebraicamente cerrado.

Finalmente, veamos que R/P es una extensión algebraica de $\mathbb{Z}_p$. Para esto basta ver que R/P es una extensión algebraica de $(\mathbb{Z} + P)/P$. Sea $\alpha + P \in R/P$, como $\alpha \in R$ existe $f(x) \in \mathbb{Z}[x]$ mónico tal que $f(\alpha) = 0$. Escribamos $f(x) = x^n + \cdots + a_1x + a_0$ y consideremos $h(x) = x^n + \cdots + \overline{a_1}x + \overline{a_0}$ donde $\overline{a_i} = a_i + P$, entonces $h(x)(\alpha + P) = f(\alpha) + P = 0$ y así $\alpha + P$ es algebraico sobre $(\mathbb{Z} + P)/P$. □

2.2. Polinomios irreducibles y Automorfismos de Galois

Los polinomios irreducibles sobre cuerpos finitos juegan un papel muy importante en la construcción y estudio de dichos cuerpos. En esta sección, mostraremos algunas propiedades y daremos una fórmula explícita para el número de polinomios mónicos irreducibles en $\mathbb{F}_q[x]$. Además, veremos como se relacionan las raíces de los polinomios minimales con ciertos automorfismos de $\mathbb{F}_{q^n}$.

Teorema 2.2.1. *Sea $\mathbb{F}_q$ el cuerpo finito de q elementos, entonces:*

I) *Para cada $d \in \mathbb{N}$, existe un polinomio irreducible sobre $\mathbb{F}_q$ de grado d. Cada polinomio irreducible sobre $\mathbb{F}_q$ de grado d, divide a $x^{q^d} - x$.*

II) *Sea $n \in \mathbb{N}$, entonces un polinomio irreducible $f \in \mathbb{F}_q[x]$ divide a $x^{q^n} - x$ si, y solo si, el grado de f divide a n.*

III) *El número de polinomios mónicos irreducibles sobre $\mathbb{F}_q$ de grado n es*

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

donde μ es la función de Möbius definida en la Sección 2.3. Si n es primo este número es $\frac{q^n-q}{n}$.

Demostración. Probaremos cada una de las afirmaciones.

I) Sea $d \in \mathbb{N}$. Por el Teorema 2.1.18 sabemos que $\mathbb{F}_{q^d}$ es una extensión de $\mathbb{F}_q$ de grado d. Sean α un elemento primitivo de $\mathbb{F}_{q^d}$ y $f(x)$ su polinomio minimal sobre $\mathbb{F}_q$, entonces $f(x)$ es irreducible con $\partial f = [\mathbb{F}_q(\alpha) : \mathbb{F}_q] = \left[\mathbb{F}_{q^d} : \mathbb{F}_q\right] = d$.
Ahora bien, sea $f(x)$ un polinomio irreducible sobre $\mathbb{F}_q$ de grado d y sea α una raíz de $f(x)$ en $\overline{\mathbb{F}_q}$. Entonces $\mathbb{F}_q(\alpha)$ es un cuerpo con q^d elementos y así α es raíz del polinomio $x^{q^d} - x$. Como el polinomio minimal de α sobre $\mathbb{F}_q$ es $f(x)$ concluimos que $f(x) \mid x^{q^d} - x$.

II) Supongamos que $f(x) \in \mathbb{F}_q[x]$ es un polinomio irreducible de grado d tal que $f(x) \mid x^{q^n} - x$. Por el mismo argumento usado en el ítem anterior, tenemos que $\mathbb{F}_{q^n}/\mathbb{F}_q$ es una extensión finita de grado n, en el que todo elemento de $\mathbb{F}_{q^n}$ es raíz de $x^{q^n} - x$. Teniendo en cuenta que $f \mid x^{q^n} - x$, tenemos que existe $\alpha \in \mathbb{F}_{q^n}$ tal que α es raíz de $f(x)$ y así:

$$[\mathbb{F}_{q^n} : \mathbb{F}_q] = [\mathbb{F}_{q^n} : \mathbb{F}_q(\alpha)]\,[\mathbb{F}_q(\alpha) : \mathbb{F}_q]$$

$$n = td$$

Por lo que concluimos que $d|n$. Recíprocamente, supongamos que f es un polinomio irreducible sobre $\mathbb{F}_q$ tal que d, el grado de f, divide a n. Entonces $q^d - 1 \mid q^n - 1$ y por tanto $x^{q^d-1} - 1 \mid x^{q^n-1} - 1$. Multiplicando por x vemos que $x^{q^d} - x \mid x^{q^n} - x$. Finalmente, como $f(x)$ es un polinomio irreducible de grado d sobre $\mathbb{F}_q$ concluimos por el ítem I) que $f \mid x^{q^d} - x$ y así $f \mid x^{q^n} - x$.

III) Para cada $n \in \mathbb{N}$ denotamos por A_n al conjunto de todos los polinomios mónicos irreducibles de grado n sobre $\mathbb{F}_q$ y por $\alpha(n)$ a la cardinalidad de A_n. Del ítem II) tenemos que los polinomios mónicos irreducibles sobre $\mathbb{F}_q$ que aparecen en la factorización de $x^{q^n} - x$ son aquellos cuyo grado divide a n y como la derivada de $x^{q^n} - x$ es -1 tenemos por el criterio de la derivada que $x^{q^n} - x$ no tiene raíces múltiples en su clausura algebraica; luego cada uno de estos polinomios irreducibles solo aparece una vez en la factorización y por lo tanto

$$x^{q^n} - x = \prod_{d|n} \prod_{f \in A_d} f(x).$$

Si nos fijamos en la cantidad de factores lineales en los que se puede expresar el polinomio de la derecha y el de la izquierda, concluimos que:

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

A partir de la ecuación anterior podemos definir $F(n) = \sum_{d|n} f(d)$ donde $f(d) = d\alpha(d)$. Usando la formula de inversión de Möbius, obtenemos que:

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

$$n\alpha(n) = \sum_{d|n} \mu(d) F(n/d) = \sum_{d|n} \mu(d) q^{n/d}$$

que implica que:

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

Finalmente, si n es primo, entonces $\alpha(n) = \frac{1}{n}\left(\mu(1)q^n + \mu(n)q\right) = \frac{q^n - q}{n}$.

□

El siguiente corolario es una consecuencia inmediata de la Proposición 2.1.15 y del ítem II) del teorema anterior tomando $q = p$.

Corolario 2.2.2. *Sea $\mathbb{F}$ un cuerpo de p^n elementos. Entonces el grado del polinomio minimal de cada elemento de $\mathbb{F}$ sobre $\mathbb{Z}_p$ es divisor de n.*

En vista de la Observación 2.1.19, tenemos un resultado más general.

Corolario 2.2.3. *Sea $\mathbb{F}_{q^n}/\mathbb{F}_q$ una extensión de cuerpos. Entonces el grado del polinomio minimal de cada elemento de $\mathbb{F}_{q^n}$ sobre $\mathbb{F}_q$ es divisor de n.*

Ejemplo 2.2.4. Usando el ítem II) del Teorema 2.2.1 tenemos que el grado de los polinomios irreducibles sobre $\mathbb{Z}_5$ que dividen al polinomio $x^{25}-x$ es uno o dos y claramente hay exactamente 5 polinomios irreducibles lineales sobre $\mathbb{Z}_5$, los cuales son:

$$x, \;\; x-1, \;\; x-2, \;\; x-3, \;\; x-4$$

Por el ítem III) del mismo teorema, sabemos que la cantidad de polinomios irreducibles de grado 2 sobre $\mathbb{Z}_5$ es:

$$\frac{5^2-5}{2} = 10$$

En particular, dado que 2 no es residuo cuadrático en $\mathbb{Z}_5$, los siguientes polinomios son irreducibles sobre $\mathbb{Z}_5$:

$$x^2-2, \;\; (x-1)^2-2, \;\; (x-2)^2-2, \;\; (x-3)^2-2, \;\; (x-4)^2-2$$

De igual forma, como 3 tampoco es residuo cuadrático en $\mathbb{Z}_5$, los otros 5 polinomios irreducibles de grado 2 sobre $\mathbb{Z}_5$ son:

$$x^2-3, \;\; (x-1)^2-3, \;\; (x-2)^2-3, \;\; (x-3)^2-3, \;\; (x-4)^2-3$$

Luego, el producto de estos 15 polinomios es la factorización en irreducibles de $x^{25}-x$ en $\mathbb{Z}_5[x]$.

A partir del Teorema 2.2.1 surge el siguiente criterio de irreducibilidad.

Corolario 2.2.5. *Sea $f(x)$ un polinomio de grado n sobre $\mathbb{F}_q$. Entonces f es irreducible, si y solo si, $x^{q^d}-x$ y $f(x)$ son primos relativos para todo $d \in \mathbb{N}$ tal que $1 \leq d \leq \frac{n}{2}$*

Demostración. Supongamos que existe $1 \leq d \leq \frac{n}{2}$ tal que $x^{q^d}-x$ y $f(x)$ no son primos relativos, esto implica que existe un polinomio irreducible no constante $q(x) \in \mathbb{F}_q[x]$ que divide a ambos polinomios. Se sigue del ítem II) del Teorema 2.2.1 que el grado de $q(x)$ divide a d, por tanto $q(x)$ es un polinomio de grado menor que n que divide a $f(x)$, luego $f(x)$ es reducible. Recíprocamente, supongamos que $f(x)$ es reducible, entonces existe un polinomio irreducible $q(x)$ de grado menor o igual que $\frac{n}{2}$ que divide a $f(x)$. Una vez más, por ítem II) del Teorema 2.2.1 $q(x)$ divide a $x^{q^d}-x$ para algún $d \leq \frac{n}{2}$ y por tanto $x^{q^d}-x$ y $f(x)$ no son primos relativos. □

Ejemplo 2.2.6. Veamos que $x^5 - x - 1$ es irreducible en $\mathbb{Z}_3[x]$. Por el Corolario 2.2.5 basta probar que $x^5 - x - 1$ es primo relativo tanto a $x^3 - x$ como a $x^9 - x$. La factorización en polinomios irreducibles de estos dos polinomios es:

$$x^9 - x = x(x-1)(x+1)(x^2+x+2)(x^2+2x+2)(x^2+1).$$

$$x^3 - x = x(x-1)(x+1).$$

Note que como $x^5 - x - 1$ no tiene raíces en $\mathbb{Z}_3$ y

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

Entonces ningún factor irreducible de $x^9 - x$ ni de $x^3 - x$ divide a dicho polinomio y así hemos mostrado que son primos relativos.

Otra característica importante de los polinomios irreducibles sobre cuerpos finitos son sus raíces. El siguiente teorema muestra que dados cualquier polinomio irreducible sobre $\mathbb{F}_q$ y α una raíz en alguna extensión se tiene que $\mathbb{F}_q(\alpha)$ contiene todas las raíces del polinomio. Este resultado no vale para cuerpos en general. Si consideramos $x^3 - 2$ un polinomio irreducible sobre $\mathbb{Q}$ y $\sqrt[3]{2}$ una raíz en $\mathbb{C}$, vemos que $\mathbb{Q}\left(\sqrt[3]{2}\right)$ no contiene a las otras dos raíces complejas.

Teorema 2.2.7. *Si $f(x)$ es un polinomio irreducible sobre $\mathbb{F}_q$ de grado n, entonces $f(x)$ tiene una raíz $\alpha \in \mathbb{F}_{q^n}$. De hecho, todas las raíces de $f(x)$ son simples y son dadas por los elementos distintos $\alpha, \alpha^q, \alpha^{q^2}, \ldots, \alpha^{q^{n-1}}$.*

Demostración. Sea $\alpha \in \overline{\mathbb{F}_q}$ una raíz de f. Entonces $[\mathbb{F}_q(\alpha) : \mathbb{F}_q] = n$, por tanto $\mathbb{F}_q(\alpha) = \mathbb{F}_{q^n}$ y así $\alpha \in \mathbb{F}_{q^n}$. Sea $\beta \in \mathbb{F}_{q^n}$ una raíz de f. Escribamos $f(x) = a_n x^n + \cdots + a_1 x + a_0$ con $a_i \in \mathbb{F}_q$ para $0 \leq i \leq n$. Entonces $f(\beta) = a_n\beta^n + \cdots + a_1\beta + a_0 = 0$. Usando la Proposición 2.1.14 y el Lema 2.1.3 obtenemos:

$$\begin{aligned} f(\beta^q) &= a_n(\beta^q)^n + \cdots + a_1\beta^q + a_0 \\ &= a_n^q(\beta^n)^q \cdots + a_1^q\beta^q + a_0^q \\ &= (a_n\beta^n + \cdots + a_1\beta + a_0)^q \\ &= f(\beta)^q = 0. \end{aligned}$$

Lo anterior muestra que como α es raíz de f, α^q también lo es. Lo que a su vez implica que $(\alpha^q)^q = \alpha^{q^2}$ sea raíz de f y de manera análoga se muestra que $\alpha^{q^3}, \alpha^{q^4}, \ldots, \alpha^{q^{n-1}}$ son raíces de f. Nos falta ver que dichas raíces son distintas.
Razonando por absurdo, supongamos que existen $j, k \in \mathbb{Z}^+$ tal que $\alpha^{q^j} = \alpha^{q^k}$ con $0 \leq j < k \leq n-1$. Entonces $(\alpha^{q^j})^{q^{n-k}} = (\alpha^{q^k})^{q^{n-k}}$ y por tanto $\alpha^{q^{n-k+j}} = \alpha^{q^n} = \alpha$. Así, α es raíz de $x^{q^{n-k+j}} - x$ y como f es un polinomio de grado mínimo de $\mathbb{F}_q$ para cual α es raíz tenemos que $f \mid x^{q^{n-k+j}} - x$ y por el ítem II) del Teorema 2.2.1 $n \mid n-k+j$. Por otro lado, note que como $j < k$ entonces $n-k+j < n$. Además, de la desigualdad $k < n$ tenemos que $0 < n-k$ y por tanto $0 \leq j < n-k+j$. De esta forma llegamos a que $0 < n-k+j < n$ que contradice que $n \mid n-k+j$. □

El siguiente corolario se sigue del Teorema 2.2.7.

Corolario 2.2.8. *Si $f(x)$ es un polinomio irreducible de grado n sobre $\mathbb{F}_q$, entonces $f(x)$ tiene todas sus raíces en $\mathbb{F}_{q^n}$.*

En la sección anterior vimos que $\mathbb{F}_{q^n}/\mathbb{F}_q$ es una extensión simple, veamos a partir de las propiedades de los polinomios irreducibles cuantos elementos generan esta extensión.

Teorema 2.2.9. *Sean $\mathbb{F}_{q^n}/\mathbb{F}_q$ una extensión de cuerpos y $H = \{\alpha \in \mathbb{F}_{q^n} \mid \mathbb{F}_q(\alpha) = \mathbb{F}_{q^n}\}$, entonces $|H| = \sum_{d|n} \mu(d) q^{n/d}$.*

Demostración. Afirmamos que

$$H = \left\{\alpha \in \overline{\mathbb{F}_q} \mid \exists p(x) \in \mathbb{F}_q[x] \text{ con } p(x) \text{ mónico e irreducible sobre } \mathbb{F}_q \text{ de grado } n \text{ y } p(\alpha) = 0\right\}$$

En efecto, sea $\alpha \in \mathbb{F}_{q^n}$ tal que $\mathbb{F}_q(\alpha) = \mathbb{F}_{q^n}$, entonces el grado del polinomio minimal de α es n y por tanto α es raíz de un polinomio mónico irreducible sobre $\mathbb{F}_q$ de grado n. Recíprocamente, sea $p(x)$ un polinomio irreducible sobre $\mathbb{F}_q$ de grado n y $\alpha \in \overline{\mathbb{F}_q}$ raíz de $p(x)$ como mostramos en el Teorema 2.2.7, $\alpha \in \mathbb{F}_{q^n}$ y $\mathbb{F}_q(\alpha) = \mathbb{F}_{q^n}$. Finalmente, para cada $p(x)$ mónico e irreducible sobre $\mathbb{F}_q$ de grado n, considere $H_{p(x)} = \left\{\alpha \in \overline{\mathbb{F}_q} \mid p(\alpha) = 0\right\}$. Entonces $|H_{p(x)}| = n$ y además como para cada $\alpha \in H$ existe un único polinomio mónico irreducible sobre $\mathbb{F}_q$ para el cual α es raíz, tenemos que los $H_{p(x)}$ forman una partición de H. Por otro lado, tenemos que la cantidad de polinomios mónicos irreducibles sobre $\mathbb{F}_q$ de grado n es $\frac{1}{n}\sum_{d|n} \mu(d) q^{n/d}$; luego $|H| = \sum_{d|n} \mu(d) q^{n/d}$. □

A continuación estudiaremos el comportamiento de un polinomio irreducible sobre $\mathbb{F}_q$, cuando es considerado sobre una extensión finita arbitraria de $\mathbb{F}_q$.

Lema 2.2.10. *Sean $\mathbb{F}_{q^n}/\mathbb{F}_q$ una extensión de cuerpos, $\mathbb{F}_{q^d}$ un cuerpo intermedio y $\alpha \in \mathbb{F}_{q^n}$ tal que $\mathbb{F}_q(\alpha) = \mathbb{F}_{q^n}$. Entonces el polinomio minimal de α sobre $\mathbb{F}_q$ se factoriza en $\mathbb{F}_{q^d}[x]$ en d polinomios irreducibles de grado n/d cada uno.*

Demostración. Sea $\alpha \in \mathbb{F}_{q^n}$ tal que $\mathbb{F}_q(\alpha) = \mathbb{F}_{q^n}$ y sea $f(x)$ el polinomio minimal de α sobre $\mathbb{F}_q$, entonces $f(x)$ tiene grado n y sus raíces son $\alpha, \alpha^q, \ldots, \alpha^{q^n}$, las cuales son todas distintas. Note que si $g(x)$ es un polinomio irreducible sobre $\mathbb{F}_{q^d}$ que divide a $f(x)$, entonces dado que $f(x)$ tiene todas sus raíces en $\mathbb{F}_{q^n}$ y como las raíces de $g(x)$ son raíces de $f(x)$ tenemos que $g(x)$ es el polinomio minimal sobre $\mathbb{F}_{q^d}$ de alguna raíz de $f(x)$. De igual forma, si β es una raíz de $f(x)$, entonces $f(\beta) = 0$ y por lo tanto el polinomio minimal de β respecto a $\mathbb{F}_{q^d}$ divide a $f(x)$.
Si consideramos la siguiente partición de las raíces de $f(x)$

$$C_i = \left\{\alpha^{q^i}, \alpha^{q^{i+d}}, \alpha^{q^{i+2d}}, \ldots, \alpha^{q^{i+(n-d)}}\right\} \text{ para } i = 0, \ldots, d-1$$

tenemos por el Teorema 2.2.7 que todos los elementos de C_i tienen el mismo polinomio minimal sobre $\mathbb{F}_{q^d}$ y que si dos elementos no pertenecen al mismo C_i, sus polinomios minimales sobre $\mathbb{F}_{q^d}$ son diferentes. Con esto hemos probado que $p_0, p_2, \ldots, p_{d-1}$, siendo p_i el polinomio minimal de α^{q^i} sobre $\mathbb{F}_{q^d}$, son exactamente los polinomios irreducibles sobre $\mathbb{F}_{q^d}$ que dividen a $f(x)$. Por otro lado, como todas las raíces de $f(x)$ son distintas concluimos que los factores irreducibles sobre $\mathbb{F}_{q^d}$ que dividen a $f(x)$ son todos distintos. Luego, la factorización en polinomios irreducibles sobre $\mathbb{F}_{q^d}$ de $f(x)$ es

$$f(x) = \prod_{i=0}^{d-1} p_i(x),$$

donde $p_i(x) = \prod_{\beta \in C_i}(x - \beta)$en $\mathbb{F}_{q^n}$. □

Teorema 2.2.11. *Sean $f(x)$ un polinomio irreducible de grado n sobre $\mathbb{F}_q$ y k un entero positivo. Considerando a $f(x)$ como un polinomio sobre $\mathbb{F}_{q^k}$, f se factoriza en d polinomios irreducibles distintos de grado n/d, donde $d = mcd(n, k)$. En particular, f se mantiene irreducible sobre $\mathbb{F}_{q^k}$ si, y solo si, $mcd(n, k) = 1$.*

Demostración. Si $k = n$ el resultado se sigue del Teorema 2.2.7. Supongamos que $k \neq n$ y sea $l = mcm(n, k)$, entonces la extensión $\mathbb{F}_{q^l}/\mathbb{F}_q$ tiene a $\mathbb{F}_{q^n}$ y a $\mathbb{F}_{q^k}$ como cuerpos intermedios. Como vimos en el Teorema 2.1.22, $\mathbb{F}_{q^n} \cap \mathbb{F}_{q^k} = \mathbb{F}_{q^d}$ y además como $f(x)$ es un polinomio irreducible de grado n, existe $\alpha \in \mathbb{F}_{q^n}$ raíz de $f(x)$ tal que $\mathbb{F}_q(\alpha) = \mathbb{F}_{q^n}$.

Luego, por el lema anterior f se factoriza en $\mathbb{F}_{q^d}$ como el producto de d polinomios irreducibles de grado n/d.

Sea $g(x)$ un factor irreducible mónico de f en $\mathbb{F}_{q^d}$, queremos ver que $g(x)$ sigue siendo irreducible sobre $\mathbb{F}_{q^k}$. Para esto, sea α una raíz de g en $\mathbb{F}_{q^n}$, entonces g es el polinomio minimal de α sobre $\mathbb{F}_{q^d}$ y como g tiene grado n/d tenemos que $\mathbb{F}_{q^d}(\alpha) = \mathbb{F}_{q^n}$. Además, tenemos que $\mathbb{F}_{q^d}(\alpha) \subseteq \mathbb{F}_{q^k}(\alpha)$; luego $\mathbb{F}_{q^k}(\alpha)$ contiene tanto a $\mathbb{F}_{q^n}$ como a $\mathbb{F}_{q^k}$.

Del Teorema 2.1.22 tenemos que $\mathbb{F}_{q^l}$ es el menor cuerpo intermedio de la extensión $\mathbb{F}_{q^l}/\mathbb{F}_q$ que contiene a $\mathbb{F}_{q^n}$ y a $\mathbb{F}_{q^k}$; es decir, no existen subcuerpos propios de $\mathbb{F}_{q^l}$ que contenga tanto a $\mathbb{F}_{q^n}$ como a $\mathbb{F}_{q^k}$ y por lo tanto $\mathbb{F}_{q^k}(\alpha) = \mathbb{F}_{q^l}$. Así, el grado del polinomio minimal de α sobre $\mathbb{F}_{q^k}$ es $\left[\mathbb{F}_{q^l} : \mathbb{F}_{q^k}\right] = \frac{l}{k} = \frac{n}{d} = \partial g$. Ahora como $g(\alpha) = 0$ y g es mónico, lo anterior muestra que g es el polinomio minimal de α sobre $\mathbb{F}_{q^k}$; luego g es irreducible sobre $\mathbb{F}_{q^k}$. □

Definición 2.2.12. Sean $\mathbb{F}_{q^n}/\mathbb{F}_q$ una extensión de cuerpos y $\alpha \in \mathbb{F}_{q^n}$. Entonces los elementos $\alpha, \alpha^q, \alpha^{q^2}, \ldots, \alpha^{q^{n-1}}$ son llamados los **conjugados** de α respecto a $\mathbb{F}_q$.

Si el polinomio minimal de α sobre $\mathbb{F}_q$ es de grado n, entonces los conjugados de α respecto a $\mathbb{F}_q$ son exactamente las raíces de su polinomio minimal. Si por el contrario, el grado d del polinomio minimal es un divisor propio de n, entonces $\alpha \in \mathbb{F}_{q^d}$ y $\alpha^q, \alpha^{q^2}, \ldots, \alpha^{q^{d-1}}$ son las otras raíces del polinomio minimal y como $\alpha^{q^d} = \alpha$, podemos ver los conjugados de α respecto a $\mathbb{F}_q$ como las raíces de su polinomio minimal repetidas $\frac{n}{d}$ veces.

Teorema 2.2.13. *Sea $\mathbb{F}_q$ el cuerpo finito de q elementos. Los conjugados de $\alpha \in \mathbb{F}_q^*$ con respecto a cualquier subcuerpo de $\mathbb{F}_q$ tiene el mismo orden en el grupo multiplicativo $\mathbb{F}_q^*$.*

Demostración. Supongamos que $q = p^n$ con p primo, $n \in \mathbb{Z}^+$. Sean β un elemento primitivo de $\mathbb{F}_q$ y $\alpha \in \mathbb{F}_q^*$, entonces existe $t \in \mathbb{Z}^+$ tal que $\alpha = \beta^t$. Sea $\mathbb{K}$ un subcuerpo de $\mathbb{F}_q$, entonces $\mathbb{K} = \mathbb{F}_{p^m}$ con $m \mid n$. Así, los conjugados de α con respecto a $\mathbb{K}$ son $\alpha, \alpha^{p^m}, \alpha^{p^{2m}}, \ldots, \alpha^{p^{n-m}}$.
Como $\alpha = \beta^t$, tenemos por el Teorema 1.2.5 que:

$$o(\alpha) = \frac{p^n - 1}{mcd(p^n - 1, t)} \quad \text{y} \quad o(\alpha^{p^j}) = \frac{p^n - 1}{mcd(p^n - 1, tp^j)}$$

Dado que $mcd(p^n - 1, p^j) = 1$, concluimos que $mcd(p^n - 1, t) = mcd(p^n - 1, tp^j)$ y así $o(\alpha) = o(\alpha^{p^j})$ para $j = m, 2m, \ldots, n - m$. □

Como consecuencia inmediata del Teorema 2.2.13 se tiene el siguiente corolario.

Corolario 2.2.14. *Si α es un elemento primitivo de un cuerpo finito $\mathbb{F}$, también lo son sus conjugados con respecto a cualquier subcuerpo de $\mathbb{F}$.*

Ejemplo 2.2.15. Sea $\alpha \in \mathbb{F}_{16}$ una raíz de $x^4 + x + 1 \in \mathbb{F}_2[x]$. Como α^3 ni $\alpha^5 = \alpha^2 + \alpha$ son iguales a la unidad, tenemos que α es un elemento primitivo $\mathbb{F}_{16}$. Por lo que concluimos que los conjugados de α respecto a $\mathbb{F}_2$ α, α^2, $\alpha^4 = \alpha + 1$, $\alpha^8 = \alpha^2 + 1$ son también elementos primitivos de $\mathbb{F}_{16}$. Por otro lado, los conjugados de α respecto a $\mathbb{F}_4$ son solo α, α^4.

Existe una relación entre los elementos conjugados y ciertos automorfismos de $\mathbb{F}_{q^n}$. Para esto necesitamos algunas nociones de la Teoría de Galois que enunciaremos a continuación.

Definición 2.2.16. Sea $\mathbb{F}/\mathbb{K}$ una extensión de cuerpos. Decimos que un automorfismo de $\mathbb{F}$ es un **automorfismo de Galois**, si fija los elementos de $\mathbb{K}$. Claramente, el conjunto de todos los automorfismos de Galois de $\mathbb{F}/\mathbb{K}$ forma un grupo con la composición de funciones, llamado el **grupo de Galois** $\mathrm{Gal}\,(\mathbb{F}/\mathbb{K})$ de $\mathbb{F}/\mathbb{K}$.

Teorema 2.2.17. *Los distintos automorfimos de Galois de $\mathbb{F}_{q^n}/\mathbb{F}_q$ son exactamente los mapeos $\sigma_0, \sigma_1, \ldots, \sigma_{n-1}$ definidos por $\sigma_j(\alpha) = \alpha^{q^j}$ para $\alpha \in \mathbb{F}_{q^n}$ y $0 \leq j \leq n-1$.*

Demostración. Sea $j \in \mathbb{Z}^+$ tal que $0 \leq j \leq n-1$. Veamos que σ_j es un automorfimo de Galois de $\mathbb{F}_{q^n}/\mathbb{F}_q$. Sean $\alpha, \beta \in \mathbb{F}_{q^n}$, es claro que $\sigma_j(\alpha\beta) = \sigma_j(\alpha)\sigma_j(\beta)$ y $\sigma_j(\alpha + \beta) = \sigma_j(\alpha) + \sigma_j(\beta)$ por el Lema 2.1.3. Luego σ_j es un homomorfismo. Ahora, para la inyectividad supongamos que $\alpha^{q^j} = \beta^{q^j}$ y una vez más por el Lema 2.1.3 tenemos $(\alpha - \beta)^{q^j} = 0$ lo que implica que $\alpha = \beta$. Por otra parte, como σ_j es una aplicación inyectiva cuyo dominio y contradominio son finitos y de la misma cardinalidad, σ_j debe ser sobreyectiva.

Sea $\delta \in \mathbb{F}_q$, entonces $\delta^q = \delta$. Si usamos la igualdad anterior y el hecho de que $q^i = q(q^{i-1})$ obtenemos:

$$\delta^{q^j} = \delta^{q^{j-1}} = \delta^{q^{j-2}} = \cdots = \delta^q = \delta.$$

Lo que muestra que σ_j fija los elementos de $\mathbb{F}_q$. El hecho de que los automorfimos σ_j sean distintos se sigue de que $\sigma_j(\beta) \neq \sigma_i(\beta)$ para todo $i \neq j$ con $0 \leq i, j \leq n-1$ donde β es un elemento primitivo de $\mathbb{F}_{q^n}$.

Nos falta ver que efectivamente los σ_j son todos los automorfismos de Galois de $\mathbb{F}_{q^n}/\mathbb{F}_q$. Supongamos que ψ un automorfismo de Galois de $\mathbb{F}_{q^n}/\mathbb{F}_q$. Sean β un elemento primitivo de $\mathbb{F}_{q^n}$ y f el polinomio minimal de β sobre $\mathbb{F}_q$. Escribamos $f(x) = x^n + a_{n-1}x^{n-1}\cdots + a_1x + a_0$ con $a_i \in \mathbb{F}_q$ para $0 \leq i \leq n-1$. Entonces $\beta^n + a_{n-1}\beta^{n-1}\cdots + a_1\beta + a_0 = 0$ que implica que $\psi(\beta^n + a_{n-1}\beta^{n-1}\cdots + a_1\beta + a_0) = 0$. Como ψ es un homomorfismo que fija los elementos de $\mathbb{F}_q$ tenemos que:

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

y asi, $\psi(\beta)$ es raíz de f. Luego, $\psi(\beta) = \beta^{q^j}$ para algun $0 \leq j \leq n-1$ por el Teorema 2.2.7. Afirmamos que $\psi = \sigma_j$. Es claro que $\psi(0) = \sigma_j(0)$. Ahora sea $x \in \mathbb{F}_{q^n}^*$, entonces existe $t \in \mathbb{Z}^+$ tal que $x = \beta^t$ y por lo tanto:

$$\psi(x) = \psi(\beta^t) = (\psi(\beta))^t = (\beta^{q^j})^t = (\beta^t)^{q^j} = x^{q^j}.$$

Luego, $\psi(x) = \sigma_j(x)$, para todo $x \in \mathbb{F}_{q^n}$.

□

Se sigue del Teorema 2.2.17 que $\mathrm{Gal}\,(\mathbb{F}_{q^n}/\mathbb{F}_q)$ es cíclico de orden n generado por σ_1, conocido como el automorfismo de Frobenius.

Ejemplo 2.2.18. Todo elemento de un cuerpo finito es la suma de dos cuadrados. En efecto, sea $\mathbb{F}$ un cuerpo finito con 2^n elementos entonces por el Teorema 2.2.17 tenemos que la aplicación $\sigma(\alpha) = \alpha^2$ es el automorfismo de Frobenius de la extensión $\mathbb{F}_{2^n}/\mathbb{F}_2$; luego todo elemento es un cuadrado.

Si $\mathbb{F}$ es un cuerpo finito con p^n elementos, con p un primo impar, entonces para cualquier $\alpha \in \mathbb{F}$ considere los conjuntos $\{\alpha - x^2 \mid x \in \mathbb{F}\}$ y $\{x^2 \mid x \in \mathbb{F}\}$. Por el ítem III) del Teorema 2.1.25 tenemos que la cardinalidad de cada uno de estos conjuntos es $\frac{p^n+1}{2}$ y así deben tener algún elemento en común; es decir, existen $x, y \in \mathbb{F}$ tal que $y^2 = \alpha - x^2$ y por lo tanto $\alpha = y^2 + x^2$.

Definición 2.2.19. Sea $\mathbb{F}$ un cuerpo. Decimos que un polinomio irreducible $f\,(x) \in \mathbb{F}\,[x]$ es **separable** si no tiene raíces múltiples en $\overline{\mathbb{F}}$. Si todo polinomio irreducible en $\mathbb{F}\,[x]$ es separable, decimos que $\mathbb{F}$ es un cuerpo **perfecto**. Dada una extensión $\mathbb{F}/\mathbb{K}$ de cuerpos, decimos que un elemento $\alpha \in \mathbb{F}$ es **separable** sobre $\mathbb{K}$, si es algebraico sobre $\mathbb{K}$ y m_α es

separable. La extensión $\mathbb{F}/\mathbb{K}$ es llamada **separable**, si todo elemento $\alpha \in \mathbb{F}$ es separable sobre $\mathbb{K}$.

Teorema 2.2.20. *Todo cuerpo finito es perfecto.*

Demostración. Sea $\mathbb{F}_q$ el cuerpo finito con q elementos y sea $f(x)$ un polinomio irreducible sobre $\mathbb{F}_q$, se sigue del Teorema 2.2.7 que $f(x)$ es separable y por tanto $\mathbb{F}_q$ es perfecto. □

Definición 2.2.21. Sea $\mathbb{F}/\mathbb{K}$ una extensión algebraica, decimos que $\mathbb{F}/\mathbb{K}$ es una extensión **normal** si todo polinomio irreducible sobre $\mathbb{K}$ que tiene alguna raíz en $\mathbb{F}$, tiene todas sus raíces en $\mathbb{F}$. Una extensión algebraica de cuerpos $\mathbb{F}/\mathbb{K}$ es llamada una **extensión de Galois** si es normal y separable.

Teorema 2.2.22. $\mathbb{F}_{q^n}/\mathbb{F}_q$ *es una extensión de Galois.*

Demostración. En primer lugar, es claro que $\mathbb{F}_{q^n}/\mathbb{F}_q$ es una extensión algebraica. Ahora, sea f un polinomio irreducible de grado m sobre $\mathbb{F}_q$ y supongamos que existe $\alpha \in \mathbb{F}_{q^n}$ raíz de f. Entonces $\mathbb{F}_q(\alpha) = \mathbb{F}_{q^m}$ es un subcuerpo de $\mathbb{F}_{q^n}$ y en virtud del Teorema 2.2.7 tenemos que $\mathbb{F}_{q^m}$ contiene todas las raíces de f, luego $\mathbb{F}_{q^n}/\mathbb{F}_q$ es una extensión normal. Por otro lado, como $\mathbb{F}_q$ es un cuerpo perfecto, $\mathbb{F}_{q^n}/\mathbb{F}_q$ es una extensión separable y por tanto de Galois. □

2.3. $\mathbb{F}_{q^n}$ como $\mathbb{F}_q$-espacio vectorial

Como mencionamos en la Sección 2.1, las extensiones de cuerpos son naturalmente espacios vectoriales. En esta sección, estudiaremos a $\mathbb{F}_{q^n}$ como un $\mathbb{F}_q$-espacio vectorial. Empezaremos introduciendo un aplicación de $\mathbb{F}_{q^n}$ a $\mathbb{F}_q$ que resultará ser una transformación lineal y será una herramienta para caracterizar las transformaciones lineales de $\mathbb{F}_{q^n}$ a $\mathbb{F}_q$. Para finalizar esta sección, presentaremos un par de resultados sobre las bases de estos espacios vectoriales.

Definición 2.3.1. Dados $\mathbb{F}_{q^n}/\mathbb{F}_q$ una extensión de cuerpos y $\alpha \in \mathbb{F}_{q^n}$, definimos la **traza** $\mathrm{Tr}_{\mathbb{F}_{q^n}/\mathbb{F}_q}(\alpha)$ de α sobre $\mathbb{F}_q$ como:

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

Sean $\alpha \in \mathbb{F}_{q^n}$, $m_\alpha = f(x)$ y $\partial m_\alpha = d$ divisor de n. Entonces, por el Teorema 2.2.7 las raíces de f en $\mathbb{F}_{q^n}$ son $\alpha, \alpha^q, \alpha^{q^2}, \ldots, \alpha^{q^{d-1}}$. Si consideramos $g(x) = f(x)^{\frac{n}{d}}$, tenemos que

$\alpha, \alpha^q, \alpha^{q^2}, \ldots, \alpha^{q^{n-1}}$ son las n raíces de g. De este modo, si escribimos a g en su expresión polinomial, se sigue que:

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

Comparando coeficientes en ambas expresiones, se concluye que $\mathrm{Tr}_{\mathbb{F}_{q^n}/\mathbb{F}_q}(\alpha) = -a_{n-1}$. Lo que muestra que $\mathrm{Tr}_{\mathbb{F}_{q^n}/\mathbb{F}_q}(\alpha) \in \mathbb{F}_q$. Algunas propiedades de la aplicación traza se resumen en la siguiente proposición.

Proposición 2.3.2. *Sea $\mathbb{F}_{q^n}/\mathbb{F}_q$ una extensión de cuerpos. Entonces la aplicación traza satisface las siguientes propiedades:*

I) $\mathrm{Tr}_{\mathbb{F}_{q^n}/\mathbb{F}_q}(\alpha+\beta) = \mathrm{Tr}_{\mathbb{F}_{q^n}/\mathbb{F}_q}(\alpha) + \mathrm{Tr}_{\mathbb{F}_{q^n}/\mathbb{F}_q}(\beta)$*, para todo* $\alpha, \beta \in \mathbb{F}_{q^n}$*.*

II) $\mathrm{Tr}_{\mathbb{F}_{q^n}/\mathbb{F}_q}(c\alpha) = c\,\mathrm{Tr}_{\mathbb{F}_{q^n}/\mathbb{F}_q}(\alpha)$*, para todo* $c \in \mathbb{F}_q, \alpha \in \mathbb{F}_{q^n}$*.*

III) $\mathrm{Tr}_{\mathbb{F}_{q^n}/\mathbb{F}_q}$ *es una transformación lineal sobreyectiva de* $\mathbb{F}_{q^n}$ *en* $\mathbb{F}_q$ *donde tanto como* $\mathbb{F}_{q^n}$ *como* $\mathbb{F}_q$ *son vistos como un* $\mathbb{F}_q$*-espacio vectorial.*

IV) $\mathrm{Tr}_{\mathbb{F}_{q^n}/\mathbb{F}_q}(a) = n \cdot a$*, para todo* $a \in \mathbb{F}_q$*.*

V) $\mathrm{Tr}_{\mathbb{F}_{q^n}/\mathbb{F}_q}(\alpha^q) = \mathrm{Tr}_{\mathbb{F}_{q^n}/\mathbb{F}_q}(\alpha)$*, para todo* $\alpha \in \mathbb{F}_{q^n}$*.*

Demostración. Probaremos cada una de las propiedades.

I) Sean $\alpha, \beta \in \mathbb{F}_{q^n}$, usando el Lema 2.1.3 obtenemos:

$$\begin{aligned}
\mathrm{Tr}_{\mathbb{F}_{q^n}/\mathbb{F}_q}(\alpha+\beta) &= (\alpha+\beta) + (\alpha+\beta)^q + (\alpha+\beta)^{q^2} + \cdots + (\alpha+\beta)^{q^{n-1}} \\
&= \alpha + \beta + \alpha^q + \beta^q + \alpha^{q^2} + \beta^{q^2} + \cdots + \alpha^{q^{n-1}} + \beta^{q^{n-1}} \\
&= \alpha + \alpha^q + \alpha^{q^2} + \cdots + \alpha^{q^{n-1}} + \beta + \beta^q + \beta^{q^2} + \cdots + \beta^{q^{n-1}} \\
&= \mathrm{Tr}_{\mathbb{F}_{q^n}/\mathbb{F}_q}(\alpha) + \mathrm{Tr}_{\mathbb{F}_{q^n}/\mathbb{F}_q}(\beta).
\end{aligned}$$

II) Sean $\alpha \in \mathbb{F}_{q^n}$ y $c \in \mathbb{F}_q$, usando el hecho de que los automorfismos σ_j con $0 \leq j \leq n-1$ fijan los elementos de $\mathbb{F}_q$, obtenemos:

$$\begin{aligned}
\mathrm{Tr}_{\mathbb{F}_{q^n}/\mathbb{F}_q}(c\alpha) &= (c\alpha) + (c\alpha)^q + (c\alpha)^{q^2} + \cdots + (c\alpha)^{q^{n-1}} \\
&= c\alpha + c^q\alpha^q + c^{q^2}\alpha^{q^2} + \cdots + c^{q^{n-1}}\alpha^{q^{n-1}} \\
&= c\alpha + c\alpha^q + c\alpha^{q^2} + \cdots + c\alpha^{q^{n-1}} \\
&= c\,\mathrm{Tr}_{\mathbb{F}_{q^n}/\mathbb{F}_q}(\alpha).
\end{aligned}$$

III) De los ítems anteriores y del hecho que $\mathrm{Tr}_{\mathbb{F}_{q^n}/\mathbb{F}_q}(\alpha) \in \mathbb{F}_q$ para todo $\alpha \in \mathbb{F}_{q^n}$, tenemos que $\mathrm{Tr}_{\mathbb{F}_{q^n}/\mathbb{F}_q}$ es una transformación lineal de $\mathbb{F}_{q^n}$ en $\mathbb{F}_q$. Ahora, sea $\alpha \in \mathbb{F}_q$, note que si existe $\beta \in \mathbb{F}_{q^n}$ tal que $\mathrm{Tr}_{\mathbb{F}_{q^n}/\mathbb{F}_q}(\beta) \neq 0$ entonces

$$\mathrm{Tr}_{\mathbb{F}_{q^n}/\mathbb{F}_q}\left(\alpha\left(\mathrm{Tr}_{\mathbb{F}_{q^n}/\mathbb{F}_q}(\beta)\right)^{-1}\beta\right) = \alpha\left(\mathrm{Tr}_{\mathbb{F}_{q^n}/\mathbb{F}_q}(\beta)\right)^{-1}\mathrm{Tr}_{\mathbb{F}_{q^n}/\mathbb{F}_q}(\beta) = \alpha.$$

Por lo que es suficiente probar que existe $\beta \in \mathbb{F}_{q^n}$ tal que $\mathrm{Tr}_{\mathbb{F}_{q^n}/\mathbb{F}_q}(\beta) \neq 0$ para mostrar que la aplicación es sobreyectiva. Supongamos por contradicción que para todo $\beta \in \mathbb{F}_{q^n}$ $\mathrm{Tr}_{\mathbb{F}_{q^n}/\mathbb{F}_q}(\beta) = 0$, entonces todo elemento de $\mathbb{F}_{q^n}$ es raíz del polinomio $x^{q^{n-1}} + \cdots + x^{q^2} + x^q + x$ pero esto es un absurdo puesto que dicho polinomio tiene a lo sumo q^{n-1} raíces en $\mathbb{F}_{q^n}$.

IV) Al igual que en el ítem II), esta propiedad es una consecuencia inmediata del hecho que los automorfismos σ_j con $0 \leq j \leq n-1$ fijan los elementos de $\mathbb{F}_q$.

V) Sea $\alpha \in \mathbb{F}_{q^n}$, entonces $\alpha^{q^n} = \alpha$ y así:

$$\begin{aligned}\mathrm{Tr}_{\mathbb{F}_{q^n}/\mathbb{F}_q}(\alpha^q) &= \alpha^q + \alpha^{q^2} + \alpha^{q^3} + \cdots + \alpha^{q^n} \\ &= \alpha^q + \alpha^{q^2} + \alpha^{q^3} + \cdots + \alpha \\ &= \mathrm{Tr}_{\mathbb{F}_{q^n}/\mathbb{F}_q}(\alpha).\end{aligned}$$

□

Teorema 2.3.3. *Sea $\mathbb{F}/\mathbb{K}$ una extensión finita de un cuerpo finito $\mathbb{K}$, ambos considerados como $\mathbb{K}$-espacios vectoriales. Entonces las transformaciones lineales de $\mathbb{F}$ en $\mathbb{K}$ son exactamente las aplicaciones L_β, $\beta \in \mathbb{F}$, donde $L_\beta(\alpha) = \mathrm{Tr}_{\mathbb{F}/\mathbb{K}}(\beta\alpha)$ para todo $\alpha \in \mathbb{F}$. Además, si β y γ son elementos distintos de $\mathbb{F}$ tenemos que $L_\beta \neq L_\gamma$.*

Demostración. Sea $\beta \in \mathbb{F}$. Veamos que L_β es una transformación lineal de $\mathbb{F}$ en $\mathbb{K}$. Sean $\alpha, \delta \in \mathbb{F}$ y $c \in \mathbb{K}$. Como $\mathrm{Tr}_{\mathbb{F}/\mathbb{K}}$ es una transformación lineal tenemos:

$$L_\beta(\alpha+\delta) = \mathrm{Tr}_{\mathbb{F}/\mathbb{K}}(\beta(\alpha+\delta)) = \mathrm{Tr}_{\mathbb{F}/\mathbb{K}}(\beta\alpha+\beta\delta) = \mathrm{Tr}_{\mathbb{F}/\mathbb{K}}(\beta\alpha) + \mathrm{Tr}_{\mathbb{F}/\mathbb{K}}(\beta\delta) = L_\beta(\alpha) + L_\beta(\delta)$$

$$L_\beta(c\alpha) = \mathrm{Tr}_{\mathbb{F}/\mathbb{K}}(\beta(c\alpha)) = \mathrm{Tr}_{\mathbb{F}/\mathbb{K}}(c(\beta\alpha)) = c\,\mathrm{Tr}_{\mathbb{F}/\mathbb{K}}(\beta\alpha) = cL_\beta(\alpha)$$

Luego, L_β es una transformación lineal. Ahora bien, sea $\gamma \in \mathbb{F}$ tal que $\beta \neq \gamma$. Como vimos en la demostración del ítem III) del teorema anterior, existe $\delta \in \mathbb{F}_{q^n}$ tal que $\mathrm{Tr}_{\mathbb{F}/\mathbb{K}}(\delta) \neq 0$. Si tomamos $\alpha = \delta(\beta-\gamma)^{-1}$, entonces $L_\beta(\alpha) - L_\gamma(\alpha) = \mathrm{Tr}_{\mathbb{F}/\mathbb{K}}((\beta-\gamma)\alpha) = \mathrm{Tr}_{\mathbb{F}/\mathbb{K}}(\delta) \neq 0$ y así,

$L_\beta \neq L_\gamma$. Finalmente, note que la cantidad de transformaciones diferentes de la forma L_β es la cardinalidad de $\mathbb{F}$ y además, toda transformación lineal de $\mathbb{F}$ en $\mathbb{K}$ se puede obtener asignando elementos arbitarios de $\mathbb{K}$ a los n elementos de una base fija de $\mathbb{F}$ como un $\mathbb{K}$-espacio vectorial. Como lo anterior se pueden hacer de $|\mathbb{F}|$ formas distintas, concluimos que efectivamente L_β con $\beta \in \mathbb{F}$ son todas las transformaciones lineales de $\mathbb{F}$ en $\mathbb{K}$. □

Teorema 2.3.4. *(Transitividad de la Traza). Sean $\mathbb{K}$ un cuerpo finito, $\mathbb{F}$ una extensión finita de $\mathbb{K}$ y $\mathbb{L}$ una extensión finita de $\mathbb{F}$. Entonces*

$$\mathrm{Tr}_{\mathbb{L}/\mathbb{K}}(\alpha) = \mathrm{Tr}_{\mathbb{F}/\mathbb{K}}(\mathrm{Tr}_{\mathbb{L}/\mathbb{F}}(\alpha)) \text{ para todo } \alpha \in \mathbb{L}.$$

Demostración. Supongamos que $\mathbb{K}$ tiene q elementos , $[\mathbb{F} : \mathbb{K}] = n$ y $[\mathbb{L} : \mathbb{F}] = m$, entonces para todo $\alpha \in \mathbb{L}$ tenemos:

$$\begin{aligned}
\mathrm{Tr}_{\mathbb{F}/\mathbb{K}}(\mathrm{Tr}_{\mathbb{L}/\mathbb{F}}(\alpha)) &= \sum_{i=0}^{n-1} \mathrm{Tr}_{\mathbb{L}/\mathbb{F}}(\alpha)^{q^i} \\
&= \sum_{i=0}^{n-1} \left(\sum_{j=0}^{m-1} \alpha^{q^{nj}} \right)^{q^i} \\
&= \sum_{i=0}^{n-1} \sum_{j=0}^{m-1} \alpha^{q^{nj+i}} \\
&= \sum_{k=0}^{mn-1} \alpha^{q^k} \\
&= \mathrm{Tr}_{\mathbb{L}/\mathbb{K}}(\alpha).
\end{aligned}$$

□

Teorema 2.3.5. *Sea $\mathbb{F}_{q^n}/\mathbb{F}_q$ una extensión de cuerpos. Entonces para $\alpha \in \mathbb{F}_{q^n}$ tenemos que $\mathrm{Tr}_{\mathbb{F}_{q^n}/\mathbb{F}_q}(\alpha) = 0$ si, y solo si, $\alpha = \beta^q - \beta$ para algún $\beta \in \mathbb{F}_{q^n}$.*

Demostración. Supongamos que $\mathrm{Tr}_{\mathbb{F}_{q^n}/\mathbb{F}_q}(\alpha) = 0$ y sea β una raíz del polinomio $x^q - x - \alpha$

en alguna extensión de $\mathbb{F}_{q^n}$, entonces

$$\begin{aligned}
0 &= \mathrm{Tr}_{\mathbb{F}_{q^n}/\mathbb{F}_q}(\alpha) \\
&= \alpha + \alpha^q + \cdots + \alpha^{q^{n-1}} \\
&= (\beta^q - \beta) + (\beta^q - \beta)^q + \cdots + (\beta^q - \beta)^{q^{n-1}} \\
&= (\beta^q - \beta) + (\beta^{q^2} - \beta^q) + \cdots + (\beta^{q^n} - \beta^{q^{n-1}}) \\
&= \beta^{q^n} - \beta,
\end{aligned}$$

por lo que $\beta \in \mathbb{F}_{q^n}$. Recíprocamente, si $\alpha = \beta^q - \beta$ para algún $\beta \in \mathbb{F}_{q^n}$, entonces por las propiedades I) y V) de la Proposición 2.3.2 tenemos que

$$\mathrm{Tr}_{\mathbb{F}_{q^n}/\mathbb{F}_q}(\alpha) = \mathrm{Tr}_{\mathbb{F}_{q^n}/\mathbb{F}_q}(\beta^q - \beta) = \mathrm{Tr}_{\mathbb{F}_{q^n}/\mathbb{F}_q}(\beta^q) - \mathrm{Tr}_{\mathbb{F}_{q^n}/\mathbb{F}_q}(\beta) = \mathrm{Tr}_{\mathbb{F}_{q^n}/\mathbb{F}_q}(\beta) - \mathrm{Tr}_{\mathbb{F}_{q^n}/\mathbb{F}_q}(\beta) = 0.$$

□

Presentamos otra interesante función de un cuerpo finito en un subcuerpo donde la imagen de un elemento del cuerpo es el producto de sus conjugados respecto al subcuerpo.

Definición 2.3.6. Dados $\mathbb{F}_{q^n}/\mathbb{F}_q$ una extensión de cuerpos y $\alpha \in \mathbb{F}_{q^n}$, definimos la **norma** $\mathrm{Norm}_{\mathbb{F}_{q^n}/\mathbb{F}_q}(\alpha)$ de α sobre $\mathbb{F}_q$ como:

$$\mathrm{Norm}_{\mathbb{F}_{q^n}/\mathbb{F}_q}(\alpha) = \alpha \cdot \alpha^q \cdot \alpha^{q^2} \cdot \cdots \cdot \alpha^{q^{n-1}} = \alpha^{\frac{q^n-1}{q-1}}$$

Comparando el coeficiente independiente de ambas expresiones en la ecuación (2.3), tenemos que $\mathrm{Norm}_{\mathbb{F}_{q^n}/\mathbb{F}_q}(\alpha) = (-1)^n a_0$. Luego, $\mathrm{Norm}_{\mathbb{F}_{q^n}/\mathbb{F}_q}(\alpha) \in \mathbb{F}_q$. Algunas propiedades de la aplicación norma se resumen en la siguiente proposición.

Proposición 2.3.7. *Sea $\mathbb{F}_{q^n}/\mathbb{F}_q$ una extensión de cuerpos. Entonces la aplicación norma satisface las siguientes propiedades:*

I) $\mathrm{Norm}_{\mathbb{F}_{q^n}/\mathbb{F}_q}(\alpha\beta) = \mathrm{Norm}_{\mathbb{F}_{q^n}/\mathbb{F}_q}(\alpha)\,\mathrm{Norm}_{\mathbb{F}_{q^n}/\mathbb{F}_q}(\beta)$, *para todo* $\alpha, \beta \in \mathbb{F}_{q^n}$.

II) $\mathrm{Norm}_{\mathbb{F}_{q^n}/\mathbb{F}_q}$ *es una función sobreyectiva de* $\mathbb{F}_{q^n}$ *en* $\mathbb{F}_q$ *y* $\mathbb{F}_q^*$ *es la imagen de* $\mathbb{F}_{q^n}^*$ *bajo esta función.*

III) $\mathrm{Norm}_{\mathbb{F}_{q^n}/\mathbb{F}_q}(a) = a^n$, *para todo* $a \in \mathbb{F}_q$.

IV) $\mathrm{Norm}_{\mathbb{F}_{q^n}/\mathbb{F}_q}(\alpha^q) = \mathrm{Norm}_{\mathbb{F}_{q^n}/\mathbb{F}_q}(\alpha)$, *para todo* $\alpha \in \mathbb{F}_{q^n}$.

Demostración. Probaremos cada una de las propiedades.

I) Es inmediato de la definición de norma.

II) Ya mostramos que $\mathrm{Norm}_{\mathbb{F}_{q^n}/\mathbb{F}_q}$ es una función de $\mathbb{F}_{q^n}$ en $\mathbb{F}_q$. Note que $\mathrm{Norm}_{\mathbb{F}_{q^n}/\mathbb{F}_q}(\alpha) = 0$ si, y solo si, $\alpha = 0$, por lo que $\mathrm{Norm}_{\mathbb{F}_{q^n}/\mathbb{F}_q}(\mathbb{F}_{q^n}^*) \subseteq \mathbb{F}_q^*$. El ítem anterior muestra que esta aplicación es un homomorfismo de grupos entre $\mathbb{F}_{q^n}^*$ y $\mathbb{F}_q^*$ y su kernel son todas las raíces del polinomio $x^{\frac{q^n-1}{q-1}} - 1$ en $\mathbb{F}_{q^n}$, así $d = |\mathrm{Ker}(\mathrm{Norm}_{\mathbb{F}_{q^n}/\mathbb{F}_q})| \leq \frac{q^n-1}{q-1}$. Ahora, por el primer teorema de isomorfismo para grupos tenemos que

$$\frac{\mathbb{F}_{q^n}^*}{\mathrm{Ker}(\mathrm{Norm}_{\mathbb{F}_{q^n}/\mathbb{F}_q})} \cong \mathrm{Norm}_{\mathbb{F}_{q^n}/\mathbb{F}_q}(\mathbb{F}_{q^n}^*)$$

y así por el Teorema de Lagrange tenemos $|\mathrm{Norm}_{\mathbb{F}_{q^n}/\mathbb{F}_q}(\mathbb{F}_{q^n}^*)| = \frac{q^n-1}{d}$. Luego, $\frac{q^n-1}{d} \geq q-1$ y por lo tanto $\mathrm{Norm}_{\mathbb{F}_{q^n}/\mathbb{F}_q}(\mathbb{F}_{q^n}^*) = \mathbb{F}_q^*$ que implica que $\mathrm{Norm}_{\mathbb{F}_{q^n}/\mathbb{F}_q}$ sea una función sobreyectiva.

III) Sea $a \in \mathbb{F}_q$, usando el hecho de que los automorfismos σ_j con $0 \leq j \leq n-1$ fijan los elementos de $\mathbb{F}_q$, obtenemos:

$$\mathrm{Norm}_{\mathbb{F}_{q^n}/\mathbb{F}_q}(a) = a \cdot a^q \cdot a^{q^2} \cdots a^{q^{n-1}} = \underbrace{a \cdot a \cdots a}_{n \text{ veces}} = a^n.$$

IV) Sea $\alpha \in \mathbb{F}_{q^n}$. Por el ítem I) y por el hecho de que $\beta^q = \beta$ para $\beta \in \mathbb{F}_q$ tenemos:

$$\mathrm{Norm}_{\mathbb{F}_{q^n}/\mathbb{F}_q}(\alpha^q) = \mathrm{Norm}_{\mathbb{F}_{q^n}/\mathbb{F}_q}(\alpha)^q = \mathrm{Norm}_{\mathbb{F}_{q^n}/\mathbb{F}_q}(\alpha).$$

□

Teorema 2.3.8. *(Transitividad de la Norma). Sean $\mathbb{K}$ un cuerpo finito, $\mathbb{F}$ una extensión finita de $\mathbb{K}$ y $\mathbb{L}$ una extensión finita de $\mathbb{F}$. Entonces*

$$\mathrm{Norm}_{\mathbb{L}/\mathbb{K}}(\alpha) = \mathrm{Norm}_{\mathbb{F}/\mathbb{K}}(\mathrm{Norm}_{\mathbb{L}/\mathbb{F}}(\alpha)), \ \textit{para todo } \alpha \in \mathbb{L}.$$

Demostración. Supongamos que $\mathbb{K}$ tiene q elementos , $[\mathbb{F} : \mathbb{K}] = n$ y $[\mathbb{L} : \mathbb{F}] = m$, entonces

para todo $\alpha \in \mathbb{L}$ tenemos:

$$\begin{aligned}\mathrm{Norm}_{\mathbb{F}/\mathbb{K}}(\mathrm{Norm}_{\mathbb{L}/\mathbb{F}}(\alpha)) &= \mathrm{Norm}_{\mathbb{F}/\mathbb{K}}(\alpha^{\frac{q^{nm}-1}{q^n-1}}) \\ &= \left(\alpha^{\frac{q^{nm}-1}{q-1}}\right)^{\frac{q^n-1}{q-1}} \\ &= \alpha^{\frac{q^{nm}-1}{q^n-1}\frac{q^n-1}{q-1}} \\ &= \alpha^{\frac{q^{nm}-1}{q-1}} \\ &= \mathrm{Norm}_{\mathbb{L}/\mathbb{K}}(\alpha).\end{aligned}$$

□

Ahora mostraremos el resultado correspondiente al Teorema 2.3.5 para la norma.

Teorema 2.3.9. *Sea $\mathbb{F}_{q^n}/\mathbb{F}_q$ una extensión de cuerpos. Entonces para $\alpha \in \mathbb{F}_{q^n}$ tenemos que $\mathrm{Norm}_{\mathbb{F}_{q^n}/\mathbb{F}_q}(\alpha) = 1$ si, y solo si, $\alpha = \beta^{q-1}$ para algún $\beta \in \mathbb{F}_{q^n}$.*

Demostración. Supongamos que $\mathrm{Norm}_{\mathbb{F}_{q^n}/\mathbb{F}_q}(\alpha) = 1$ y sea β una raíz del polinomio $x^{q-1} - \alpha$ en alguna extensión de $\mathbb{F}_{q^n}$, entonces

$$\begin{aligned}1 &= \mathrm{Norm}_{\mathbb{F}_{q^n}/\mathbb{F}_q}(\alpha) \\ &= \alpha^{\frac{q^n-1}{q-1}} \\ &= \left(\beta^{q-1}\right)^{\frac{q^n-1}{q-1}} \\ &= \beta^{q^n-1}.\end{aligned}$$

Lo que implica que $\beta^{q^n} = \beta$ y por lo tanto $\beta \in \mathbb{F}_{q^n}$. Recíprocamente, si $\alpha = \beta^{q-1}$ para algún $\beta \in \mathbb{F}_{q^n}$, entonces $\mathrm{Norm}_{\mathbb{F}_{q^n}/\mathbb{F}_q}(\alpha) = (\beta^{q-1})^{\frac{q^n-1}{q-1}} = \beta^{q^n-1} = 1$. □

Definición 2.3.10. Sean $\mathbb{F}_{q^n}/\mathbb{F}_q$ una extensión de cuerpos y $\alpha \in \mathbb{F}_{q^n}$. Entonces una base de $\mathbb{F}_{q^n}$ sobre $\mathbb{F}_q$ de la forma $\left\{\alpha, \alpha^q, \ldots, \alpha^{q^{n-1}}\right\}$ que consiste de un elemento $\alpha \in \mathbb{F}_{q^n}$ y sus conjugados respecto a $\mathbb{F}_q$ es llamada una **base normal** de $\mathbb{F}_{q^n}$ sobre $\mathbb{F}_q$.

Ejemplo 2.3.11. Sea $\alpha \in \mathbb{F}_8$ una raíz del polinomio irreducible $x^3 + x^2 + 1$ sobre $\mathbb{F}_2$. Entonces la base $\{\alpha, \alpha^2, \alpha^2 + \alpha + 1\}$ es una base normal de $\mathbb{F}_8$ sobre $\mathbb{F}_2$ ya que $\alpha^4 = \alpha\alpha^3 = \alpha(\alpha^2 + 1) = \alpha^3 + \alpha = \alpha^2 + \alpha + 1$.

Procederemos a mostrar la existencia de una base normal para toda extensión $\mathbb{F}_{q^n}/\mathbb{F}_q$. Para esto, empezaremos mostrando un lema acerca de homomorfismos de un grupo arbitrario en el grupo multiplicativo $\mathbb{F}^*$ de un cuerpo $\mathbb{F}$.

Lema 2.3.12. *(Lema de Artin). Sean $\psi_1, \ldots, \psi_n$ distintos homomorfimos de un grupo G a el grupo multiplicativo $\mathbb{F}^*$ de un cuerpo arbitrario $\mathbb{F}$ y sean $a_1, \ldots a_n$ elementos de $\mathbb{F}$ no todos nulos. Entonces para algún $g \in G$ tenemos:*

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

Demostración. Haremos esta prueba por inducción en n. Para el caso base, $n = 1$, tenemos que $a_1 \neq 0$ y por tanto cualquier $g \in G$ cumple que $a_1\psi_1(g) \neq 0$. Ahora, supongamos que el resultado es verdadero para cualesquiera $k-1$ homomorfismos distintos y $k-1$ elementos no todos nulos de $\mathbb{F}$. Sean $\psi_1, \ldots, \psi_k$ homomorfismos distintos y $a_1, \ldots, a_k \in \mathbb{F}$ no todos nulos. Si $a_i = 0$ para algún i, entonces el resultado es inmediato de la hipotesis inductiva. En caso contrario, supongamos que para todo $g \in G$ se tiene:

$$a_1\psi_1(g) + \cdots + a_k\psi_k(g) = 0. \tag{2.2}$$

Como ψ_1 y ψ_k son homomorfismos distintos existe $h \in G$ tal que $\psi_1(h) \neq \psi_k(h)$. Sustituyendo g por hg en la ecuación (2.2) obtenemos:

$$a_1\psi_1(h)\psi_1(g) + \cdots + a_k\psi_k(h)\psi_k(g) = 0, \text{ para todo } g \in G.$$

Multiplicando la ecuación anterior por $\psi_k(h)^{-1}$

$$a_1\psi_1(h)\psi_k(h)^{-1}\psi_1(g) + \cdots + a_k\psi_k(h)\psi_k(h)^{-1}\psi_k(g) = 0, \text{ para todo } g \in G. \tag{2.3}$$

Restando las ecuaciones 2.2 y 2.3, tenemos:

$$\left(a_1 - a_1\psi_1(h)\psi_k(h)^{-1}\right)\psi_1(g) + \cdots + \left(a_{k-1} - a_{k-1}\psi_{k-1}(h)\psi_k(h)^{-1}\right)\psi_{k-1}(g) = 0, \text{ para todo} g \in G.$$

Como $a_1 - a_1\psi_1(h)\psi_k(h)^{-1} \neq 0$, la ecuación anterior contradice el resultado de aplicar la hipotesis inductiva a ψ_i y $a_i - a_i\psi_i(h)\psi_k(h)^{-1}$ con $i \in \{1, 2, \ldots, k-1\}$. □

Para la demostración del teorema de la base normal necesitamos algunas nociones y resultados del álgebra lineal sobre operadores lineales que se encuentra en el Apéndice A. En este apéndice mostraremos que un operador lineal T en un espacio de dimensión finita tiene un vector cíclico si, y solo si, el polinomio característico y minimal de T son iguales.

Teorema 2.3.13. *(Teorema de la Base Normal). Para cualquier cuerpo finito $\mathbb{F}_q$ y cualquier extensión finita $\mathbb{F}_{q^n}$ de $\mathbb{F}_q$, existe una base normal de $\mathbb{F}_{q^n}$ sobre $\mathbb{F}_q$.*

Demostración. En el Teorema 2.2.17 mostramos que $\mathrm{Gal}(\mathbb{F}_{q^n}/\mathbb{F}_q)$ es cíclico de orden n generado por $\sigma(\alpha) = \alpha^q$ con $\alpha \in \mathbb{F}_{q^n}$. Note que los automorfismos de Galois $\sigma, \sigma^1, \ldots, \sigma^n$ también pueden ser vistos como operadores lineales en el espacio vectorial $\mathbb{F}_{q^n}$ sobre $\mathbb{F}_q$ puesto que:

$$\sigma^j(\alpha + \beta) = \sigma^j(\alpha) + \sigma^j(\beta)$$

$$\sigma^j(c\alpha) = \sigma^j(c)\sigma^j(\alpha) = c\sigma^j(\alpha),$$

para todo $1 \leq j \leq n, \alpha, \beta \in \mathbb{F}_{q^n}$ y $c \in \mathbb{F}_q$. Como $\sigma^n = \mathrm{I}$ tenemos que el polinomio $x^n - 1 \in \mathbb{F}_q[x]$ anula al operador σ. Por otro lado, si consideramos las restricciones de los automorfismos σ^i a $\mathbb{F}_{q^n}^*$, por el Lema 2.3.12 tenemos que ningún polinomio en $\mathbb{F}_q[x]$ de grado menor que n anula a σ. Por lo tanto, $x^n - 1$ es el polinomio minimal de σ. Así, tanto el polinomio caracterísitico como el minimal tiene el mismo grado y como mencionamos en la Observación A.0.8 esto implica que sean iguales. Finalmente, por el Teorema A.0.13 tenemos que existe $\alpha \in \mathbb{F}_{q^n}$ tal que $\mathbb{F}_{q^n} = Z(\alpha, \sigma)$. Del ítem II) del Teorema A.0.7 concluimos que $x^n - 1$ es el σ-anulador de α y por ítem I) de este mismo teorema tenemos que

$$\left\{\alpha, \sigma(\alpha), \sigma^2(\alpha), \ldots, \sigma^{n-1}(\alpha)\right\} = \left\{\alpha, \alpha^q, \ldots, \alpha^{q^{n-1}}\right\}$$

es una base para $\mathbb{F}_{q^n}$ como $\mathbb{F}_q$-espacio vectorial. □

Finalizamos esta sección con un criterio que nos permite determinar si un conjunto de n elementos de $\mathbb{F}_{q^n}$ es una base para $\mathbb{F}_{q^n}$ como $\mathbb{F}_q$-espacio vectorial.

Definición 2.3.14. Sea $\mathbb{F}_{q^n}/\mathbb{F}_q$ una extensión de cuerpos. Entonces el **discriminante** $\Delta_{\mathbb{F}_{q^n}/\mathbb{F}_q}\{\alpha_1, \alpha_2, \ldots, \alpha_n\}$ de los elementos $\alpha_1, \alpha_2, \ldots, \alpha_n \in \mathbb{F}_{q^n}$ está dado por el determinante de la siguiente matriz de orden n

$$\Delta_{\mathbb{F}_{q^n}/\mathbb{F}_q}(\alpha_1, \cdots, \alpha_n) = \begin{vmatrix} \mathrm{Tr}_{\mathbb{F}_{q^n}/\mathbb{F}_q}(\alpha_1\alpha_1) & \mathrm{Tr}_{\mathbb{F}_{q^n}/\mathbb{F}_q}(\alpha_1\alpha_2) & \ldots & \mathrm{Tr}_{\mathbb{F}_{q^n}/\mathbb{F}_q}(\alpha_1\alpha_n) \\ \mathrm{Tr}_{\mathbb{F}_{q^n}/\mathbb{F}_q}(\alpha_2\alpha_1) & \mathrm{Tr}_{\mathbb{F}_{q^n}/\mathbb{F}_q}(\alpha_2\alpha_2) & \ldots & \mathrm{Tr}_{\mathbb{F}_{q^n}/\mathbb{F}_q}(\alpha_2\alpha_n) \\ \vdots & \vdots & & \vdots \\ \mathrm{Tr}_{\mathbb{F}_{q^n}/\mathbb{F}_q}(\alpha_n\alpha_1) & \mathrm{Tr}_{\mathbb{F}_{q^n}/\mathbb{F}_q}(\alpha_n\alpha_2) & \ldots & \mathrm{Tr}_{\mathbb{F}_{q^n}/\mathbb{F}_q}(\alpha_n\alpha_n) \end{vmatrix} \tag{2.4}$$

Como $\mathrm{Tr}_{\mathbb{F}_{q^n}/\mathbb{F}_q}(\alpha) \in \mathbb{F}_q$, para todo $\alpha \in \mathbb{F}_{q^n}$ se sigue de la definición anterior que $\Delta_{\mathbb{F}_{q^n}/\mathbb{F}_q}\{\alpha_1, \alpha_2, \ldots, \alpha_n\} \in \mathbb{F}_q$.

Teorema 2.3.15. *Sean $\mathbb{F}_{q^n}/\mathbb{F}_q$ una extensión de cuerpos y $\alpha_1, \alpha_2, \ldots, \alpha_n \in \mathbb{F}$. Entonces $\{\alpha_1, \alpha_2, \ldots, \alpha_n\}$ es una base de $\mathbb{F}_{q^n}$ sobre $\mathbb{F}_q$ si, y solo si, $\Delta_{\mathbb{F}_{q^n}/\mathbb{F}_q}\{\alpha_1, \alpha_2, \ldots, \alpha_n\} \neq 0$.*

Demostración. Supongamos que $\{\alpha_1, \alpha_2, \ldots, \alpha_n\}$ es una base de $\mathbb{F}_{q^n}$ como $\mathbb{F}_q$-espacio vectorial, queremos ver que $\Delta_{\mathbb{F}_{q^n}/\mathbb{F}_q}\{\alpha_1, \alpha_2, \ldots, \alpha_n\} \neq 0$. Recordemos que los vectores $v_1, v_2, \ldots, v_n \in \mathbb{F}_q^n$ son linealmente independientes sobre $\mathbb{F}_q$ si, y solo si, el determinante de la matriz de orden n cuya i-esima fila es el vector v_i, es no nulo. Así, basta ver que los vectores fila de la matriz (2.4) son linealmente independientes.

Denotemos por $v_i = \left(\mathrm{Tr}_{\mathbb{F}_{q^n}/\mathbb{F}_q}(\alpha_i\alpha_1), \mathrm{Tr}_{\mathbb{F}_{q^n}/\mathbb{F}_q}(\alpha_i\alpha_2), \ldots, \mathrm{Tr}_{\mathbb{F}_{q^n}/\mathbb{F}_q}(\alpha_i\alpha_n)\right)$ con $1 \leq i \leq n$ y sean $c_1, c_2, \ldots, c_n \in \mathbb{F}_q$ tales que $c_1v_1 + c_2v_2 + \cdots + c_nv_n = 0$. Considerando $\beta = c_1\alpha_1 + c_2\alpha_2 + \cdots + c_n\alpha_n$, entonces para todo $1 \leq i \leq n$, tenemos que:

$$\begin{aligned}\mathrm{Tr}_{\mathbb{F}_{q^n}/\mathbb{F}_q}(\beta\alpha_i) &= \mathrm{Tr}_{\mathbb{F}_{q^n}/\mathbb{F}_q}(c_1\alpha_1\alpha_i + c_2\alpha_2\alpha_i + \cdots + c_n\alpha_n\alpha_i)\\ &= c_1\,\mathrm{Tr}_{\mathbb{F}_{q^n}/\mathbb{F}_q}(\alpha_1\alpha_i) + c_2\,\mathrm{Tr}_{\mathbb{F}_{q^n}/\mathbb{F}_q}(\alpha_2\alpha_i) + \cdots + c_n\,\mathrm{Tr}_{\mathbb{F}_{q^n}/\mathbb{F}_q}(\alpha_n\alpha_i)\\ &= 0.\end{aligned}$$

puesto que es la coordenada i-esima del vector $c_1v_1 + c_2v_2 + \cdots + c_nv_n$. Ahora bien, si α es un elemento arbitrario de $\mathbb{F}_{q^n}$ entonces α es una combinación lineal de los α_i y por lo anterior se sigue que $\mathrm{Tr}_{\mathbb{F}_{q^n}/\mathbb{F}_q}(\beta\alpha) = 0$, para todo $\alpha \in \mathbb{F}_{q^n}$. Note que si $\beta \neq 0$ y $\gamma \in \mathbb{F}_{q^n}$, entonces tomando $\alpha = \beta^{-1}\gamma$ tenemos que $\mathrm{Tr}_{\mathbb{F}_{q^n}/\mathbb{F}_q}(\beta\alpha) = \mathrm{Tr}_{\mathbb{F}_{q^n}/\mathbb{F}_q}(\gamma) = 0$, para todo $\gamma \in \mathbb{F}_{q^n}$, lo que es un absurdo. Luego, $\beta = c_1\alpha_1 + c_2\alpha_2 + \cdots + c_n\alpha_n = 0$ y por la independencia lineal de los α_i tenemos que $c_1 = c_2 = \cdots = c_n = 0$.

Recíprocamente, supongamos que $\Delta_{\mathbb{F}_{q^n}/\mathbb{F}_q}\{\alpha_1, \alpha_2, \ldots, \alpha_n\} \neq 0$, basta ver que $\{\alpha_1, \alpha_2, \ldots, \alpha_n\}$ son linealmente independientes. Para esto, sean $c_1, c_2, \ldots, c_n \in \mathbb{F}_q$ tales que $c_1\alpha_1 + c_2\alpha_2 + \cdots + c_n\alpha_n = 0$. Sea $i \in \{1, \ldots, n\}$, entonces $c_1\alpha_1\alpha_i + c_2\alpha_2\alpha_i + \cdots + c_n\alpha_n\alpha_i = 0$. Lo que implica que:

$$c_1\,\mathrm{Tr}_{\mathbb{F}_{q^n}/\mathbb{F}_q}(\alpha_1\alpha_i) + c_2\,\mathrm{Tr}_{\mathbb{F}_{q^n}/\mathbb{F}_q}(\alpha_2\alpha_i) + \cdots + c_n\,\mathrm{Tr}_{\mathbb{F}_{q^n}/\mathbb{F}_q}(\alpha_n\alpha_i) = 0.$$

Por lo tanto, $c_1v_1 + c_2v_2 + \cdots + c_nv_n = 0$ y como estos vectores son linealmente independientes, concluimos que $c_1 = c_2 = \cdots = c_n = 0$. □

Corolario 2.3.16. *Sean $\alpha_1, \alpha_2, \ldots, \alpha_n \in \mathbb{F}_{q^n}$. Entonces $\{\alpha_1, \alpha_2, \ldots, \alpha_n\}$ es una base de*

$\mathbb{F}_{q^n}$ *como* $\mathbb{F}_q$*-espacio vectorial si, y solo si,* $det(A) \neq 0$ *donde*

$$A = \begin{pmatrix} \alpha_1 & \alpha_2 & \dots & \alpha_n \\ \alpha_1^q & \alpha_2^q & \dots & \alpha_n^q \\ \vdots & \vdots & & \vdots \\ \alpha_1^{q^{n-1}} & \alpha_2^{q^{n-1}} & \dots & \alpha_n^{q^{n-1}} \end{pmatrix}$$

Demostración. Sea $B = A^T A = (b_{ij})$ donde A^T es la matriz transpuesta de A y llamemos $A = (a_{ij})$ y $A^T = (a'_{ij})$, entonces para $i, j \in \{1, \dots, n\}$ tenemos que:

$$b_{ij} = \sum_{k=1}^{n} a'_{ik} a_{kj} = \sum_{k=1}^{n} \alpha_i^{q^{k-1}} \alpha_j^{q^{k-1}} = \sum_{k=1}^{n} (\alpha_i \alpha_j)^{q^{k-1}} = \mathrm{Tr}_{\mathbb{F}/\mathbb{K}}(\alpha_i \alpha_j).$$

Por lo tanto, B es la matriz de ecuación (2.4), lo que implica que $\Delta_{\mathbb{F}/\mathbb{K}}(\alpha_1, \cdots, \alpha_n) = det(A)^2$. De esta forma, el resultado se sigue del Teorema 2.3.15. □

3. Álgebras de grupo y teoría de códigos

En este último capítulo presentaremos una aplicación de los cuerpos finitos a la teoría de códigos donde estudiaremos los códigos cíclicos, los cuales poseen propiedades algebraicas que son útiles para la codificación y decodificación. En una primera instancia mencionaremos los elementos básicos de un código y la relación entre los códigos cíclicos de longitud n sobre $\mathbb{F}_q$ y los ideales del anillo cociente $\mathbb{F}_q[x]/\langle x^n - 1\rangle$, tomando como referencia el libro [8] y el artículo [9]. Posteriormente, relacionaremos los códigos cíclicos con álgebras de grupo y finalmente mostraremos como generar los códigos cíclicos minimales de longitud n sobre $\mathbb{F}_q$ en ciertos casos particulares.

3.1. Hechos básicos de la teoría de códigos

En las últimas décadas, la teoría de códigos ha sido un objeto de estudio de gran interés pues es una pieza clave en la comunicación de la información. Desde los inicios de la computación, se han diseñado métodos que permitan identificar y corregir errores que se produzcan en la transmisión de la información.

Por ejemplo, si se desea transmitir una "palabra" que consiste en una cadena de 8 dígitos, los cuales pueden ser ceros o unos, entonces un dígito extra es añadido al final de cada palabra, llamado el dígito de control de paridad. Dicho dígito es 0 si la cantidad de unos en la palabra es par y 1 si la cantidad es impar. De esta forma, cada palabra enviada tiene 9 dígitos y una cantidad par de unos. Una vez recibida la palabra, se verifica la cantidad de unos y si esta es impar se identificará que hubo un error y se detendrá el proceso. Sin embargo, si dos errores se cometieron no podrán ser detectados e incluso si un error se detecta, no es posible determinar donde se encuentra el error.

Este método fue usado por Richard Hamming en 1947 y posteriormente se desarrollaron métodos en los que se añaden al final de cada palabra no solo un dígito de control de paridad sino más dígitos llamados dígitos redundantes los cuales permiten detectar

---

[8] Chaoping LING San y XING. *Coding Theory: A First Course*. Cambridge University Press, 2004.

[9] Cesar POLCINO. "Group algebras and coding theory: a short survey". En: *Revista de Integración, Escuela de Matemáticas, Universidad Industrial de Santander* 37.1 (2019), págs. 153-166.

e incluso corregir errores. En la Figura 3.1 se muestra un modelo simple de comunicación.

En esencia, un código es un lenguaje usado para comunicarse con una máquina

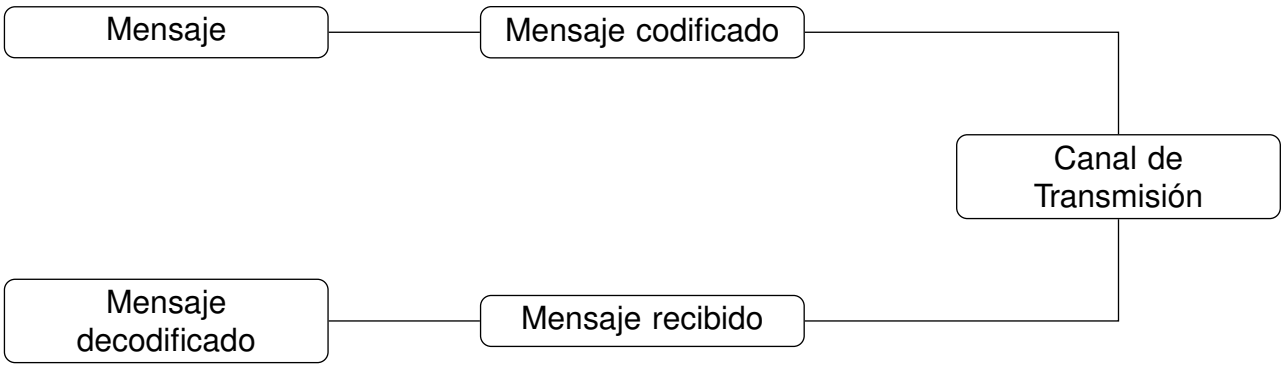

Figura 3.1: Esquema de comunicación.

o entre máquinas. Presentamos a continuación los elementos básicos de un código:

Un conjunto finito $\mathcal{A}$ de q elementos es llamado el **alfabeto del código** y sus elementos son llamados **letras o símbolos del código**. **Las palabras** son sucesiones finitas de elementos de $\mathcal{A}$ y el número de letras en una palabra es llamada su **longitud**. En este trabajo, todas las palabras en los códigos tienen la misma longitud.

Un código q-ario de longitud n es un conjunto de palabras de longitud n sobre $\mathcal{A}$, esto es, un subconjunto de $\mathcal{A}^n$.

Definición 3.1.1. Sean $x = (x_1, \ldots, x_n)$ y $y = (y_1, \ldots, y_n)$ dos palabras en un código $\mathcal{C} \subset \mathcal{A}^n$, entonces la **distancia de Hamming** entre x y y es:

$$d(x, y) = |\{i \in \{1, \ldots, n\} \mid x_i \neq y_i\}|$$

Dado un código $\mathcal{C} \subset \mathcal{A}^n$, definimos la **distancia mínima** de $\mathcal{C}$ como

$$d = min\,\{d(x, y) \mid x, y \in \mathcal{C}, x \neq y\}$$

Un código q-ario de longitud n que contiene M palabras y su distancia mínima es d es llamado un (n, M, d)-código. En este trabajo tomaremos el alfabeto como un cuerpo finito de q elementos, donde q es la potencia de un número primo.

Ejemplo 3.1.2. Un código sobre $\mathbb{F}_2 = \{0, 1\}$ es llamado un código binario. Algunos ejemplos de códigos binarios son:

I) $C_1 = \{(0,0), (0,1), (1,1), (1,0)\}$ es un $(2, 4, 1)$-código.

II) $C_2 = \{(0,0,0), (0,1,1), (1,0,1), (1,1,0), (1,1,1), (0,0,1)\}$ es un $(3, 6, 1)$-código.

Un tipo importante de códigos son los códigos lineales que presentaremos a continuación.

Definición 3.1.3. Un **código lineal** $\mathcal{C}$ de longitud n sobre $\mathbb{F}_q$ es un subespacio de $\mathbb{F}_q^n$.

Ejemplo 3.1.4. Los siguientes son ejemplos de códigos lineales:

I) $\mathcal{C} = \{(\lambda, \lambda, \ldots, \lambda) \mid \lambda \in \mathbb{F}_q\}$. Este código es llamado el **código de repetición**.

II) $\mathcal{C} = \{(0,0,0), (0,0,1), (0,1,0), (0,1,1)\}$ es un código lineal de longitud 3 sobre $\mathbb{F}_2$.

III) $\mathcal{C} = \{(0,0,0,0), (1,1,0,0), (2,2,0,0)\}$ es un código lineal de longitud 4 sobre $\mathbb{F}_3$.

Note que si $\mathcal{C}$ es un código lineal de longitud n sobre $\mathbb{F}_q$ cuya dimensión es $m \leq n$, entonces el número de palabras en $\mathcal{C}$ es q^m. Así que de ahora en adelante, nos referimos a este código como un (n, m, d)-código.

Es importante resaltar que como los códigos lineales son espacios vectoriales entonces poseen una estructura algebraica muy amplia que permite describirlos con facilidad. Veamos ahora una clase de códigos lineales que será de nuestro interés.

Definición 3.1.5. Dada una palabra $(x_1, x_2, \ldots, x_{n-1}, x_n) \in \mathbb{F}_q^n$, su **giro a la derecha** es la palabra $(x_n, x_1, \ldots, x_{n-1})$. Un código lineal $\mathcal{C}$ es **cíclico** si para cada palabra en el código su giro a la derecha también está en el código.

Note que esto implica que si una palabra $(x_1, x_2, \ldots, x_{n-1}, x_n)$ está en un código cíclico $\mathcal{C}$, entonces todas las permutaciones circulares están en $\mathcal{C}$.

Ejemplo 3.1.6. Los siguientes códigos son códigos cíclicos:

I) Los códigos triviales $\{(0,0,0)\}$, el código de repetición y $\mathbb{F}_{q^n}$.

II) El (3,2,2)-código binario $\mathcal{C} = \{(0,0,0), (1,1,0), (0,1,1), (1,0,1)\}$.

Consideremos la siguiente aplicación $\varphi : \mathbb{F}_q^n \to \mathbb{F}_q[x]/\langle x^n - 1\rangle$ dado por:

$$\varphi(a_0, a_1, \ldots, a_{n-1}) = \left(a_{n-1}x^{n-1} + \cdots + a_1 x + a_0\right) + \langle x^n - 1\rangle$$

Es fácil verificar que φ es un isomorfismo entre $\mathbb{F}_q^n$ y $\mathbb{F}_q[x]/\langle x^n - 1\rangle$ como $\mathbb{F}_q$-espacios vectoriales. De ahora en adelante, veremos los elementos de $\mathbb{F}_q[x]/\langle x^n - 1\rangle$ como polinomios sobre $\mathbb{F}_q$ de grado a lo sumo $n-1$ con la suma usual entre polinomios y multiplicación módulo $x^n - 1$.

Teorema 3.1.7. *Sea φ la transformación lineal definida anteriormente. Entonces un subconjunto no vacío $\mathcal{C}$ de $\mathbb{F}_q^n$ es un código cíclico si, y solo si, $\varphi(\mathcal{C})$ es un ideal de $\mathbb{F}_q[x]/\langle x^n - 1\rangle$.*

Demostración. Supongamos que $\mathcal{C} \subseteq \mathbb{F}_q^n$ es un código cíclico. Veamos que $\varphi(\mathcal{C})$ es un ideal de $\mathbb{F}_q[x]/\langle x^n - 1\rangle$. Para esto sean f y g en $\varphi(\mathcal{C})$, entonces existen $x, y \in \mathcal{C}$ tal que $\varphi(x) = f$ y $\varphi(y) = g$. Como $\mathcal{C}$ es un espacio vectorial tenemos que $x - y \in \mathcal{C}$ y como φ es una transformación lineal $\varphi(x - y) = f - g$; luego $f - g \in \varphi(\mathcal{C})$. Ahora, note que si $f(x) = a_0 + a_1 x + \cdots + a_{n-1}x^{n-1} \in \varphi(\mathcal{C})$ entonces $(a_0, a_1, \ldots, a_{n-1}) \in \mathcal{C}$ y además tenemos que el polinomio

$$xf(x) = a_0 x + a_1 x^2 + \cdots + a_{n-2}x^{n-1} + a_{n-1}x^n = a_{n-1} + a_0 x + a_1 x^2 + \cdots + a_{n-2}x^{n-1}$$

también está en $\varphi(\mathcal{C})$ pues $\mathcal{C}$ es cíclico. Así, tenemos que $x^i f(x) \in \varphi(\mathcal{C})$ para todo $i \geq 0$. Si tomamos $h(x) = b_0 + b_1 x + \cdots + b_{n-1}x^{n-1}$, entonces

$$h(x)f(x) = \sum_{i=0}^{n-1} b_i(x^i f(x)).$$

Como $\mathcal{C}$ es un espacio vectorial sobre $\mathbb{F}_q$ y φ es una transformación lineal tenemos que $\varphi(\mathcal{C})$ es un espacio vectorial sobre $\mathbb{F}_q$ y por lo tanto $b_i(x^i f(x)) \in \varphi(\mathcal{C})$ para todo $i \geq 0$. De lo anterior se sigue que $\varphi(\mathcal{C})$ es un ideal de $\mathbb{F}_q[x]/\langle x^n - 1\rangle$.

Recíprocamente, supongamos que $\varphi(\mathcal{C})$ es un ideal de $\mathbb{F}_q[x]/\langle x^n - 1\rangle$. Sean $\alpha, \beta \in \mathcal{C}$ y $c \in \mathbb{F}_q$, entonces como $\varphi(\mathcal{C})$ es un ideal tenemos que $\varphi(\alpha) + \varphi(\beta) = \varphi(\alpha + \beta) \in \varphi(\mathcal{C})$ y $c\varphi(\alpha) = \varphi(c\alpha) \in \varphi(\mathcal{C})$; luego $\alpha + \beta \in \mathcal{C}$ y $c\alpha \in \mathcal{C}$. Así, hemos mostrado que $\mathcal{C}$ es un código lineal. Restar ver que $\mathcal{C}$ es cíclico, para esto sea $\alpha = (a_0, a_1, \ldots, a_{n-1}) \in \mathcal{C}$, entonces $f(x) = a_0 + a_1 x + \cdots + a_{n-1}x^{n-1} \in \varphi(\mathcal{C})$ y como $\varphi(\mathcal{C})$ es ideal tenemos

que $xf(x) = a_{n-1} + a_0x + a_1x^2 + \cdots + a_{n-2}x^{n-1} \in \varphi(\mathcal{C})$, lo que implica que $(a_{n-1}, a_0, \ldots, a_{n-2}) \in \mathcal{C}$. □

Mostraremos ahora que $\mathbb{F}_q[x]/\langle x^n - 1\rangle$ es un dominio de ideales principales.

Teorema 3.1.8. *Sea I un ideal no nulo en $\mathbb{F}_q[x]/\langle x^n - 1\rangle$ y sea $g(x)$ un polinomio mónico de grado mínimo en I. Entonces $I = \langle g(x)\rangle$ y $g(x) \mid x^n - 1$.*

Demostración. Es claro que $\langle g(x)\rangle \subseteq I$. Sea $p(x) \in I$, entonces por el algoritmo de la división existen $h(x), r(x) \in \mathbb{F}_q[x]$ tales que $p(x) = h(x)g(x) + r(x)$ donde $r(x) = 0$ o $\partial r(x) < \partial g(x)$. Note que si $r(x) \neq 0$ entonces $p(x) - h(x)g(x) = r(x) \in I$, lo que contradice que $g(x)$ tiene grado mínimo en I. Luego, $r(x) = 0$ y así $I = \langle g(x)\rangle$.

Veamos que $g(x) \mid x^n - 1$. Por el algoritmo de la división, existen $h(x), r(x) \in \mathbb{F}_q[x]$ tales que $x^n - 1 = h(x)g(x) + r(x)$ donde $r(x) = 0$ o $\partial r(x) < \partial g(x)$. Pero como $x^n - 1$ es el elemento neutro en $\mathbb{F}_q[x]/\langle x^n - 1\rangle$ tenemos que $x^n - 1 \in I$. Luego, $(x^n - 1) - h(x)g(x) = r(x) \in I$ y así $r(x) = 0$. □

Teorema 3.1.9. *Existe un único polinomio mónico de grado mínimo en cada ideal no nulo I de $\mathbb{F}_q[x]/\langle x^n - 1\rangle$.*

Demostración. Sean $g_1(x)$ y $g_2(x)$ dos polinomios diferentes mónicos de grado mínimo en I, entonces algún múltiplo escalar conveniente de $g_1(x) - g_2(x)$ es un polinomio mónico de menor grado en I. Un absurdo. □

Definición 3.1.10. El único polinomio de grado mínimo en el ideal no nulo I de $\mathbb{F}_q[x]/\langle x^n - 1\rangle$ es llamado el **polinomio generador** de I. Para un código cíclico $\mathcal{C}$, el polinomio generador de $\varphi(\mathcal{C})$ es también llamado el **polinomio generador** de $\mathcal{C}$.

Ejemplo 3.1.11. Sea $\mathcal{C} = \{(0,0,0), (1,1,0), (0,1,1), (1,0,1)\}$. Entonces

$$\varphi(\mathcal{C}) = \left\{0, x+1, x^2+x, x^2+1\right\}$$

y por lo tanto el polinomio generador de $\mathcal{C}$ es $x + 1$.

Teorema 3.1.12. *Cada divisor mónico de $x^n - 1$ es el polinomio generador de algún código en $\mathbb{F}_q^n$.*

Demostración. Sea $h(x)$ divisor de $x^n - 1$. Considere $I = \langle h(x)\rangle$. Sea $g(x)$ el polinomio generador de I, veamos que $h(x) = g(x)$. Como $I = \langle h(x)\rangle$ entonces existe $r(x) \in \mathbb{F}_q[x]$

tal que $g(x) \equiv h(x)r(x) \pmod{x^n - 1}$; luego $x^n - 1 \mid g(x) - h(x)r(x)$. Como $h(x) \mid x^n - 1$, tenemos que $h(x) \mid g(x) - h(x)r(x)$ y por tanto $h(x) \mid g(x)$. Esto es, $g(x) = h(x)a(x)$ pero como $g(x)$ tiene grado mínimo en I, $a(x)$ debe ser una constante y además como tanto $g(x)$ como $h(x)$ son mónicos concluimos que $a(x) = 1$. □

El siguiente corolario es una consecuencia inmediata de los Teoremas 3.1.8 y 3.1.12.

Corolario 3.1.13. *Existe una función biyectiva entre los códigos cíclicos en $\mathbb{F}_q^n$ y los divisores mónicos de $x^n - 1 \in \mathbb{F}_q[x]$.*

Ejemplo 3.1.14. Para encontrar todos los códigos binarios cíclicos de longitud 6, escribimos a $x^6 - 1$ como producto de polinomios irreducibles sobre $\mathbb{F}_2$:

$$x^6 - 1 = (1 + x)^2(1 + x + x^2)^2$$

Así, hay 9 códigos binarios cíclicos de longitud 6 y se determinan a partir de la preimagen de los ideales generados por estos polinomios bajo φ.

3.2. Álgebras de grupo

Estamos interesados en mostrar otra forma de construir códigos cíclicos usando álgebras de grupo. Para esto, empezaremos con algunas definiciones y propiedades sobre álgebras de grupo. Posteriormente, necesitaremos algunos conceptos y resultados sobre módulos y anillos semisimples que se encuentran en el Apéndice B.

Sea G un grupo y R un anillo. Denotamos por RG al conjunto de todas las combinaciones lineales formales:

$$\alpha = \sum_{g \in G} a_g g,$$

donde $a_g \in R$ y $a_g = 0$ casi en toda parte, esto es, solo un número finito de coeficientes son diferentes de cero.

Dado un elemento $\alpha = \sum_{g \in G} a_g g$ definimos el **soporte** de α como el conjunto

$$supp(\alpha) = \{g \in G : a_g \neq 0\}.$$

Definimos la suma de dos elementos de RG componente a componente:

$$\left(\sum_{g\in G} a_g g\right) + \left(\sum_{g\in G} b_g g\right) = \sum_{g\in G}(a_g + b_g)g.$$

También, definimos la multiplicación de dos elementos $\alpha = \sum_{g\in G} a_g g$ y $\beta = \sum_{g\in G} b_g g$ por

$$\alpha\beta = \sum_{g,h\in G} a_g b_h gh.$$

Es fácil verificar que con las operaciones anteriormente definidas, RG es un anillo con unidad $1_{RG} = \sum_{g\in G} u_g G$ donde $u_{1_G} = 1_R$ y $u_g = 0_G$ con $g \neq 1_G$.

Podemos dar a RG una estructura de R-módulo vía:

$$\lambda\left(\sum_{g\in G} a_g g\right) = \sum_{g\in G}(\lambda a_g)g.$$

Proposición 3.2.1. *Sean R un anillo conmutativo y G un grupo. Entonces:*

$$r(\alpha\beta) = (r\alpha)\beta = \alpha(r\beta),$$

para todo $r \in R$ y $\alpha, \beta \in RG$.

Demostración. Sean $\alpha = \sum_{g\in G} a_g g, \beta = \sum_{g\in G} b_g g$ y $r \in R$, entonces:

$$\begin{aligned}
r(\alpha\beta) &= r\left(\sum_{g,h\in G} a_g b_h gh\right) \\
&= \sum_{g,h\in G} (r(a_g b_h))gh \\
&= \sum_{g,h\in G} ((ra_g)b_h)gh \\
&= \left(\sum_{g\in G} ra_g g\right)\left(\sum_{g\in G} b_g g\right) \\
&= \left(r\left(\sum_{g\in G} a_g g\right)\right)\left(\sum_{g\in G} b_g g\right) \\
&= (r\alpha)\beta.
\end{aligned}$$

De igual forma,

$$\begin{aligned} r(\alpha\beta) &= \sum_{g,h\in G}(a_g(rb_h))gh \\ &= \left(\sum_{g\in G} a_g g\right)\left(\sum_{g\in G}(rb_g)g\right) \\ &= \left(\sum_{g\in G} a_g g\right)\left(r\left(\sum_{g\in G} b_g g\right)\right) \\ &= \alpha(r\beta). \end{aligned}$$

□

Definición 3.2.2. Sea R un anillo conmutativo. Un R-módulo M es llamado un R-**álgebra** si existe una multiplicación definida en M tal que con la suma dada, M sea un anillo y verifique:

$$r(\alpha\beta) = (r\alpha)\beta = \alpha(r\beta),$$

para todo $r \in R$ y $\alpha, \beta \in M$.

De esta forma, el conjunto RG con las operaciones definidas anteriormente es llamado el **anillo de grupo** de G sobre R. Si R es conmutativo, RG es también llamado el **álgebra de grupo** de G sobre R.

Ahora mostraremos otra forma de encontrar códigos cíclicos usando álgebras de grupo.

Teorema 3.2.3. *Sea C_n el grupo cíclico de orden n y $\mathbb{F}_q C_n$ su álgebra de grupo sobre $\mathbb{F}_q$. Entonces $\mathbb{F}_q[x]/\langle x^n - 1\rangle \cong \mathbb{F}_q C_n$ como anillos.*

Demostración. Sea $C_n = \{e, a, a^2, \ldots, a^{n-1}\}$. Considere $\varphi : \mathbb{F}_q[x] \to \mathbb{F}_q C_n$ tal que $\varphi(f(x)) = f(a)$. Es fácil ver que φ es un epimorfismo de anillos. Además, por el primer teorema de isomorfismo para anillos tenemos que $\mathbb{F}_q[x]/\operatorname{Ker}(\varphi) \cong \mathbb{F}_q C_n$; así basta ver que $\operatorname{Ker}(\varphi) = \langle x^n - 1\rangle$.
Note que como $a^n = 1$ entonces $x^n - 1 \in \operatorname{Ker}(\varphi)$. De igual forma, si $c_{n-1}a^{n-1} + \cdots + c_1 a + c_0 e = 0_{\mathbb{F}G}$, entonces $c_i = 0_{\mathbb{F}}$. Luego, $x^n - 1$ es un polinomio no nulo de grado mínimo en el ideal $\operatorname{Ker}(\varphi)$ y por lo tanto $\operatorname{Ker}(\varphi) = \langle x^n - 1\rangle$. □

Así, el estudio de códigos cíclicos de longitud n sobre $\mathbb{F}_q$ también puede verse como el estudio de ideales en el álgebra de grupo $\mathbb{F}_q C_n$. En la siguiente sección estaremos interesados en estudiar los ideales minimales de $\mathbb{F}_q C_n$. A continuación, mencionaremos algunos resultados que serán fundamentales para hallar dichos ideales.

Teorema 3.2.4. *(Teorema de Maschke) Sea G un grupo. Entonces, el anillo de grupo RG es semisimple si, y solo si, se verifican las siguientes condiciones:*

I) *R es un anillo semisimple.*

II) *G es finito.*

III) *$|G|$ es invertible en R.*

Demostración. Ver [10], Sección 3.4. □

Corolario 3.2.5. *Sea G un grupo finito y sea $\mathbb{F}$ un cuerpo. Entonces $\mathbb{F}G$ es semisimple si, y solo si, la característica de $\mathbb{F}$ no divide a $|G|$.*

Demostración. Como $\mathbb{F}$ es cuerpo, los únicos ideales de $\mathbb{F}$ son los triviales que son generados por el 1 y el 0, elementos idempotentes; luego $\mathbb{F}$ es semisimple. $|G|$ es invertible si, y solo si, $|G| \neq 0 \in \mathbb{F}$; esto sucede si, y solo si, la característica de $\mathbb{F}$ no divide a $|G|$. □

El Teorema Wedderburn-Artin en este contexto nos proporciona gran información sobre la estructura del álgebra de grupo.

Teorema 3.2.6. *Sea G un grupo finito y sea $\mathbb{F}$ un cuerpo tal que la característica de $\mathbb{F}$ no divide a $|G|$. Entonces:*

I) *$\mathbb{F}G$ es la suma directa de un número finito de ideales minimales bilaterales $\{B_i\}_{1 \leq i \leq r}$, las componentes simples de $\mathbb{F}G$. Cada B_i es un anillo simple.*

II) *Cualquier ideal bilateral de $\mathbb{F}G$ es la suma directa de algunos miembros de la familia $\{B_i\}_{1 \leq i \leq r}$.*

III) *Cada componente simple B_i es isomorfa un anillo de matrices de la forma $M_{n_i}(D_i)$ donde D_i es un anillo de división que contiene una copia isomorfa a $\mathbb{F}$ en su centro y el isomorfismo $KG \cong \oplus_{i=1}^{t} M_{n_i}(D_i)$ es un isomorfismo de K-álgebras.*

---

[10] Sudarshan POLCINO Cesar y SEHGAL. *An Introduction to Group Rings*. Kluwer Academic Publishers, Dortrecht, 2002.

3.3. Idempotentes en álgebras de grupo y códigos cíclicos minimales

Como mencionamos en la sección anterior hallar ideales minimales en $\mathbb{F}_q C_n$ es equivalente a hallar códigos cíclicos minimales de longitud n sobre $\mathbb{F}_q$. Mostraremos como hallar dichos ideales en ciertos casos particulares, ayudándonos de la semisimplicidad de dichos anillos. Empezaremos hallando el número de componentes simples de un álgebra de grupo finito, abeliano y semisimple.

Sea $\mathbb{F}_q$ el cuerpo finito con q elementos y sea A un grupo abeliano finito tal que $mcd(q, |A|) = 1$. Entonces por el Corolario 3.2.5 tenemos que $\mathbb{F}_q A$ es semisimple y si $\{e_1, \ldots, e_r\}$ es el conjunto de idempotentes primitivos de $\mathbb{F}_q A$ (ver el apéndice B), entonces:

$$\mathbb{F}_q A = \oplus_{i=1}^{r} (\mathbb{F}_q A)\, e_i \cong \oplus_{i=1}^{r} M_{n_i}(D_i) \cong \oplus_{i=1}^{r} F_i,$$

donde $(\mathbb{F}_q A)\, e_i \cong F_i$. Note que como $\mathbb{F}_q A$ es conmutativo, entonces cada $M_{n_i}(D_i)$ también debe serlo y por lo tanto $n_i = 1$ para todo $i \in \{1, \ldots, r\}$ y D_i debe ser un cuerpo finito que contiene una copia de $\mathbb{F}_q$; luego $D_i = F_i$ es una extensión finita de $\mathbb{F}_q$.

Lema 3.3.1. *Sea $\mathcal{A} = \oplus_{i=1}^{r} \mathbb{F}_q e_i$. Entonces para todo $i \in \{1, \ldots, r\}$, $\mathbb{F}_q e_i \cong \mathbb{F}_q$ como anillos y el número r de componentes simples de $\mathbb{F}_q A$ es también la dimensión de $\mathcal{A}$ como $\mathbb{F}_q$-espacio vectorial.*

Demostración. Sea $i \in \{1, \ldots, r\}$ y consideremos $\varphi : \mathbb{F}_q \to \mathbb{F}_q e_i$ dado por $\varphi(\alpha) = \alpha e_i$, para todo $\alpha \in \mathbb{F}_q$. Sean $\alpha, \beta \in \mathbb{F}_q$, entonces

$$\varphi(\alpha + \beta) = (\alpha + \beta)e_i = \alpha e_i + \beta e_i = \varphi(\alpha) + \varphi(\beta)$$

$$\varphi(\alpha\beta) = (\alpha\beta)e_i = (\alpha\beta)e_i e_i = (\alpha e_i)(\beta e_i) = \varphi(\alpha)\varphi(\beta)$$

Luego, φ es un homomorfismo de anillos. Supongamos ahora que $\varphi(\alpha) = \varphi(\beta)$ y escribamos $e_i = \sum_{g \in A} a_g g$ entonces $\sum_{g \in A} (\alpha a_g) g = \sum_{g \in A} (\beta a_g) g$. Como e_i es un elemento no nulo existe $g_1 \in A$ tal que $a_{g_1} \neq 0$ y además como $\alpha a_{g_1} = \beta a_{g_1}$ concluimos que $\alpha = \beta$. De esta forma φ es una función inyectiva y como es claro que es sobreyectiva concluimos que es un isomorfismo.

Finalmente, veamos que $\{e_1, \ldots, e_r\}$ es una base para $\mathcal{A}$ como $\mathbb{F}_q$-espacio vectorial. De la definición de $\mathcal{A}$ es claro que estos idempotentes generan este espacio vectorial. Restar ver que son linealmente independientes. Sean $c_1, \ldots, c_r \in \mathbb{F}_q$ tales que $c_1 e_1 + \cdots + c_r e_r = 0$.

Dado que la suma es directa concluimos que $c_i e_i = 0$, para todo $1 \leq i \leq r$. Escribamos $e_i = \sum_{g \in A} a_{ig} g$, como cada e_i es no nulo entonces para cada e_i existe un g_i tal que $a_{ig_i} \neq 0$ y como $c_i a_{ig_i} = 0$ concluimos que $c_i = 0$. □

Lema 3.3.2. *Sea $\alpha \in \mathbb{F}_q A$. Entonces $\alpha \in \mathcal{A}$ si, y solo si, $\alpha^q = \alpha$.*

Demostración. Sea $\alpha \in \mathbb{F}_q A$, entonces $\alpha = \sum_{i=1}^{r} \alpha_i$ siendo $\alpha_i = \alpha e_i \in (\mathbb{F}_q A) e_i$. Así, $\alpha \in \mathcal{A}$ si, y solo si, $\alpha_i \in \mathbb{F}_q e_i$ para cada $i \in \{1, \ldots, r\}$. Pero como $\mathbb{F}_q e_i \cong \mathbb{F}_q$, esto sucede, si, y solo si, $\alpha_i^q = \alpha_i$. Además, $\alpha^q = \sum_{i=1}^{r} \alpha_i^q$; luego $\alpha \in \mathcal{A}$ si, y solo si, $\alpha^q = \alpha$. □

Sea g un elemento de un grupo abeliano finito A. Si $mcd(q, |A|) = 1$, entonces q y $o(g)$ son primeros relativos y por lo tanto existen algún entero positivo x tal que

$$q^x \equiv 1 \pmod{o(g)}. \tag{3.1}$$

Así, definimos la **clase q-ciclotómica** de g como el conjunto:

$$S_g = \left\{ g^{q^j} \mid 0 \leq j \leq t_g - 1 \right\},$$

donde t_g es el menor entero positivo que verifica (3.1).

Lema 3.3.3. *La familia $\{S_g\}_{g \in A}$ definida anteriormente forman una partición de A.*

Demostración. Como para $g \in A$ se tiene que $g \in S_g$, entonces $\bigcup_{g \in A} S_g = A$. Veamos que si $S_g \cap S_h \neq \emptyset$ entonces $S_g = S_h$. Fijemos $x \in S_g \cap S_h$, entonces $x = g^{q^i}$ con $1 \leq i \leq t_g - 1$ y $x = h^{q^j}$ con $1 \leq j \leq t_h - 1$. Sea $z \in S_g$, entonces $z = g^{q^k}$ con $1 \leq k \leq t_g - 1$, note que

$$z = (g^{q^i})^{q^{k-i}} = x^{q^{k-i}} = (h^{q^j})^{q^{k-i}} = h^{q^{k+j-i}}.$$

Por el algoritmo de la división existen $r, s \in \mathbb{Z}$ tales que $k+j-i = t_h s + r$ con $0 \leq r \leq t_h - 1$. Así,

$$z = h^{q^{k+j-i}} = h^{q^{t_h s + r}} = \left(h^{q^{t_h s}} \right)^{q^r} = h^{q^r}$$

pues $(q^{t_h})^s \equiv 1 \pmod{o(h)}$ y así $S_g \subseteq S_h$. Análogamente se muestra que $S_h \subseteq S_g$. □

Teorema 3.3.4. *Sea $\mathbb{F}_q$ el cuerpo finito con q elementos y sea A un grupo abeliano finito tal que $mcd(q, |A|) = 1$. Entonces, el número de componentes simples de $\mathbb{F}_q A$ es igual al número de clases q-ciclotómicas de A.*

Demostración. Sea $T = \{g_1, \ldots, g_s\}$ un conjunto de representantes de las clases q-ciclotómicas. Como probamos en el Lema 3.3.1 el número de componentes simples de $\mathbb{F}_q A$ es igual a la dimensión de $\mathcal{A}$ como $\mathbb{F}_q$-espacio vectorial, así que mostaremos una base para $\mathcal{A}$ con s elementos. Sea S_g una clase q-ciclotómica, definimos $n_g = \sum_{h \in S_g} h \in \mathbb{F}_q A$. Afirmamos que $\mathcal{B} = \{n_{g_i} \mid 1 \leq i \leq s\}$ es una base para $\mathcal{A}$ como $\mathbb{F}_q$-espacio vectorial. Note que como $n_g = g + g^q + g^{q^2} + \cdots + g^{q^{t_g - 1}}$ entonces

$$n_g^q = g^q + g^{q^2} + \cdots + g^{q^{t_g - 1}} + g^{q^{t_g}} = g^q + g^{q^2} + \cdots + g^{q^{t_g - 1}} + g = n_g,$$

lo que implica que $n_g \in \mathcal{A}$ por el Lema 3.3.2. De lo anterior, $\mathcal{B} \subseteq \mathcal{A}$. Es claro que $\mathcal{B}$ es linealmente independiente, luego restar ver que $\mathcal{B}$ genera $\mathcal{A}$.

Sea $\alpha = \sum_{g \in A} a_g g \in \mathcal{A}$, del Lema 3.3.2 tenemos que $\alpha^q = \alpha$; luego

$$\alpha = \sum_{g \in A} a_g g = \left(\sum_{g \in A} a_g g \right)^q = \sum_{g \in A} a_g^q g^q,$$

pero como $a_g \in \mathbb{F}_q$ tenemos que $a_g^q = a_g$ y así

$$\alpha = \sum_{g \in A} a_g g = \sum_{g \in A} a_g g^q.$$

De esta forma, para cada $g \in A$, $a_g = a_{g^q} = \cdots = a_{g^{q^{t_g - 1}}}$ y por lo tanto

$$\alpha = \sum_{g \in T} a_g n_g.$$

□

Lema 3.3.5. *Sea A un grupo abeliano finito y $g \in A$, entonces:*

I) *Cada clase q-ciclótomica S_g es un subconjunto del conjunto $\mathcal{G}_g$ de todos los generadores del grupo cíclico $\langle g \rangle$.*

II) *El número de grupos cíclicos de A es igual al de las componentes simples de $\mathbb{F}_q A$ si, y sólo si, $S_g = \mathcal{G}_g$, para todo $g \in A$*

Demostración. Probaremos cada una de las afirmaciones.

I) Sea $x \in S_g$, entonces $x = g^{q^j}$ con $1 \leq j \leq t_g - 1$ y por lo tanto $o(x) = \frac{o(g)}{mcd(q^j, o(g))}$. Como q y $o(g)$ son primos relativos concluimos que $o(x) = o(g)$. Luego, x es un generador del grupo cíclico $\langle g \rangle$.

II) Del ítem anterior tenemos que si dos elementos pertenecen a la misma clase q-ciclotómica entonces su grupo cíclico es el mismo, lo que implica que el número de grupos cíclicos de A es menor o igual que el número de componentes simples de $\mathbb{F}_q A$. Luego estas cantidades coinciden si, y solo si, $S_g = \mathcal{G}_g$.

□

Mostraremos una condición necesaria y suficiente para que $S_g = \mathcal{G}_g$ pero para eso necesitamos algunos resultados sobre el exponente de un grupo y los elementos invertibles de $\mathbb{Z}_n$.

Definición 3.3.6. Sea G un grupo, definimos el **exponente** de G como el menor entero positivo e tal que $g^e = 1$, para todo $g \in G$.

Proposición 3.3.7. *Sea $G = \{g_1, \ldots, g_r\}$ un grupo abeliano finito, entonces el exponente e de G es el $max\{o(g_1), \ldots, o(g_r)\}$.*

Demostración. Veamos que $g^n = 1$, para todo $g \in G$ donde $n = max\{o(g_1), \ldots, o(g_r)\}$. Fijemos $a \in G$ tal que $o(a) = n$ y sea g un elemento arbitario de G. Llamemos $d = o(g)$. Afirmamos que si p es un primo que divide a d entonces p divide a n.

Suponga por contradicción que existe un primo p tal que $p|d$ pero $p \nmid n$, entonces como G es abeliano es claro que $\left(ag^{d/p}\right)^{np} = e$. Sea $s = o(ag^{d/p})$, tenemos dos casos: si $p|s$ entonces $s = px$ y por lo tanto $a^{px}g^{dx} = 1$; luego $a^{px} = 1$, lo que implica que $n|px$ pero como n y p son primos relativos tenemos que $n|x$. Además, $s = px|np$ y por lo tanto $x|n$, concluyendo que $s = pn$. Ahora, si $p \nmid s$, como $s|np$, entonces $s|n$. De igual forma, tenemos que $a^s = g^{\frac{-sd}{p}}$ y por lo tanto

$$o(a^s) = \frac{n}{mcd(s,n)} = \frac{n}{s} = \frac{d}{mcd(d, \frac{-sd}{p})} = \frac{d}{d/p}$$

Luego, $n = ps$, lo que no puede ser ya que p no divide a n. Así, hemos mostrado que $ag^{d/p}$ tiene orden $np > n$, un absurdo.

Ahora, sea p un primo que divide a d y escribamos $n = p^x r$ y $d = p^y s$ con

$mcd(p^x, r) = mcd(p^y, s) = 1$. Entonces, de manera similar a la anterior se puede probar que $a^{p^x} g^s$ tiene orden $p^y r \leq n = p^x r$ y por lo tanto $y \leq x$. Lo anterior, muestra que $d|n$ y por lo tanto $g^n = 1$. Como n es el menor entero tal que $a^n = 1$, concluimos que el exponente de G es n. □

Lema 3.3.8. *Sean n un entero positivo y $d \mid n$. Si $U(n)$ es un grupo cíclico generado por $q \in U(n)$, entonces $U(d)$ es un grupo cíclico generado por q donde q es visto como elemento de $U(d)$.*

Demostración. Como $q \in U(n)$ entonces $mcd(q, n) = 1$ y como $d \mid n$ concluimos que $mcd(q, d) = 1$; luego $q \in U(d)$. Veamos que q es generador de $U(d)$. Sea $y \in U(d)$. Afirmamos que existe $z \in U(n)$ tal que $y \equiv z \,(\mathrm{mód}\, d)$. En efecto, definamos t como el producto de todos los primos p tales que $p|n$ pero $p \nmid d$. De la definición de t es claro que t y d son primos relativos y por lo tanto existen $m, s \in \mathbb{Z}$ tales que $y - 1 = dm + ts$. Lo que implica que $y - dm \equiv 1 \,(\mathrm{mód}\, t)$ y por lo tanto $y - dm \in U(t)$. Por otro lado, como $y \equiv y - dm \,(\mathrm{mód}\, d)$ resta ver que $z = y - dm \in U(n)$. Para esto, sea p un primo que divide a n. Si $p|d$ entonces $p \nmid y - dm$ pues $y - dm$ y d son coprimos. Si $p \nmid d$ entonces $p|t$ y por lo tanto $p \nmid y - dm$. Así, hemos probado que $z \in U(n)$.
Como $z \in U(n)$, entonces existe algún entero positivo r tal que $q^r \equiv z \,(\mathrm{mód}\, n)$. Pero como $d \mid n$ esto implica que $z \equiv q^r \,(\mathrm{mód}\, d)$ y por lo tanto $y \equiv q^r \,(\mathrm{mód}\, d)$. □

Para todos los enteros positivos r y m denotamos por $\overline{r} \in \mathbb{Z}_m$ al residuo que deja r al dividirse entre m y por lo tanto,

$$\mathcal{G}_g = \{g^r \mid mcd(r, o(g)) = 1\} = \{g^r \mid \overline{r} \in U(o(g))\}.$$

Teorema 3.3.9. *Sea $\mathbb{F}_q$ el cuerpo finito con q elementos y sea A un grupo abeliano finito de exponente e tal que $mcd(q, |A|) = 1$. Entonces $S_g = \mathcal{G}_g$, para todo $g \in A$ si, y solo si, $U(e)$ es un grupo cíclico generado por $\overline{q} \in \mathbb{Z}_e$.*

Demostración. Supongamos que $S_g = \mathcal{G}_g$ para todo $g \in A$. Como A es un grupo abeliano finito de exponente e tenemos por la Proposición 3.3.7 que existe $g_0 \in A$ tal que $o(g_0) = e$. Como $S_{g_0} = \mathcal{G}_{g_0}$ concluimos que para cualquier entero positivo r tal que $\overline{r} \in U(e)$, $g_0^r \in S_{g_0}$ y por lo tanto existe algún entero j tal que $g_0^r = g_0^{q^j}$, esto es, $e|r - q^j$ y por lo tanto $\overline{r} = \overline{q}^j$. Luego, $\overline{q}$ es un generador de $U(e)$.

Recíprocamente, supongamos que $U(e)$ es generado por $\overline{q}$. Como $S_g \subseteq \mathcal{G}_g$, basta

mostar que $\mathcal{G}_g \subseteq S_g$, para todo $g \in A$. Sea $g \in A$, entonces $o(g)|e$ y por el Lema 3.3.8 tenemos que $\overline{q}$ es un generador de $U(o(g))$. Ahora sea $h \in \mathcal{G}_g$, entonces $h = g^r$ para algún entero positivo r tal que $\overline{r} \in U(o(g))$ y por lo tanto existe algún entero positivo j tal que $\overline{r} = \overline{q}^j$, lo que implica que $o(g)|r - q^j$ y por lo tanto $g^r = g^{q^j} \in S_g$. Lo que muestra que $\mathcal{G}_g \subseteq S_g$. □

$U(e)$ es cíclico si, y solo si, $e = 2, 4, p^n$, o $2p^n$, donde p es un primo impar y n es un entero positivo (Ver [11], Sección 7.3). Por lo tanto, tenemos el siguiente corolario:

Corolario 3.3.10. *Sea $\mathbb{F}_q$ el cuerpo finito de q elementos y sea A un grupo abeliano finito de exponente e. Entonces $S_g = \mathcal{G}_g$ para todo $g \in A$ si, y solo si, una de las siguientes condiciones se valen:*

I) $e = 2$ *y* q *es impar.*

II) $e = 4$ *y* $q \equiv 3 \pmod 4$.

III) $e = p^n$ *y* $o(q) = \phi(p^n)$ *en* $U(p^n)$, *con* p *impar.*

IV) $e = 2p^n$ *y* $o(q) = \phi(p^n)$ *en* $U(2p^n)$, *con* p *impar.*

Proposición 3.3.11. *Sea H un subgrupo de un grupo finito G. Si $mcd(q, |G|) = 1$, entonces*

$$\widehat{H} = \frac{1}{|H|} \sum_{g \in H} g$$

es un elemento idempotente de $\mathbb{F}_q G$.

Demostración. En primer lugar, como $|H|$ divide a $|G|$ y $mcd(q, |G|) = 1$ tenemos que $mcd(q, |H|) = 1$; luego $|H|$ es invertible en $\mathbb{F}_q$ y por lo tanto $\widehat{H}$ está bien definido. Llamemos $x = \sum_{g \in H} g$, usando la Proposición 3.2.1 y el hecho de que H es subgrupo de G tenemos:

$$\widehat{H}\widehat{H} = \frac{1}{|H|^2} \left(\sum_{g \in H} g \right) x = \frac{1}{|H|^2} \sum_{g \in H} gx = \frac{1}{|H|^2} \sum_{g \in H} x = \frac{1}{|H|^2} |H| x = \widehat{H}.$$

□

[11] Paulo MARTIN. *Grupos, Corpos e Teoria de Galois*. Editora Livraria de Fisica, 2010.

Lema 3.3.12. *Sean $\mathbb{F}_q$ el cuerpo finito de q elementos, A un grupo cíclico de p^n elementos donde p es un primo tal que p no divide a q y*

$$A = A_0 \supset A_1 \supset \cdots \supset A_n = \{1\}$$

la cadena descendente de todos los subgrupos de A. Entonces los elementos

$$\widehat{e_0} = \widehat{A} \text{ y } e_i = \widehat{A_i} - \widehat{A_{i-1}}, 1 \leq i \leq n$$

forman un conjunto de idempotentes ortogonales de $\mathbb{F}_q A$ tal que $e_0 + e_1 + \cdots + e_n = 1$.

Demostración. De la proposición anterior tenemos que e_0 es un elemento idempotente. Sea $1 \leq i \leq n$, veamos que e_i es idempotente.

$$e_i e_i = \left(\widehat{A_i} - \widehat{A_{i-1}}\right)\left(\widehat{A_i} - \widehat{A_{i-1}}\right) = \widehat{A_i}\widehat{A_i} - 2\widehat{A_i}\widehat{A_{i-1}} + \widehat{A_{i-1}}\widehat{A_{i-1}} = \widehat{A_i} - 2\widehat{A_i}\widehat{A_{i-1}} + \widehat{A_{i-1}}$$

Llamando $x = \sum_{g \in A_{i-1}} g$, note que como $A_i \subset A_{i-1}$ entonces:

$$\begin{aligned}
\widehat{A_i}\widehat{A_{i-1}} &= \left(\frac{1}{|A_i|}\sum_{g \in A_i} g\right)\left(\frac{1}{|A_{i-1}|}\sum_{g \in A_{i-1}} g\right) \\
&= \frac{1}{|A_i||A_{i-1}|}\sum_{g \in A_i} gx \\
&= \frac{1}{|A_i||A_{i-1}|}\sum_{g \in A_i} x \\
&= \frac{1}{|A_i||A_{i-1}|}|A_i|x \\
&= \widehat{A_{i-1}}.
\end{aligned}$$

Luego; $e_i e_i = e_i$.

Por otro lado, note que si $j \leq i$, se puede probar con el argumento anterior que $\widehat{A_j}\widehat{A_i} = A_j$. Sean $j, i \in \{1, \ldots, n\}$ con $j \neq i$, supongamos sin pérdida de generalidad con $j < i$ entonces

$$e_i e_j = \widehat{A_i}\widehat{A_j} - \widehat{A_i}\widehat{A_{j-1}} - \widehat{A_{i-1}}\widehat{A_j} + \widehat{A_{i-1}}\widehat{A_{j-1}} = \widehat{A_j} - \widehat{A_{j-1}} - \widehat{A_j} + \widehat{A_{j-1}} = 0$$

$$e_0 e_i = \widehat{A_0}\widehat{A_i} - \widehat{A_0}\widehat{A_{i-1}} = \widehat{A_0} - \widehat{A_0} = 0$$

Finalmente, tenemos que

$$e_0 + e_1 + \cdots + e_n = e_0 + \sum_{i=1}^{n} \left(\widehat{A_i} - \widehat{A_{i-1}} \right) = e_0 + \widehat{A_n} - \widehat{A_0} = \widehat{A_n} = 1.$$

□

Teniendo en cuenta que la cantidad de idempotentes descritos anteriormente es $n+1$, estos idempotentes son los primitivos si, y solo si, $\mathbb{F}_q A$ tiene $n+1$ componentes simples. Además, como el exponente de un grupo cíclico de p^n elementos es p^n tenemos a partir del Corolario 3.3.10 el siguiente resultado.

Corolario 3.3.13. *Sea $\mathbb{F}_q$ el cuerpo finito con q elementos y sea A un grupo cíclico de p^n elementos. Entonces, el conjunto de idempotentes dados en el lema anterior es el conjunto de idempotentes primitivos de $\mathbb{F}_q A$ si, y solo si, alguna de las siguientes condiciones se vale:*

I) *$p = 2$, $n = 1$ y q impar.*

II) *$p = 2$, $n = 2$ y $q \equiv 3 \pmod 4$.*

III) *p es un primo impar y $o(q) = \phi(p^n)$ en $U(p^n)$.*

El siguiente teorema es inmediato de los resultados anteriores.

Teorema 3.3.14. *Sean $\mathbb{F}_q$ el cuerpo finito con q elementos, A un grupo cíclico de p^n elementos, con p impar tal que $o(q) = \phi(p^n)$ en $U(p^n)$ y*

$$A = A_0 \supset A_1 \supset \cdots \supset A_n = \{1\}$$

la cadena descendente de todos los subgrupos de A. Entonces, el conjunto de los elementos idempotentes primitivos de $\mathbb{F}_q A$ son:

$$\widehat{e_0} = \frac{1}{p^n} \sum_{a \in A} a \text{ y } e_i = \widehat{A_i} - \widehat{A_{i-1}}, 1 \leq i \leq n.$$

Por el Teorema B.0.18 y la Proposición B.0.23 del Apéndice B tenemos que estos idempotentes determinan el conjunto de todos ideales minimales de $\mathbb{F}_q A$ y por lo tanto, todos los códigos cíclicos minimales de longitud p^n sobre $\mathbb{F}_q$.

Teorema 3.3.15. *Sean $\mathbb{F}_q$ el cuerpo con q elementos y $G = \langle a \rangle$ un grupo cíclico de $2p^n$ elementos con p un primo impar tal que $o(q) = \phi(p^n)$ en $U(2p^n)$. Entonces*

I) *$G = C \times A$, donde $A = \langle a^2 \rangle$ y $C = \{1, t\}$ con $t = a^{p^n}$.*

II) *Si e_i, $0 \leq i \leq n$, denota los idempotentes primitivos de $\mathbb{F}_q A$ entonces, los idempotentes primitivos de $\mathbb{F}_q G$ son*

$$\frac{1+t}{2}e_i \text{ y } \frac{1-t}{2}e_i,\ 0 \leq i \leq n.$$

Demostración. Probaremos cada una de las afirmaciones.

I) Como $A = \langle a^2 \rangle = \left\{1, a^2, a^4, \ldots, a^{2(p^n-1)}\right\}$, es claro que $C \cap A = \{1\}$. Además, si $g \in G$, entonces $g = a^x$ y dado que 2 y p^n son primos relativos existen enteros s, r tales que $x = 2s + rp^n$; luego $g = a^x = a^{2s}a^{rp^n}$ y por lo tanto $g \in CA$.

II) Por el Corolario 3.3.13 tenemos que $\frac{1+t}{2}$ y $\frac{1-t}{2}$ son los idempotentes primitivos de $\mathbb{F}_q C$. Por otro lado, como q es generador de $U(2p^n)$ y $p^n \mid 2p^n$ tenemos por el Lema 3.3.8 que q es generador de $U(p^n)$ y por tanto los e_i del Lema 3.3.12 son los idempotentes primitivos de $\mathbb{F}_q A$.

El hecho de que $\frac{1+t}{2}e_i$ y $\frac{1-t}{2}e_i$ sean idempotentes ortogonales se sigue de lo anterior y de que $\mathbb{F}_q G$ es un anillo conmutativo. Veamos que la suma de estos idempotentes es 1.

$$\sum_{i=0}^{n} \frac{1+t}{2}e_i + \sum_{i=0}^{n} \frac{1-t}{2}e_i = \sum_{i=0}^{n}(\frac{1+t}{2} + \frac{1-t}{2})e_i = \sum_{i=0}^{n} e_i = 1.$$

Como $\mathbb{F}_q G$ tiene $2(n+1)$ componentes simples y tenemos $2(n+1)$ idempotentes ortogonales cuya suma es 1 concluimos que dichos idempotentes son los primitivos.

□

Bibliografía

BELK, James. *Classification of Finite Fields*. URL: https://e.math.cornell.edu/people/belk (vid. pág. 24).

FERRAZ Raul y POLCINO, Cesar. "Idempotents in group algebras and minimal abelian codes". En: *Finite Field and Their Applications* 13.2 (2007), págs. 382-393 (vid. págs. 8, 9).

FRALEIGH, Jhon. *A First Course in Abstract Algebra*. Addison-Wesley, 2003 (vid. pág. 17).

GALLIAN, Joseph. *Contemporary Abstract Algebra*. 8.ª ed. Brooks/Cole, Cengage Learning (vid. pág. 19).

HACHENBERGER Dirk y JUNGNICKEL, Dieter. *Topics in Galois Fields*. Algoritms y Computation in Mathematics, Springer, 2020 (vid. pág. 24).

HOFFMAN Kenneth y KUNZE, Ray. *Linear Algebra*. Prentice-Hall (vid. págs. 80, 82).

JIMENEZ Luis, GORDILLO Jorge y RUBIANO Gustavo. *Teoría de números [para principiantes]*. Facultad de Ciencias, Universidad Nacional de Colombia, Sede Bogotá, 2004 (vid. pág. 20).

LIDL Rudolf y NIEDERREITER, Harald. *Introduction to finite fields and their applications*. New York Cambridge University Press, 2002 (vid. pág. 24).

LING San y XING, Chaoping. *Coding Theory: A First Course*. Cambridge University Press, 2004 (vid. pág. 59).

MARTIN, Paulo. *Grupos, Corpos e Teoria de Galois*. Editora Livraria de Fisica, 2010 (vid. pág. 73).

POLCINO, Cesar. “Group algebras and coding theory: a short survey”. En: *Revista de Integración, Escuela de Matemáticas, Universidad Industrial de Santander* 37.1 (2019), págs. 153-166 (vid. pág. 59).

POLCINO Cesar y SEHGAL, Sudarshan. *An Introduction to Group Rings*. Kluwer Academic Publishers, Dortrecht, 2002 (vid. págs. 67, 87, 89, 91).

SPINDLER, Karlheinz. *Abstract Algebra with Applications. Volume 2: Rings and Fiels*. Chapman, Hall/CRC Pure y Applied Mathematics, 1993 (vid. págs. 17, 36).

A. Operadores Lineales

En este apéndice revisaremos algunas nociones y resultados sobre operadores lineales en un espacio vectorial de dimensión finita que utilizamos en la demostración del teorema de la base normal.

Definición A.0.1. Un **operador lineal** es una transformación lineal $\mathrm{T} : V \to V$ donde V es un espacio vectorial sobre un cuerpo $\mathbb{K}$.

Si n es un entero positivo, denotamos por T^n a la composición del operador lineal T consigo mismo n veces y por T^0 al operador identidad I en V. Si $\alpha \in V$, escribimos $\mathrm{T}\,\alpha$ en vez de $\mathrm{T}(\alpha)$. El conjunto de todos los operadores lineales en V es denotado por $\mathcal{L}(V)$ y es un espacio vectorial sobre $\mathbb{K}$ con las siguientes operaciones:

$$(\mathrm{T}_1 + \mathrm{T}_2)(\alpha) = \mathrm{T}_1(\alpha) + \mathrm{T}_2(\alpha) \text{ con } \mathrm{T}_1, \mathrm{T}_2 \in \mathcal{L}(V) \text{ y } \alpha \in V$$

$$(c\,\mathrm{T}_1)(\alpha) = c\,\mathrm{T}_1(\alpha) \text{ con } \mathrm{T}_1 \in \mathcal{L}(V), c \in \mathbb{K}, \text{ y } \alpha \in V$$

Por otra parte, si $g(x) = a_n x^n + \cdots + a_1 x + a_0 \in \mathbb{K}[x]$, entonces el operador lineal $a_n\,\mathrm{T}^n + \cdots + a_1\,\mathrm{T} + a_0\,\mathrm{I}$ es denotado por $g(\mathrm{T})$.

Supongamos que V es un espacio de dimensión finita n y sea β una base para V. Recordemos que se denota por $[\mathrm{T}]_\beta$ a la matriz de T relativa β. Si β' es otra base para V, se puede probar que las matrices $[\mathrm{T}]_\beta$ y $[\mathrm{T}]_{\beta'}$ son similares, es decir, existe una matriz invertible P de tamaño $n \times n$ tal que $[\mathrm{T}]_\beta = P^{-1}\,[\mathrm{T}]_{\beta'}\,P$. No es difícil ver que el polinomio característico de dos matrices similares es el mismo, por lo que tenemos la siguiente definición.

Definición A.0.2. Sea T un operador lineal en un espacio vectorial V de dimensión finita. El polinomio $g(x) = \det(xI - A)$ es llamado el **polinomio característico** de T donde A es la matriz de T relativa alguna base β de V.

Es importante tener en cuenta que si la dimensión de V es n, entonces el polinomio característico de T es mónico y de grado n.

Definición A.0.3. Sean T un operador lineal en un espacio vectorial V sobre un cuerpo $\mathbb{K}$ y $g(x) \in \mathbb{K}[x]$, decimos que g **anula** a T si el operador lineal $g(\mathrm{T}) = 0$ donde 0 es el operador nulo.

Es claro que el polinomio nulo anula a cualquier operador T. Ahora, si $f, g \in \mathbb{K}[x]$ anulan a T entonces el polinomio $f - g$ también lo anula y si $h \in \mathbb{K}[x]$, fh anula a T. Luego, la colección de todos los polinomios sobre $\mathbb{K}$ que anulan al operador lineal T es un ideal de $\mathbb{K}[x]$. En general no se puede garantizar que existe algún polinomio no nulo que anule a T. Sin embargo, en espacios de dimensión finita si se puede garantizar. En efecto, si V es un espacio de dimensión finita n, entonces $\mathcal{L}(V)$ es un espacio de dimensión n^2. Por lo tanto, los operadores $\mathrm{I}, \mathrm{T}, \ldots, \mathrm{T}^{n^2}$ son linealmente dependientes y así existen escalares $a_0, a_1, \ldots, a_{n^2} \in \mathbb{K}$ no todos nulos tal que $a_{n^2}\,\mathrm{T}^{n^2} + \cdots + a_1\,\mathrm{T} + a_0\,\mathrm{I} = 0$; luego el polinomio $g(x) = a_{n^2}x^{n^2} + \cdots + a_1 x + a_0$ anula a T. Además, como $\mathbb{K}[x]$ es un dominio de ideales principales tenemos que el ideal de los polinomios en $\mathbb{K}[x]$ que anulan al operador T es generado por un polinomio no nulo de grado mínimo en dicho ideal.

Definición A.0.4. Sea T un operador lineal en un espacio vectorial V de dimensión finita. El único polinomio mónico de grado mínimo que anula a T es llamado el **polinomio minimal** de T.

De esta forma el polinomio minimal de T, divide a cualquier otro polinomio que anula a este operador.

Teorema A.0.5. *(Teorema de Cayley-Hamilton). Sea T un operador lineal en un espacio vectorial V de dimensión finita. Entonces el polinomio característico de T anula a este operador.*

Demostración. Ver [12], página 194. □

Definición A.0.6. Sean T un operador lineal en un espacio vectorial V y $\alpha \in V$, el subespacio de V generado por los vectores $\mathrm{T}^k\,\alpha$ con $k \geq 0$ es denotado por $Z(\alpha, \mathrm{T})$.

De la definición de $Z(\alpha, \mathrm{T})$, es claro que dicho subespacio consiste de todos los vectores de la forma $g(\mathrm{T})\alpha$ con $g \in \mathbb{K}[x]$. Si $Z(\alpha, \mathrm{T}) = V$, decimos que α es un **vector cíclico** para T. Por otro lado, la colección de todos los polinomios g en $\mathbb{K}[x]$ tal que $g(\mathrm{T})\alpha = 0$ es también un ideal no nulo en $\mathbb{K}[x]$ puesto que contiene al polinomio minimal del operador T. El único polinomio mónico que genera este ideal es llamado el T**-anulador** de α y se denota por p_α.

Teorema A.0.7. *Sean T un operador lineal en un espacio vectorial V de dimensión finita, α cualquier vector no nulo y p_α su T-anulador. Entonces:*

---

[12] Ray HOFFMAN Kenneth y KUNZE. *Linear Algebra*. Prentice-Hall.

I) *Si n es el grado de p_α, entonces los vectores $\alpha, \mathrm{T}\,\alpha, \mathrm{T}^2\,\alpha, \ldots, \mathrm{T}^{n-1}\,\alpha$ forman una base para $Z(\alpha, \mathrm{T})$ y por tanto el grado de p_α es igual a la dimensión del subespacio $Z(\alpha, \mathrm{T})$.*

II) *Si U es la transformación lineal que se obtiene al restringir al operador T a $Z(\alpha, \mathrm{T})$, entonces U es un operador lineal en $Z(\alpha, \mathrm{T})$ cuyo polinomio minimal es p_α.*

Demostración. Probaremos cada una de las afirmaciones.

I) Sea $\beta \in Z(\alpha, \mathrm{T})$, entonces existe un polinomio $g \in \mathbb{K}[x]$ tal que $\beta = g(\mathrm{T})\alpha$. Por el algoritmo de la división para $\mathbb{K}[x]$ tenemos que existen $q(x), r(x) \in \mathbb{K}[x]$ tal que $g(x) = p_\alpha(x)q(x) + r(x)$ con $r(x) = 0$ o $\partial r(x) < n$. Como $p_\alpha(\mathrm{T})\alpha = 0$ concluimos que $g(\mathrm{T})\alpha = r(T)\alpha$. Además, si escribimos $r(x) = a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$ vemos que $\beta = r(\mathrm{T})\alpha = a_{n-1}\,\mathrm{T}^{n-1}\,\alpha + \cdots + a_1\,\mathrm{T}\,\alpha + a_0\alpha$. Lo que muestra que los vectores $\alpha, \mathrm{T}\,\alpha, \mathrm{T}^2\,\alpha, \ldots, \mathrm{T}^{n-1}\,\alpha$ generan $Z(\alpha, \mathrm{T})$. Nos falta ver que dichos vectores son linealmente independientes. Para esto sean $b_0, b_1, b_2 \ldots, b_{n-1} \in \mathbb{K}$ tal que $b_0\alpha + b_1\,\mathrm{T}\,\alpha + b_2\,\mathrm{T}^2\,\alpha + \cdots + b_{n-1}\,T^{n-1}\alpha = 0$. Si alguno de estos escalares es distinto de cero entonces el polinomio $h(x) = b_{n-1}x^{n-1} + \cdots + b_2x^2 + b_1x + b_0$ cumple que $h(T)\alpha$ lo que contradice la propiedad minimal de p_α.

II) Si $\beta \in Z(\alpha, \mathrm{T})$ y escribimos $\beta = a_m\,\mathrm{T}^m\,\alpha + \cdots + a_1\,\mathrm{T}\,\alpha + a_0\alpha$ entonces $\mathrm{U}(\beta) = \mathrm{T}(\beta) = a_m\,\mathrm{T}^{m+1}\,\alpha + \cdots + a_1\,\mathrm{T}^2\,\alpha + a_0\,\mathrm{T}\,\alpha \in Z(\alpha, \mathrm{T})$ y así U es un operador lineal en $Z(\alpha, \mathrm{T})$. Sea $g \in \mathbb{K}[x]$, entonces:

$$\begin{aligned} p_\alpha(\mathrm{U})g(\mathrm{T})\alpha &= p_\alpha(\mathrm{T})g(\mathrm{T})\alpha \\ &= g(\mathrm{T})p_\alpha(\mathrm{T})\alpha \\ &= g(\mathrm{T})0 \\ &= 0. \end{aligned}$$

Finalmente, si $h \in \mathbb{K}[x]$ es un polinomio cuyo grado es menor que el de p_α tal que $h(\mathrm{U}) = 0$ entonces $h(\mathrm{U})\alpha = h(\mathrm{T})\alpha = 0$ lo que contradice la propiedad minimal de p_α. Luego, p_α es el polinomio minimal del operador U.

□

Observación A.0.8. Una consecuencia inmediata del teorema anterior es que si α es un vector ciclíco para T entonces el polinomio minimal y característico de T tienen el mismo

grado. Como ambos polinomios son mónicos y el polinomio minimal divide al polinomio característico, concluimos que son iguales.

Definición A.0.9. Sea V un espacio de dimensión finita. Sean $W_1, W_2, \ldots, W_k$ subespacios de V y $W = W_1 + W_2 + \cdots + W_k$. Decimos que $W_1, W_2, \ldots, W_k$ son **independientes** si $\alpha_1 + \alpha_2 + \cdots + \alpha_k = 0$ con $\alpha_i \in W_i$ implica que $\alpha_i = 0$, para todo $i \in \{1, \ldots, k\}$. En esta caso decimos que W es la **suma directa** de $W_1, W_2, \ldots, W_k$ y escribimos $W = W_1 \oplus W_2 \oplus \cdots \oplus W_k$.

Definición A.0.10. Sea V un espacio vectorial y T un operador lineal en V. Si W es un subespacio de V, decimos que W es **invariante bajo** T si para cada vector $\alpha \in W$, el vector $\mathrm{T}\,\alpha \in W$.

Definición A.0.11. Sea T un operador lineal en un espacio vectorial V y sea W un subespacio de V. Decimos que W es T**-admisible** si:

I) W es invariante bajo T.

II) Si $f(\mathrm{T})\beta \in W$, entonces existe un vector $\gamma \in W$ tal que $f(\mathrm{T})\beta = f(\mathrm{T})\gamma$.

Teorema A.0.12. *(Teorema de Descomposición Cíclica). Sea T un operador lineal en un espacio V de dimensión finita y sea W_0 un subespacio propio T-admisible. Entonces existen vectores no nulos $\alpha_1, \ldots, \alpha_r \in V$ con sus respectivos T-anuladores $p_1, \ldots, p_r$ tal que:*

I) $V = W_0 \oplus Z(\alpha_1, \mathrm{T}) \oplus \cdots \oplus Z(\alpha_r, \mathrm{T})$

II) p_k divide p_{k-1} con $k = 2, \ldots, r$

Demostración. Ver [12], página 233. □

Teorema A.0.13. *Sea T un operador lineal en un espacio de dimensión finita V. Entonces T tiene un vector cíclico si, y solo si, el polinomio característico y minimal de T son iguales.*

Demostración. En la Observación A.0.8 mostramos que si T tiene un vector cíclico, entonces el polinomio característico y minimal de T son iguales. Para mostrar la recíproca de la implicación anterior, mostraremos primero que existe un vector $\alpha \in V$ tal que el T-anulador de α es el polinomio minimal de T. Si $V = 0$, no hay nada que mostrar. Ahora,

si $V \neq 0$, tome $W = 0$. Por el Teorema A.0.12 existen vectores no nulos $\alpha_1, \ldots, \alpha_r \in V$ tal que:

$$V = Z(\alpha_1, \mathrm{T}) \oplus \cdots \oplus Z(\alpha_r, \mathrm{T}),$$

donde $p_1, \ldots, p_r$ son los T-anuladores y $p_k \mid p_{k-1}$ con $k = 2, \ldots, r$. Veamos que p_1 es el polinomio minimal de T. Sea $\alpha = b_1 + b_2 + \cdots + b_r$ donde $b_i \in Z(\alpha_i, \mathrm{T})$, entonces:

$$p_1(T)\alpha = p_1(T)b_1 + p_1(T)b_2 + \cdots + p_1(T)b_r.$$

Como p_i es el polinomio minimal de $\mathrm{U_i} : Z(\alpha_i, \mathrm{T}) \to Z(\alpha_i, \mathrm{T})$, $p_i(\mathrm{T})b_i = 0$ pero como $p_i \mid p_1$, $p_1(\mathrm{T})b_i = 0$. Lo que muestra que $p_1(\mathrm{T})\alpha = 0$. Así, p_1 es un polinomio mónico que anula a T. Si $f(x)$ es un polinomio que anula T, entonces f anula al operador U_1 lo que implica que el grado de p_1 es menor o igual que el de f y por tanto p_1 es el polinomio minimal de T.

Ahora, si suponemos que el polinomio minimal y característico de T son iguales. Por lo anterior, sabemos que existe $\alpha \in V$ tal que el grado p_α es igual a la dimensión del espacio V y así por el ítem I) del Teorema A.0.7 $Z(\alpha, \mathrm{T})$ es un subespacio de igual dimensión que el espacio V; luego $V = Z(\alpha, \mathrm{T})$. □

B. Anillos Semisimples

La semisimplicidad de un álgebra de grupo juega un papel fundamental para hallar sus ideales minimales. Por tal motivo, en este apéndice se encuentra en detalle los preliminares necesarios para entender algunos conceptos y resultados usados en el Capítulo 4.

Definición B.0.1. Sea R un anillo y $(M,+)$ un grupo abeliano. Decimos que M es un R**-módulo** si existe una función $R \times M \to M$, denotada por $(r,m) \longmapsto rm$ tal que:

I) $(r_1 + r_2)m = r_1 m + r_2 m$;

II) $r(m_1 + m_2) = rm_1 + rm_2$;

III) $(r_1 r_2)m = r_1(r_2 m)$.

para todos $m_1, m_2 \in M$ y todos $r_1, r_2 \in R$.

Si R tiene 1_R y vale $1_R m = m$, para todo $m \in M$ decimos que M es un **R-módulo unitario**. En adelante, todos los anillos tendrán unidad y todos los módulos serán unitarios.

Ejemplo B.0.2. I) Sea R un anillo, entonces R es un módulo sobre si mismo.

II) Sea $(G,+)$ un grupo abeliano. Entonces G es un $\mathbb{Z}$-módulo vía: $\mathbb{Z} \times G \to G$ donde

$$(n,g) \longmapsto ng = \begin{cases} \underbrace{g + \cdots + g}_{n \text{ veces}} & \text{si } n > 0; \\ 0_G & \text{si } n = 0; \\ \underbrace{(-g) + \cdots + (-g)}_{-n \text{ veces}} & \text{si } n < 0. \end{cases}$$

Definición B.0.3. Sea M un R-módulo y $N \subseteq M$. Decimos que N es un **submódulo** de M si N es un subgrupo abeliano de M y si dados $r \in R$ y $n \in N$, $rn \in N$. Esto se denotará por $N \leq M$.

Ejemplo B.0.4. Sea R un anillo y considere a R como un R-módulo. Entonces I es submódulo de R si, y solo si, I es un ideal a izquierda de R.

Definición B.0.5. Sea M un R-módulo y sean $m_1, \ldots, m_k \in M$. El módulo generado por $m_1, \ldots, m_k$ se denota por $\langle m_1, \ldots, m_k \rangle$ y es

$$\langle m_1, \ldots, m_k \rangle = \{r_1 m_1 + \ldots r_k m_k \mid r_1, \ldots, r_k \in R\}.$$

Además, decimos que $N \leq M$ es **finitamente generado** si existen $m_1, \ldots, m_k \in M$ tales que $N = \langle m_1, \ldots, m_k \rangle$. En el caso donde $N = \langle m \rangle$ decimos que N es el **módulo cíclico** generado por m.

Ejemplo B.0.6. Sea R un anillo. Entonces R es un R-módulo cíclico pues $R = \langle 1_R \rangle$.

Definición B.0.7. Sea M un R-módulo. Decimos que M es **simple** si $\{0\}$ y M son sus únicos submódulos.

Sea M un R-módulo y $\{M_i\}_{i \in I}$ una familia de submódulos, definimos

$$\sum_{i \in I} M_i = \left\{ \sum_{i \in I} m_i \ \mid \ (m_i)_{i \in I} \text{ tiene soporte finito} \right\},$$

donde $supp(m_i) = \{i \in I \mid m_i \neq 0\}$.

Proposición B.0.8. *Si $\{M_i\}_{i \in I}$ es una familia de submódulos de un módulo M, entonces $\sum_{i \in I} M_i$ es un submódulo de M.*

Demostración. Sean $\sum_{i \in I} m_i$ y $\sum_{i \in I} n_i$ en $\sum_{i \in I} M_i$. Es fácil ver que:

I) $supp((m_i) + (n_i)) \subseteq supp(m_i) \cup supp(n_i)$;

II) $supp(-m_i) = supp(m_i)$;

III) $supp(r m_i) \subseteq supp(m_i)$, para cualquier $r \in R$.

Luego, como $(m_i)_{i \in I}$ y $(n_i)_{i \in I}$ tienen soporte tenemos por el ítem I) que $(m_i)_{i \in I} + (n_i)_{i \in I}$ tiene soporte finito. Además como cada M_i es submódulo tenemos que $m_i + n_i \in M_i$ para todo $i \in I$ y por lo tanto $(m_i)_{i \in I} + (n_i)_{i \in I} = (m_i + n_i)_{i \in I} \in \sum_{i \in I} M_i$. Ahora, por el ítem II) es claro que $\sum_{i \in I} (-m_i) \in \sum_{i \in I} M_i$ y por el ítem III) tenemos que $r \left(\sum_{i \in I} m_i \right) = \sum_{i \in I} r m_i \in \sum_{i \in I} M_i$. Luego, $\sum_{i \in I} M_i \leq M$. □

Proposición B.0.9. *Sea $\{M_i\}_{i \in I}$ es una familia de submódulos de un módulo M. Entonces, las siguientes condiciones son equivalentes:*

I) *Si* $\sum_{i\in I} m_i = \sum_{i\in I} m_i'$ *en* $\sum_{i\in I} M_i$*, entonces* $m_i = m_i'$*, para todo* $i \in I$*.*

II) *Si* $\sum_{i\in I} m_i = 0_M$*, entonces* $m_i = 0_M$*, para todo* $i \in I$*.*

III) $M_j \cap \left(\sum_{i\in I\setminus\{j\}} M_j\right) = \{0_M\}$*, para todo* $j \in I$*.*

Demostración. Veamos que I) implica II). Supongamos que $\sum_{i\in I} m_i = 0_M = \sum_{i\in I} 0_M$, entonces por I) tenemos que $m_i = 0_M$, para todo $i \in I$. Ahora, probaremos que II) implica III). Fijemos $j \in I$ y sea $x \in M_j \cap \left(\sum_{i\in I\setminus\{j\}} M_j\right)$, entonces $x \in M_j$ y $x = \sum_{i\in I\setminus\{j\}} m_i$ con $m_i \in M_i$, $i \neq j$. Note que $0_M = x - x = \sum_{i\in I} m_i$ con $m_j = -x$ y por II) $x = -m_j = 0_M$.

Finalmente, veamos que III) implica I). Supongamos que $\sum_{i\in I} m_i = \sum_{i\in I} m_i'$ en $\sum_{i\in I} M_i$ y tomemos $j \in I$. Afirmamos que $m_j = m_j'$. En efecto, tenemos que $m_j - m_j' = \sum_{i\in I\setminus\{j\}}(m_i' - m_i) \in M_j \cap \left(\sum_{i\in I\setminus\{j\}} M_j\right) = \{0_M\}$ y por lo tanto $m_j = m_j'$. □

Definición B.0.10. Si $\{M_i\}_{i\in I}$, una familia de submódulos de un módulo M, verifica alguna (y por lo tanto todas) las condiciones de la proposición anterior decimos que la suma $\sum_{i\in I} M_i$ es **directa** y se denota por $\oplus_{i\in I} M_i$.

Ejemplo B.0.11. Sea R un anillo. Consideremos $R^n = R \times \cdots \times R$ como un R-módulo. Afirmamos que $R^n = \oplus_{i=1}^n Re_i$ siendo e_i el vector cuyas componentes son todas nulas excepto en la i-ésima componente donde es 1_R. En efecto, sea $x \in R^n$, entonces $x = (r_1, r_2, \ldots, r_n)$ y por lo tanto $x = r_1e_1 + r_2e_2 + \cdots + r_ne_n \in \sum_{i=1}^n Re_i$. Resta ver que la suma es directa. Tomemos $\sum_{i=1}^n r_ie_i = 0_{R^n}$, entonces $(r_1, r_2, \ldots, r_n) = (0_R, 0_R, \ldots, 0_R)$ y por lo tanto $r_i = 0_R$ que implica que $r_ie_i = 0_{R^n}$.

Definición B.0.12. Un submódulo N de un R-módulo M es llamado un **sumando directo** si existe otro submódulo N' tal que $M = N \oplus N'$.

Definición B.0.13. Un R-módulo M es llamado **semisimple** si todo submódulo de M es un sumando directo.

Mencionaremos a continuación algunas caracterizaciones de la semisimplicidad.

Teorema B.0.14. *Sea* M *un* R*-módulo. Entonces, las siguientes condiciones son equivalentes.*

I) M *es semisimple.*

II) M *es la suma directa de submódulos simples.*

III) M *es la suma (no necesariamente directa) de submódulos simples.*

Demostración. Ver [10], página 92. □

Definición B.0.15. Un anillo R es llamado **semisimple** si R como R-módulo es semisimple.

Note que por el Ejemplo B.0.4 tenemos que R es semisimple si, y solo si, todo ideal a izquierda de R es un sumando directo.

Teorema B.0.16. *Sea R un anillo. Entonces, las siguientes condiciones son equivalentes.*

I) *Todo R-módulo es semisimple.*

II) R *es un anillo semisimple.*

III) R *es la suma directa de un número finito de ideales minimales a izquierda.*

Demostración. Ver [10], página 94. □

Presentamos una caracterización de los anillos semisimples en términos de elementos idempotentes.

Teorema B.0.17. *Sea R un anillo. Entonces R es semisimple si, y solo si, todo ideal a izquierda L de R es de la forma $L = Re$, donde $e \in R$ es un idempotente.*

Demostración. Supongamos que R es semisimple y sea L un ideal a izquierda de R, entonces existe otro ideal a izquierda L' de R tal que $R = L \oplus L'$ y por lo tanto existen $x \in L, y \in L'$ tales que $1_R = x + y$. Entonces $x = 1_R - y$ y multiplicando a izquierda por x tenemos que $x^2 = x - xy$. Note que como L' es un ideal a izquierda de R, $xy \in L'$ y como $x - x^2 = xy \in L$ tenemos que $xy \in L \cap L'$; luego $xy = 0$ y así x es un elemento idempotente. Restar ver que $L = Rx$. Sea $l \in L$,entonces $l = lx + ly$ pero $l = l + 0$ y como la suma es directa tenemos que $lx = l$; luego $l \in Rx$.

Recíprocamente, supongamos que todo ideal izquierdo es de la forma Re con e un elemento idempotente. Veamos que $R = Re \oplus R(1 - e)$. Sea $x \in R$, entonces $x = xe + x - xe$; luego $x \in Re + R(1 - e)$. Finalmente, veamos que la suma es directa. Supongamos que $r_1e + r_2(1 - e) = 0_R$, entonces $r_1e + r_2 - r_2e = 0_R$. Multiplicando a derecha por e y usando que e es idempotente tenemos: $r_1e + r_2e - r_2e = 0_R$. Luego, $r_1e = 0_R$ que implica que $r_2(1 - e) = 0_R$. □

Teorema B.0.18. *Sea $R = \oplus_{i=1}^{t} L_i$ una descomposición de un anillo semisimple como la suma directa de ideales minimales a izquierda. Entonces, existe una famila $\{e_1, \ldots, e_t\}$ de elementos de R tal que:*

I) *$e_i \neq 0$ es un idempotente, $1 \leq i \leq t$.*

II) *Si $i \neq j$, entonces $e_i e_j = 0$.*

III) *$1 = e_1 + \cdots + e_t$.*

IV) *e_i no se puede escribir como $e_i = e_i' + e_i''$ donde e_i', e_i'' son dos idempotentes tales que $e_i', e_i'' \neq 0$ y $e_i' e_i'' = 0$, $1 \leq i \leq t$.*

Recíprocamente, si existe una familia de idempotentes $\{e_1, \ldots, e_t\}$ que satisface las condiciones anteriores, entonces los ideales a izquierda $L_i = Re_i$ son minimales y $R = \oplus_{i=1}^{t} L_i$.

Demostración. Supongamos que R es semisimple y $R = \oplus_{i=1}^{t} L_i$. Entonces existen $e_1, e_2, \ldots, e_t$ tales que $1 = e_1 + e_2 + \cdots + e_t$. Sea $1 \leq i \leq t$, entonces $e_i = e_i^2 + \sum_{k \neq i} e_i e_k$. Note que $\sum_{k \neq i} e_i e_k \in \sum_{k \neq i} L_k$ y como $e_i - e_i^2 = \sum_{k \neq i} e_i e_k \in L_i$ tenemos que $\sum_{k \neq i} e_i e_k \in L_i \cap \sum_{k \neq i} L_k = \{0\}$ y así e_i es idempotente. Sea $i \neq j$, por lo anterior tenemos que $\sum_{k \neq i} e_i e_k = 0$ y como la suma es directa tenemos que $e_i e_j = 0$.

Ahora supongamos que para algún índice i, $e_i = e_i' + e_i''$ donde e_i', e_i'' son dos idempotentes no nulos con $e_i' e_i'' = 0$. Afirmamos que $L_i = Re_i' \oplus Re_i''$. Supongamos que $r_1 e_i' + r_2 e_i'' = 0$, multiplicando a derecha por e_i'' tenemos que $r_1 e_i' e_i'' + r_2 e_i'' = 0$; luego $r_2 e_i'' = 0$ y por lo tanto $r_1 e_i' = 0$. Por otro lado, si $x \in L_i$, como mostramos en el teorema anterior $x = x e_i$ y por lo tanto $x = x e_i' + x e_i''$; luego $x \in Re_i' + Re_i''$. Finalmente, como $e_i = e_i' + e_i''$ tenemos que $e_i' e_i' + e_i' e_i'' \in L_i$. Esto es, $e_i' \in L_i$ y de forma análoga $e_i'' \in L_i$. Lo anterior implica que $Re_i' + Re_i'' \subseteq L_i$ y por lo tanto hemos probado que $L_i = Re_i' \oplus Re_i''$ con $Re_i', Re_i'' \neq 0$, lo que contradice la minimalidad de L_i.

Recíprocamente, supongamos que existe una familia de idempotentes $\{e_1, \ldots, e_t\}$ con las condiciones mencionadas. Veamos que los ideales a izquierda $L_i = Re_i$ son minimales. Supongamos por contradicción que existe $J \subseteq L_i$ un ideal a izquierda tal que $J \neq 0$ y $J \neq L_i$. Como R es semisimple, no es díficil ver que cualquier ideal a izquierda de R visto como R-módulo es semisimple, luego existe J' ideal a izquierda de R contenido en L_i tal que $L_i = J \oplus J'$. Así, existen $x \in J$, $y \in J'$ tal que $e_i = x + y$. Utilizando argumentos

muy similares a los que hemos usado, se puede probar que x, y son idempotentes no nulos cuyo producto es nulo, una contradicción. Resta ver que $R = \oplus_{i=1}^{t} L_i$. El hecho de que $R = \sum_{i=1}^{t} L_i$ se sigue de la condición III). Finalmente, si $r_1e_1 + r_2e_2 + \cdots + r_te_t = 0$ entonces para cualquier $i \in \{1, \ldots, t\}$ tenemos que $r_ie_i + \sum_{k \neq i} e_ke_i = 0$ y por la condición II) concluimos que $r_ie_i = 0$. □

Definición B.0.19. Sea R un anillo, una famila de idempotentes $\{e_1, \ldots, e_t\}$ que satisface las condiciones I), II) y III) es llamada una **familia de idempotentes ortogonales completa**. Un idempotente que satisface las condición IV es llamado **primitivo**.

Dada una descomposición de un anillo semisimple R como la suma directa de ideales minimales a izquierda, podemos agrupar a los ideales a izquierda isomorfos:

$$R = \underbrace{L_{11} \oplus \cdots \oplus L_{1r_1}} \oplus \underbrace{L_{21} \oplus \cdots \oplus L_{2r_2}} \oplus \cdots \oplus \underbrace{L_{s1} \oplus \cdots \oplus L_{sr_s}}$$

Teorema B.0.20. *Con la notación anterior, sea A_i la suma de todos los ideales a izquierda isomorfos a L_{i1}, $1 \leq i \leq s$. Entonces:*

I) *Cada A_i es un ideal bilateral minimal de R.*

II) *$A_iA_j = \{0\}$ si $i \neq j$.*

III) *$R = \oplus_{i=1}^{s} A_i$, donde s es el número de clases isomorfas de ideales minimales a izquierda de R.*

Demostración. Ver [10], página 99. □

Definición B.0.21. Un anillo R es llamado **simple** si sus únicos ideales bilaterales son $\{0\}$ y R.

Corolario B.0.22. *Los ideales A_i definidos en el Teorema B.0.20 son anillos simples.*

Demostración. Como A_i es un ideal minimal bilateral de R, es suficiente mostrar que cualquier ideal bilateral B de A_i es también un ideal bilateral de R. Sea $b \in B$, $r \in R$, entonces podemos escribir $r = x_1 + \cdots + x_s$ con $x_j \in A_j$, $1 \leq j \leq s$. Así, $rb = x_1b + \cdots + x_sb$ y como $x_jb = 0$ si $i \neq j$ tenemos que $rb = x_ib \in B$ ya que B es un ideal bilateral de A_i. Análogamente se muestra que $br \in B$. □

Proposición B.0.23. *Sea $R = \oplus_{i=1}^{s} A_i$ una descomposición de un anillo semisimple R como suma directa de ideales bilaterales minimales. Entonces*

I) *Todo ideal bilateral I de R puede escribirse de la forma $I = A_{i_1} \oplus \cdots \oplus A_{i_t}$, donde $1 \leq i_1 < \ldots < i_t \leq s$.*

II) *Si $R = \oplus_{j=1}^{r} B_j$ es otra descomposición de R como suma directa de ideales bilaterales minimales, entonces $s = r$ y, después de una posible renumeración de índices, $A_i = B_i$ para todo i.*

Demostración. Probaremos cada una de las afirmaciones.

I) Sea I un ideal bilateral de R, entonces $I = \oplus_{i=1}^{s}(A_i \cap I)$. Como $A_i \cap I$ es un ideal bilateral de R contenido en A_i tenemos que $A_i \cap I = \{0\}$ o $A_i \cap I = A_i$ y así $I = A_{i_1} \oplus \cdots \oplus A_{i_t}$, donde $1 \leq i_1 < \ldots < i_t \leq s$.

II) Como cada B_j es minimal y usando el ítem anterior, B_j es igual a algún A_i y recíprocamente.

□

Definición B.0.24. Los únicos ideales bilaterales minimales de un anillo semisimple R son llamadas las **componentes simples** de R.

El siguiente teorema relaciona la descomposición de R como suma directa de ideales bilaterales minimales a una familia de idempotentes.

Teorema B.0.25. *Sea $R = \oplus_{i=1}^{s} A_i$ la descomposición de un anillo semisimple como la suma directa de ideales bilaterales minimales. Entonces, existe una famila $\{e_1, \ldots, e_s\}$ de elementos de R tal que:*

I) *$e_i \neq 0$ es un idempotente central, $1 \leq i \leq s$.*

II) *Si $i \neq j$, entonces $e_i e_j = 0$.*

III) *$1 = e_1 + \cdots + e_s$.*

IV) *e_i no se puede escribir como $e_i = e_i' + e_i''$ donde e_i', e_i'' son dos idempotentes centrales tales que $e_i', e_i'' \neq 0$ y $e_i' e_i'' = 0$,$1 \leq i \leq s$.*

Demostración. Por el Teorema B.0.18 solo falta ver que los elementos e_i son centrales. Sea $x \in R$, entonces $x = xe_1 + \cdots + xe_s = e_1 x + \cdots + e_s x$. Como los A_i son ideales bilaterales tenemos que tanto xe_i como $e_i x$ pertenecen a A_i para todo $i \in \{1, \ldots, s\}$. Teniendo en cuenta que la suma es directa, la representanción es única; luego $xe_i = e_i x$ para todo $i \in \{1, \ldots, s\}$. □

Definición B.0.26. Los elementos $\{e_1, \ldots, e_s\}$ en el teorema anterior son llamados los **idempotentes centrales primitivos** de R.

Teorema B.0.27. *(Teorema Wedderburn-Artin) Un anillo R es semisimple si, y solo si, es la suma directa de álgebras de matrices sobre anillos de división:*

$$R \cong M_{n_1}(D_1) \oplus \cdots \oplus M_{n_s}(D_s)$$

Demostración. Ver [10], Sección 2.6. □