People's Democratic Republic of Algeria

Ministry of Higher Education

and Scientific Research

Uviversity oF Echahid Hamma Lakhdar,El-oued

FACULTY OF EXACT SCIENCES

Academic Master

Domain: Mathematics and Informatics

Sector: Mathematics

Specialty: Fundamental and applied mathematics

Title :

Finite Fields and Their Applications

Presented by :**Maria Ghemam Amara** and **Islam Mesai Belgacem**

Discussed by the jury:

M: Youmbai Reyad	MA(A) University of El-Oued	President
M: Youmbai Ahmed El-Amine	MA(B) University of El-Oued	Examiner
M: Zelaci Hacen	MA(A) University of El-Oued	Rapporteur

Academic year : 2024 – 2025

شكر وتقدير

بسم الله الرحمن الرحيم

الحمد لله الذي بنعمته تتم الصالحات وبتوفيقه تتحق الغايات والصلاة والسلام على خير الأنام رسول الله صلى الله عليه وسلم حيث قال : **لا يشكر اللهَ من لا يشكر الناسَ**

الحمد والشكر لله على نعمه الظاهرة والباطنة وتوفيقنا لانجاز هذه المذكرة

نتوجه بالشكر الجزيل إلى الأستاذ المشرف حسن زلاسي على توجيهاته القيمة وصبره ودعمه المستمر طوال فترة إعداد المذكرة .

كما نتقدم بجزبل الشكر إلى الأساتذة لجنة المناقشة الذين تحملوا عناء قراءة وتفحص المذكرة لتقييم هذا العمل وتقديم ملاحظاتهم

.والشكر موصول إلى عائلتنا التي كانت أكبر داعم ومشجع لنا للوصول إلى هذه المرحلة

ونختم بالدعاء أن يتقبل الله هذا العمل خالصًا لوجهه الكريم ، وأن يجعله نافعًا لطلاب العلم.

Abstract

This thesis aims to analyze finite fields, both theoretically and practically, emphasizing their algebraic structure and their applications in various fields such as cryptography and coding theory. We first introduced the fundamental concepts related to groups, rings, and fields, then we presented finite fields in detail, describing their characteristics and providing concrete examples. Subsequently, we examined key applications such as the design of error-correcting codes and some cryptographic algorithms. The theoretical content is accompanied by practical examples to demonstrate the importance of these structures in applied mathematics.

This project falls within the field of abstract algebra and highlights the significance of finite fields in mathematics and computer science.

Keywords: finite fields, algebra, cryptography, coding theory, applications.

Résumé

Ce mémoire vise à analyser les corps finis, sur le plan théorique et pratique, en soulignant leur structure algébrique et leurs usages dans divers domaines comme la cryptographie et la théorie des codes. Nous avons tout d'abord exposé les concepts fondamentaux relatifs aux groupes, anneaux et corps, ensuite nous avons présenté les corps finis en détaillant leurs caractéristiques et en fournissant des exemples concrets. Par la suite, nous avons examiné des applications fondamentales comme la création de codes de correction d'erreurs et quelques algorithmes de cryptographie. Le contenu théorique est assorti d'exemples pratiques pour démontrer l'importance de ces structures en mathématiques appliquées.

Ce projet s'inscrit dans le domaine de l'algèbre abstraite et souligne l'importance des corps finis en mathématiques et en informatique.

Mots-clés : corps finis, algèbre, cryptographie, théorie des codes, applications.

ملخص

يهدف هذا البحث إلى تحليل الحقول المتنهية، سواء من الناحية النظرية أو العملية، مع تسليط الضوء على بنيتها الجبرية واستخداماتها في مجالات متعددة مثل التشفير ونظرية الأكواد. قدمنا أولاً المفاهيم الأساسية المتعلقة بالمجموعات والحلقات والحقول، ثم فصلنا خصائص الحقول المتنهية مع تقديم أمثلة عملية. بعد ذلك، درسنا تطبيقات أساسية مثل تصميم أكواد تصحيح الأخطاء وبعض خوارزميات التشفير. تم دعم المحتوى النظري بأمثلة تطبيقية لإظهار أهمية هذه البنى في الرياضيات التطبيقية.

يندرج هذا المشروع في مجال الجبر المجرد ويؤكد على أهمية الحقول المتنهية في الرياضيات وعلوم الحاسب.

الكلمات المفتاحية: الحقول المتنهية، الجبر، التشفير، نظرية الترميز، التطبيقات.

Notation and Symbols

$\mathbb{F}_q$	:	Finite field with q elements
$\mathbb{F}_q^*$	:	Multiplicative group of $\mathbb{F}_q$
$\deg(P)$	:	Degree of polynomial P
$\mathbb{Z}/p\mathbb{Z}$	:	Ring of integers modulo prime p
$\mathbb{N}$	:	Natural numbers
$\mathbb{Z}$	:	Integers
$\mathbb{Q}$	:	Rational numbers
$\mathbb{R}$	:	Real numbers
$\mathrm{char}(K)$	:	Characteristic of field K
R/I	:	Quotient ring of R by ideal I
$F[x]$	:	Polynomial ring over field F
$d_H(x, y)$	:	Hamming distance between x and y
$w(x)$	:	Weight of codeword x
$d_{\min}$	:	Minimum Hamming distance
$\cong$	:	Algebraic isomorphism
(a)	:	Ideal generated by element a
$U(R)$	:	Group of units in ring R
$\lvert S\rvert$	:	Cardinality of set S

Contents

General Introduction

FINITE FIELDS are algebraic entities that comprise a limited number of elements. They are viewed as essential in contemporary algebra and have wide-ranging applications across numerous areas like mathematics, computer science, and engineering. The significance of finite fields was initially uncovered through Évariste Galois's contributions in the 19^{th} century and continues to hold importance today.

Finite fields are employed in various theoretical and practical uses, such as cryptography, error-correcting codes, number theory, and beyond. They are robust mathematical instruments utilized to tackle intricate issues that demand exact organization.

This dissertation seeks to examine the fundamental principles of finite fields, emphasizing their relevance in practical and engineering contexts. We will examine their characteristics and internal composition while emphasizing the different contemporary techniques used in their application.

This work is structured into three main chapters as follows:

- **Chapter One:** Covers basic algebraic concepts and foundational structures such as groups, rings, and fields, with a focus on the structure of finite fields.
- **Chapter Two:** Dedicated to the construction of finite fields, their existence proofs, and the study of their main characteristics such as the field's characteristic and its order.
- **Chapter Three:** Focuses on practical applications of finite fields in error-correcting codes (linear/cyclic), with computational examples demonstrating their effectiveness.

The goal of this dissertation is to present a concise overview of finite fields and their main applications.

CHAPTER 1

Foundations of Algebraic Structures

IN THIS CHAPTER, we review the theoretical foundations of algebraic structures by presenting the basic concepts and recalling important related results. We also discuss the fundamental properties of groups, rings, and fields, highlighting the relationships between them, thus laying the groundwork for deeper study of advanced theories and applications.

1.1 Groups

Definition 1.1 *A **group** is a set G equipped with a binary operation $*$ (which can represent multiplication or addition) that satisfies the following four fundamental properties:*

1. ***Closure**: The operation $*$ is closed in G, meaning that for any two elements $a, b \in G$, their product $a * b$ also belongs to G.*

$$\forall a, b \in G, \quad a * b \in G.$$

2. ***Associativity**: The operation is associative, which means that for all elements $a, b, c \in G$, the following equation holds:*

$$(a * b) * c = a * (b * c).$$

3. ***Existence of an Identity Element**: There exists an element $e \in G$ such that for every element*

$a \in G$, performing the operation with e leaves a unchanged:

$$a * e = e * a = a.$$

4. ***Existence of an Inverse Element**: For every element $a \in G$, there exists an element $a^{-1} \in G$ such that applying the operation between them results in the identity element:*

$$a * a^{-1} = a^{-1} * a = e.$$

where e is the identity element.

*A group is called **abelian** (or **commutative**) if, in addition, the operation satisfies the commutative property:*

$$a * b = b * a, \quad \forall a, b \in G.$$

Example 1.1

1. ***Additive Group of Integers** $(\mathbb{Z}, +)$.*
2. ***Multiplicative Group of Nonzero Rationals** $(\mathbb{Q}^*, \times)$.*

1.1.1 Subgroup

Definition 1.2 *(Subgroup) Consider a group $(G, *)$. A nonempty subset H of G is called a **subgroup** of G if H itself forms a group under the same operation $*$ inherited from G.*

The following theorem provides a criterion to determine whether a subset qualifies as a subgroup:

Theorem 1.1 *Let $(G, *)$ be a group, and let H be a nonempty subset of G. Then H is a subgroup of G if and only if the following conditions hold:*

1. ***Closure**: If $x, y \in H$, then $x * y \in H$.*
2. ***Inverses**: If $x \in H$, then $x^{-1} \in H$.*

Example 1.2 *In the additive group $\mathbb{Z}$, the set $n\mathbb{Z} = \{nk \mid k \in \mathbb{Z}\}$ is a subgroup of $\mathbb{Z}$, where n is an arbitrary natural number.*

Proposition 1.1 *(Subgroup Characterization)*

A subset H of a group G qualifies as a subgroup if and only if:

1. *H is nonempty, i.e., $H \neq \emptyset$.*
2. *For every $x, y \in H$, the element xy^{-1} also belongs to H.*

Moreover, if H is a finite set, verifying that it is nonempty and closed under multiplication is sufficient to confirm that it is a subgroup.

1.1.2 Cyclic Group

Definition 1.3 *A group G is called a cyclic group if there exists an element $a \in G$, called a generator, such that every element $b \in G$ can be written as*

$$b = a^j, \quad \text{for some integer } j.$$

In other words, G consists entirely of integer powers of a, and we write

$$G = \langle a \rangle.$$

*If the generator a has **finite order** n, meaning the smallest positive integer satisfying $a^n = e$ (where e is the identity element), then G is called a cyclic group of order n and contains exactly n elements.*
If no such finite n exists, then G is called a cyclic group of infinite order, meaning that G has infinitely many elements.
Note that a cyclic group may have multiple generators. For instance, in the additive group $\mathbb{Z}$, both 1 and -1 serve as generators of the group.

1.2 Rings

Definition 1.4 *A **ring** $(R, +, \times)$ is a set R equipped with two binary operations:*

- ***Addition*** *$(+)$.*
- ***Multiplication*** *$(\times)$.*

satisfying the following axioms:

1. Additive Structure *$(R, +)$ must form an abelian group:*

1. ***Associativity****:* $a + (b + c) = (a + b) + c \quad \forall a, b, c \in R$.
2. ***Additive identity****:* $\exists\, 0 \in R$ *such that* $a + 0 = 0 + a = a \quad \forall a \in R$.
3. ***Additive inverses****:* $\forall a \in R$, $\exists(-a) \in R$ *with* $a + (-a) = 0$.
4. ***Commutativity****:* $a + b = b + a \quad \forall a, b \in R$.

2. Multiplicative Structure

1. ***Associativity****:* $(a \times b) \times c = a \times (b \times c) \quad \forall a, b, c \in R$.

3. Distributive Laws

$$a \times (b + c) = (a \times b) + (a \times c).$$
$$(a + b) \times c = (a \times c) + (b \times c) \quad \forall a, b, c \in R.$$

Example 1.3 *The following are fundamental examples of rings in abstract algebra:*

- ***Integers****:* $(\mathbb{Z}, +, \times)$ *forms a commutative ring with identity.*
- ***Even Integers****:* $(2\mathbb{Z}, +, \times)$ *is a commutative ring without identity.*
- ***Matrices****:* $(M_2(\mathbb{R}), +, \times)$ *constitutes a non-commutative ring with identity.*
- ***Polynomials****:* $(\mathbb{R}[x], +, \times)$ *forms a commutative ring with identity.*
- ***Modular Arithmetic****:* $(\mathbb{Z}/n\mathbb{Z}, +, \times)$ *is a finite commutative ring with identity when* $n > 1$.

Special Types of Rings :

- A **commutative ring** satisfies: $a \times b = b \times a \quad \forall a, b \in R$.
- A **ring with identity** (unital ring) has: $\exists\, 1 \in R$ such that $1 \times a = a \times 1 = a \quad \forall a \in R$.

1.2.1 Subrings

Definition 1.5 *A subset B of a ring A is a **subring** if $B \neq \emptyset$ and B is itself a ring under A's operations.*

Theorem 1.2 *A subset $B \subseteq A$ is a subring of A if and only if $(B, +)$ forms a subgroup of $(A, +)$ and B is closed under the multiplication operation $\times$.*

Example 1.4

- *$2\mathbb{Z}$ is a subring of $\mathbb{Z}$, as is $n\mathbb{Z}$ for any integer n.*
- *The ring $\mathbb{Z}/n\mathbb{Z}$ is not a subring (or a subgroup) of $\mathbb{Z}$ for any $n \geq 2$.*

1.2.2 Ideals

Definition 1.6 *A subset I of A is called a **left ideal** of A if it satisfies the following two conditions:*

1. *I is a subgroup of $(A, +)$.*
2. *For all $x \in I$ and all $a \in A$, the product $xa \in I$.*

*A **right ideal** is defined similarly.*

*We say I is an **ideal** of A if it is both a left ideal and a right ideal.*

Example 1.5

1. *For any natural number n, the set $n\mathbb{Z}$ is an **ideal** of the ring $(\mathbb{Z}, +, \cdot)$, and every ideal of $\mathbb{Z}$ is of the form $n\mathbb{Z}$.*
2. *If A is a ring and a is an element of A, then the set $\{a \cdot x \mid x \in A\}$ is a **left ideal** of A.*

Prime ideals

Definition 1.7 *Let A be a commutative ring. An ideal $I \subseteq A$ is called **prime** if it satisfies:*

$$\forall x, y \in A, \quad x \cdot y \in I \implies x \in I \text{ or } y \in I.$$

Equivalently, I is prime if the quotient ring A/I is an integral domain.

Example 1.6 *In the ring of integers $\mathbb{Z}$:*

- *For any prime number p, the ideal $p\mathbb{Z}$ is prime.*
- *The zero ideal (0) is prime.*
- *No other ideals are prime in $\mathbb{Z}$.*

Theorem 1.3 *Let A be a commutative ring, and let P_1, P_2 be prime ideals of A. For any ideal I of A, the following implication holds:*

$$I \subseteq P_1 \cup P_2 \quad \Longrightarrow \quad I \subseteq P_1 \text{ or } I \subseteq P_2.$$

Proof The proof follows from the prime avoidance lemma. Assume for contradiction that $I \nsubseteq P_1$ and $I \nsubseteq P_2$. Then there exist elements:

$$x \in I \setminus P_1 \quad \text{and} \quad y \in I \setminus P_2.$$

However, $x + y \in I \subseteq P_1 \cup P_2$ leads to a contradiction since:

- If $x + y \in P_1$, then $y = (x + y) - x \in P_1$ (as $x \notin P_1$).
- If $x + y \in P_2$, then $x = (x + y) - y \in P_2$ (as $y \notin P_2$).

Both cases contradict the choice of x and y.

Maximal Ideals

Definition 1.8 *Let A be a commutative ring with multiplicative identity. A proper ideal I of A is called **maximal** if it satisfies either of the following equivalent conditions:*

1. *There exists no proper ideal J such that $I \subsetneq J \subsetneq A$.*
2. *For any ideal J, $I \subseteq J$ implies $J = I$ or $J = A$.*

Theorem 1.4 (Characterization of Maximal Ideals) *For a commutative ring A with identity:*

1. *Every maximal ideal is prime, but not conversely.*

2. *An ideal I is maximal if and only if the quotient ring A/I is a field.*

3. *(Assuming Zorn's Lemma) Every proper ideal is contained in some maximal ideal.*

Principal Ideals

Definition 1.9 *Let R be a ring and $a \in R$. The principal ideal generated by a is defined as:*

$$(a) = \{ra \mid r \in R\}.$$

*That is, the set of all multiples of a by elements of R. An ideal $I \subseteq R$ is called a **principal ideal** if there exists an element $a \in R$ such that $I = (a)$.*

Example 1.7 *Let $\mathbb{F}_3 = \{0, 1, 2\}$ be the finite field with three elements, and consider the polynomial ring $\mathbb{F}_3[x]$. Let $f(x) = x^2 + 1 \in \mathbb{F}_3[x]$, and define the ideal $I = (f(x)) = (x^2 + 1)$, which consists of all multiples of $f(x)$ by polynomials in $\mathbb{F}_3[x]$, i.e.,*

$$I = \{g(x)(x^2 + 1) \mid g(x) \in \mathbb{F}_3[x]\}.$$

*For example, if $g(x) = 1$, then $f(x) = x^2 + 1 \in I$, if $g(x) = x$, then $xf(x) = x^3 + x \in I$; and if $g(x) = x + 2$, then $(x + 2)(x^2 + 1) = x^3 + 2x^2 + x + 2 \in I$. Thus, the ideal I is a **principal ideal** generated by the polynomial $x^2 + 1$.*

*Hence, the ideal I is a **principal ideal** generated by the polynomial $x^2 + 1$.*
This concept is fundamental in constructing finite fields. For example, if $x^2 + 1$ is irreducible over $\mathbb{F}_3$, then the quotient ring:

$$\mathbb{F}_3[x]/(x^2 + 1).$$

is a finite field with $3^2 = 9$ elements.

Factor Ring

Definition 1.10 *Let A be a ring and I an ideal of A. The quotient ring A/I consists of:*

1. ***Equivalence classes** (cosets) modulo I, denoted $a + I$ for $a \in A$.*

2. *Operations defined by:*

$$(a + I) + (b + I) = (a + b) + I.$$
$$(a + I) \cdot (b + I) = (ab) + I.$$

Note: *If the ring A is commutative and I is an ideal of A, then the quotient ring A/I is also commutative.*

Example 1.8 *For every natural number n, the quotient ring $\mathbb{Z}/n\mathbb{Z}$ is:*

- *Commutative.*
- *Unital (with multiplicative identity $\overline{1}$).*
- *Finite (of order n).*

Special cases:

1. *When $n = 1$:*

$$\mathbb{Z}/\mathbb{Z} \cong \{0\}$$

. *This is the zero ring - commutative and finite but* ***not unital*** *(by standard definitions).*

2. *When $n = 0$:*

$$\mathbb{Z}/0\mathbb{Z} \cong \mathbb{Z}$$

. *This is the ring of integers - commutative and unital but* ***not finite****.*

1.2.3 Polynomials rings

Definition 1.11 *Let R be a ring. A polynomial over R is an expression of the form:*

$$f(x) = \sum_{i=0}^{n} a_i x^i = a_0 + a_1 x + \cdots + a_n x^n.$$

where: For a non-negative integer n with coefficients $\alpha_i \in R$ $(0 < i < n)$, x is an indeterminate over R *(a symbol not in R) used to construct polynomials.*

Example 1.9 *Let $\mathbb{F}_3 = \{0, 1, 2\}$ be the finite field with 3 elements. The polynomial ring $\mathbb{F}_3[x]$ consists of all polynomials with coefficients in $\mathbb{F}_3$.*

For example, the polynomial

$$f(x) = 2x^3 + x + 1 \in \mathbb{F}_3[x].$$

is an element of this ring.

Definition 1.12 *(Degree of a Polynomial) The **degree** of a polynomial is the highest power of the variable with a non-zero coefficient.*

Example 1.10 *Consider the polynomial:*

$$f(x) = 4x^5 + 3x^2 + 7.$$

The highest exponent of x with a non-zero coefficient is 5, so:

$$\deg(f(x)) = 5.$$

Special Cases

- If the polynomial is a constant (e.g. $f(x) = 7$), then:

$$\deg(f(x)) = 0.$$

- If the polynomial is the zero polynomial $f(x) = 0$, then:

$$\deg(0) = -\infty \quad \text{(or undefined)}.$$

Theorem 1.5 *(Polynomial Division Algorithm)*

Let F be a field and $F[x]$ its polynomial ring. For any nonzero polynomial $g \in F[x]$ and any polynomial $f \in F[x]$, there exist unique polynomials $q, r \in F[x]$ such that:

$$f = q \cdot g + r.$$

where either $\deg(r) < \deg(g)$ *or* $r = 0$.

Theorem 1.6 *Let* F *be a field. The polynomial ring* $F[x]$ *is a principal ideal domain. Moreover, for every nonzero ideal* $J \neq (0)$ *of* $F[x]$*, there exists a uniquely determined monic polynomial* $g \in F[x]$ *such that* $J = (g)$.

1.2.4 Ring homomorphism

Definition 1.13 *Let* R *and* S *be rings.*

1. *A* ring homomorphism *is a map* $\varphi : R \to S$ *satisfying:*

   (a) $\varphi(a + b) = \varphi(a) + \varphi(b)$ *for all* $a, b \in R$ *(additive group homomorphism).*

   (b) $\varphi(ab) = \varphi(a)\varphi(b)$ *for all* $a, b \in R$ *(multiplicative preservation).*

2. *The* kernel *of* φ*, denoted* $\ker \varphi$*, is the set* $\{a \in R \mid \varphi(a) = 0_S\}$.

3. *A bijective ring homomorphism is called an* isomorphism.

Example 1.11 *The reduction map* $\varphi\colon \mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$, $\varphi(k) = \overline{k}$ *is a surjective ring homomorphism with* $\ker(\varphi) = n\mathbb{Z}$ *and* $\mathrm{Im}(\varphi) = \mathbb{Z}/n\mathbb{Z}$.

Proposition 1.2 *Let* R *and* S *be rings and* $\varphi : R \to S$ *be a ring homomorphism.*

1. *The image of* φ, $\mathrm{Im}(\varphi)$, *is a subring of* S.

2. *The kernel of* φ, $\ker(\varphi)$, *is:*

   - *A subring of* R.
   - *Closed under multiplication by elements from* R *(i.e., for any* $\alpha \in \ker(\varphi)$ *and* $r \in R$*, both* $r\alpha$ *and* αr *belong to* $\ker(\varphi)$*).*

1.3 Fields

Definition 1.14 *A* ***field*** *is a set* $\mathbb{F}$ *containing at least two elements, equipped with two binary operations, denoted by* $\oplus$ *(addition) and* $*$ *(multiplication), that satisfy the following axioms:*

- *The set $\mathbb{F}$, under the operation $\oplus$, forms an **abelian group** with an identity element denoted as 0.*
- *The set $\mathbb{F}^* = \mathbb{F} \setminus \{0\} = \{a \in \mathbb{F} \mid a \neq 0\}$, under the operation $*$, forms an **abelian group** with an identity element denoted as 1.*
- ***Distributive Law:** For all $a, b, c \in \mathbb{F}$, the following holds:*

$$(a \oplus b) * c = (a * c) \oplus (b * c).$$

This structure ensures that both addition and multiplication behave consistently within the field, making it a fundamental algebraic system.

Example 1.12 *The ring $(\mathbb{Z}_p, +, \times)$ forms a commutative field when p is a prime number.*

1.3.1 Subfields

Definition 1.15 *A subset K of a field F is called a subfield of F if K itself is a field with respect to the operations defined on F.*

Theorem 1.7 *A subset K of a field F is a subfield of F if and only if:*

(a) K contains the additive identity (zero) and the multiplicative identity (one) of F.

(b) If $a, b \in K$, then $a + b \in K$ and $ab \in K$ (closed under addition and multiplication).

(c) If $a \in K$, then $-a \in K$ (closed under additive inverses).

(d) If $a \in K$ and $a \neq 0$, then $a^{-1} \in K$ (closed under multiplicative inverses).

Example 1.13 *The field $\mathbb{Q}$ (rational numbers) is a subfield of the field $\mathbb{R}$ (real numbers), and both are subfields of $\mathbb{C}$ (complex numbers).*

1.3.2 Irreducible Polynomials of field

An *irreducible polynomial* is a polynomial that cannot be factored into polynomials of lower degree with coefficients from a given field or ring.

Definition 1.16 *A polynomial $f(x)$ is called **irreducible** over a field F if it cannot be expressed as a product of two non-constant polynomials with coefficients in F. That is, if:*

$$f(x) = g(x)h(x).$$

then either $g(x)$ or $h(x)$ must be a constant polynomial.

Example 1.14 ***Over $\mathbb{R}$ (Real Numbers):***

- *$x^2 + 1$ is irreducible (since it has no real roots).*
- *$x^2 - 4$ is reducible.*

Lemma 1.1 *Let $f \in \mathbb{F}_q[x]$ be an irreducible polynomial over a finite field $\mathbb{F}_q$, and let α be a root of f in some extension field of $\mathbb{F}_q$. Then, for any polynomial $h \in \mathbb{F}_q[x]$, the equation $h(\alpha) = 0$ holds if and only if f divides h.*

Number of Irreducible Polynomials over Finite Fields

The number of monic irreducible polynomials of degree n over a finite field $\mathbb{F}_q$ is given by:

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

where $\mu(d)$ is the Möbius function. This formula guarantees the existence of irreducible polynomials of any degree $\leq n!$ over $\mathbb{F}_q$. Such polynomials are essential in constructing field extensions $\mathbb{F}_q$ and have important applications in areas like coding theory and cryptography.

Lemma 1.2 *Let f be an irreducible polynomial of degree m over the finite field $\mathbb{F}_q$. Then, the polynomial f divides $x^{q^n} - x$ if and only if the degree m is a divisor of n.*
In other words:

$$f \mid (x^{q^n} - x) \iff m \mid n.$$

Theorem 1.8 *For any finite field $\mathbb{F}_q$ and any positive integer $n \in \mathbb{N}$, the polynomial $x^{q^n} - x$ factors exactly into the product of all monic irreducible polynomials over $\mathbb{F}_q$ whose degrees divide n.*

That is:

$$x^{q^n} - x = \prod_{\substack{f \text{ monic irreducible} \\ \deg(f) | n}} f.$$

Example 1.15 *Consider the case when $q = n = 2$. The monic irreducible polynomials over $\mathbb{F}_2[x]$ whose degrees divide 2 are:*

$$x, \quad x+1, \quad \textit{and} \quad x^2 + x + 1.$$

We can verify the factorization:

$$x(x+1)(x^2+x+1) = x^4 + x = x^4 - x \quad \textit{in} \quad \mathbb{F}_2[x].$$

Rabin's Irreducibility Test

Rabin's test is a probabilistic algorithm used to check whether a monic polynomial $f(x) \in \mathbb{F}_q[x]$ of degree n is irreducible. The method relies on the following facts:

- If $f(x)$ is irreducible, then $f(x) \mid x^{q^n} - x$.
- For every proper divisor $d \mid n$, it must hold that $\gcd(f(x), x^{q^d} - x) = 1$.

Test Procedure:

1. Verify that $x^{q^n} \equiv x \mod f(x)$.
2. For all proper divisors $d < n$ of n, check that

$$\gcd(f(x), x^{q^d} - x) = 1.$$

If both conditions hold, then $f(x)$ is declared irreducible with high probability.

Example 1.16 *Let us consider the polynomial $f(x) = x^3 + x + 1 \in \mathbb{F}_2[x]$. We aim to determine its irreducibility using Rabin's test. Since the degree of f is $n = 3$ and the field is $\mathbb{F}_2$, we compute*

$x^{2^3} = x^8 \mod f(x)$. *Using modular exponentiation, we find that* $x^8 \equiv x \mod f(x)$, *which satisfies the first condition of Rabin's test.*

Next, we check all proper divisors of n. *The only proper divisor of 3 is 1, so we compute* $\gcd(f(x), x^{2^1} - x) = \gcd(f(x), x^2 - x)$. *Since this GCD is equal to 1, the second condition is also satisfied.*

Therefore, by Rabin's test, the polynomial $f(x) = x^3 + x + 1$ *is irreducible over* $\mathbb{F}_2$.

Example 1.17 *Consider* $f(x) = (x^2 + x + 1)^2$ *in* $\mathbb{F}_2[x]$ *(degree* $n = 4$*).*

- ***First condition:*** $f(x)$ *divides* $x^{16} - x$ *because its roots lie in* $\mathbb{F}_{16}$.
- ***Second condition:*** *For* $d = 2$, $\gcd(f(x), x^4 - x) = x^2 + x + 1 \neq 1$.

Since the second condition fails, $f(x)$ *is reducible (as expected from its factored form). This shows that Rabin's test correctly detects reducibility even when the first condition holds.*

1.3.3 Field extension

Definition 1.17 *Let* F *be a field. If* F *is a subfield of a field* E, *then we also say that* E *is an* ***extension field*** *of* F. *We may view* E *as a vector space over* F, *and we say that* E *is a* ***finite*** *or* ***infinite*** *extension of* F *according as the dimension of this vector space is finite or infinite.*

Example 1.18 *The field extension* $\mathbb{Q}(\sqrt{2})$ *consists of all numbers of the form* $a + b\sqrt{2}$ *where* $a, b \in \mathbb{Q}$. *This is an* ***algebraic extension*** *because* $\sqrt{2}$ *is a root of the irreducible polynomial* $x^2 - 2$ *over* $\mathbb{Q}$.

Definition 1.18 (Prime Field) *A field that contains no proper subfields (other than itself) is called a* prime field.

Example 1.19 *The finite field* $\mathbb{F}_p$ *(for prime* p*) is a prime field since any subfield containing* 0 *and* 1 *must be closed under addition and thus equal* $\mathbb{F}_p$ *itself.*

Definition 1.19 *Let* K/F *be a field extension. The* degree *of the extension, denoted* $[K : F]$, *is defined as:*

$$[K : F] = \dim_F K,$$

where $\dim_F K$ *represents the dimension of* K *as a vector space over* F. *We classify the extension as:*

- finite *if* $[K : F] < \infty$.
- infinite *otherwise.*

Example 1.20

(1) $\mathbb{Q}(\sqrt{2})/\mathbb{Q}$ *has basis* $\{1, \sqrt{2}\}$*, degree* 2*, with elements* $a + b\sqrt{2}$ $(a, b \in \mathbb{Q})$*.*

(2) $\mathbb{R}/\mathbb{Q}$ *is infinite-dimensional (uncountable basis) with degree* ∞*.*

Proposition 1.3 *Let* $k \subseteq F \subseteq E$ *be fields. Then:*

- $[E : k] = [E : F][F : k]$.
- *If* $\{x_i\}_I$ *is a basis of* F/k *and* $\{y_j\}_J$ *is a basis of* E/F*, then* $\{x_i y_j\}_{IJ}$ *is a basis of* E/k*.*

Proof Let $z \in E$. By hypothesis there exist elements $a_j \in F$, almost all $a_j = 0$, such that

$$z = \sum_{j \in J} a_j y_j.$$

For each $j \in J$ there exist elements $b_{ji} \in k$, almost all of which are equal to 0, such that

$$a_j = \sum_{i \in I} b_{ji} x_i,$$

and hence

$$z = \sum_{j \in J} \sum_{i \in I} b_{ji} x_i y_j.$$

This shows that $\{x_i y_j\}$ is a family of generators for E over k. We must show that it is linearly independent. Let $\{c_{ij}\}$ be a family of elements of k, almost all of which are 0, such that

$$\sum_{j \in J} \sum_{i \in I} c_{ij} x_i y_j = 0.$$

Then for each j,

$$\sum_{i \in I} c_{ij} x_i = 0.$$

because the elements y_j are linearly independent over F. Finally $c_{ij} = 0$ for each i because $\{x_i\}$ is a basis of F over k, thereby proving our proposition.

Proposition 1.4 (Properties of algebraic elements) .

Let K be a field extension of F and let $\alpha \in K$ be algebraic over F.

1. *The minimal polynomial $\min(F, \alpha)$ is irreducible over F.*
2. *For any polynomial $g(x) \in F[x]$, $g(\alpha) = 0$ if and only if $\min(F, \alpha)$ divides $g(x)$.*
3. *If $n = \deg(\min(F, \alpha))$, then:*
   - *The elements $\{1, \alpha, \ldots, \alpha^{n-1}\}$ form a basis for $F(\alpha)$ over F.*
   - $[F(\alpha) : F] = \deg(\min(F, \alpha)) < \infty$.
   - $F(\alpha) = F[\alpha]$.

Example 1.21 (Minimal polynomials and extension degrees) .

1. *$\sqrt[3]{2}$ has minimal polynomial $x^3 - 2$ over $\mathbb{Q}$ (Eisenstein), so $[\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = 3$.*
2. *For prime p, $x^n - p$ is irreducible over $\mathbb{Q}$ (Eisenstein), thus $[\mathbb{Q}(\sqrt[n]{p}) : \mathbb{Q}] = n$.*
3. *$\omega = e^{2\pi i/3}$ has minimal polynomial $x^2 + x + 1$ over $\mathbb{Q}$, hence $[\mathbb{Q}(\omega) : \mathbb{Q}] = 2$.*

Definition 1.20 (Simple Field Extension) *An extension field E of a field F is called a **simple extension** of F if there exists an element $\alpha \in E$ such that $E = F(\alpha)$. In this case, α is said to **generate** the extension E over F.*

Example 1.22 *$\mathbb{Q}(\sqrt{5})/\mathbb{Q}$ is a simple field extension of degree 2, where every element has the form $a + b\sqrt{5}$ with $a, b \in \mathbb{Q}$.*

Theorem 1.9 (Structure of Simple Algebraic Extensions) *Let $E = F(\alpha)$ be a simple extension of a field F, where α is algebraic over F. If the minimal polynomial $\operatorname{irr}(\alpha, F)$ has degree $n \geq 1$, then:*

1. *Every element $\beta \in E$ has a unique representation:*

$$\beta = b_0 + b_1\alpha + \cdots + b_{n-1}\alpha^{n-1},$$

where $b_i \in F$ for $0 \leq i \leq n - 1$.

2. *The set* $\{1, \alpha, \ldots, \alpha^{n-1}\}$ *forms a basis for* E *as a vector space over* F.

Proof Let $E = F(\alpha)$ be a simple algebraic extension of F with $\deg(\text{irr}(\alpha, F)) = n \geq 1$.

1. **Representation of elements:** For the evaluation homomorphism $\phi_\alpha : F[x] \to E$ where $\phi_\alpha(f(x)) = f(\alpha)$, every element $\beta \in E$ has the form:

$$\beta = f(\alpha) \quad \text{for some} \quad f(x) \in F[x].$$

Let $p(x) = \text{irr}(\alpha, F) = x^n + a_{n-1}x^{n-1} + \cdots + a_0$ be the minimal polynomial of α over F. Since $p(\alpha) = 0$, we have:

$$\alpha^n = -a_{n-1}\alpha^{n-1} - \cdots - a_0.$$

This relation allows reduction of any α^m with $m \geq n$ to lower powers. For example:

$$\alpha^{n+1} = \alpha \cdot \alpha^n = -a_{n-1}\alpha^n - \cdots - a_0\alpha.$$

and iteratively substituting higher powers gives expressions in terms of $\{1, \alpha, \ldots, \alpha^{n-1}\}$.

2. **Uniqueness:** Suppose $\beta = b_0 + b_1\alpha + \cdots + b_{n-1}\alpha^{n-1} = c_0 + c_1\alpha + \cdots + c_{n-1}\alpha^{n-1}$. Then:

$$(b_0 - c_0) + (b_1 - c_1)\alpha + \cdots + (b_{n-1} - c_{n-1})\alpha^{n-1} = 0.$$

which implies $b_i = c_i$ for all i by linear independence of $\{1, \alpha, \ldots, \alpha^{n-1}\}$.

Thus, every $\beta \in F(\alpha)$ has a unique representation as:

$$\beta = b_0 + b_1\alpha + \cdots + b_{n-1}\alpha^{n-1} \quad \text{with} \quad b_i \in F.$$

1.3.4 Characteristic of a fields

Definition 1.21 *The* ***characteristic*** *of a field* F*, denoted* $\text{ch}(F)$*, is defined as:*

- *The smallest positive integer* p *such that* $p \cdot 1_F = 0$*, where* 1_F *is the multiplicative identity of* F.

- *If no such p exists, then $\mathrm{ch}(F) = 0$.*

Equivalently, $\mathrm{ch}(F)$ is the generator of the kernel of the canonical ring homomorphism $\mathbb{Z} \to F$ sending $n \mapsto n \cdot 1_F$.

Proposition 1.5 *The characteristic of a field F, denoted $\mathrm{ch}(F)$, satisfies:*

1. *$\mathrm{ch}(F)$ is either 0 or a prime p.*
2. *If $\mathrm{ch}(F) = p$, then for all $\alpha \in F$:*

$$p \cdot \alpha = \underbrace{\alpha + \alpha + \cdots + \alpha}_{p \text{ times}} = 0.$$

Proof Only the first statement requires proof.

1. Assume $\mathrm{ch}(F) = n \neq 0$, where n is the smallest positive integer such that:

$$n \cdot 1 = \underbrace{1 + 1 + \cdots + 1}_{n \text{ times}} = 0$$

2. **Showing n is prime:**
   - Suppose (for contradiction) that n is composite, i.e., $n = ab$ where $1 < a, b < n$.
   - Then:
   $$(a \cdot 1)(b \cdot 1) = (ab) \cdot 1 = n \cdot 1 = 0$$
   - Since F is a field (and has no zero divisors), this implies either $a \cdot 1 = 0$ or $b \cdot 1 = 0$.
   - This contradicts the minimality of n (because $a, b < n$).
3. **The $\mathrm{ch}(F) = 0$ case:**
   - If no positive integer n satisfies $n \cdot 1 = 0$, then $\mathrm{ch}(F) = 0$ by definition.

Remark 1.1 *The concept of characteristic extends naturally to integral domains, where $\mathrm{ch}(R)$ equals the characteristic of its field of fractions.*

Example 1.23 (Characteristics of Common Fields)

1. *The fields $\mathbb{Q}$ and $\mathbb{R}$ both have characteristic 0:*

$$\mathrm{ch}(\mathbb{Q}) = \mathrm{ch}(\mathbb{R}) = 0.$$

   The integral domain $\mathbb{Z}$ also has characteristic 0.

2. *The finite field $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ has characteristic p for any prime p:*

$$\mathrm{ch}(\mathbb{F}_p) = p.$$

Definition 1.22 *The* prime subfield *of a field F is the smallest subfield of F containing the multiplicative identity 1_F. It satisfies:*

$$\textit{Prime subfield} \cong \begin{cases} \mathbb{Q} & \textit{if } \mathrm{ch}(F) = 0. \\ \mathbb{F}_p & \textit{if } \mathrm{ch}(F) = p \textit{ (prime)}. \end{cases}$$

Example 1.24

1. *The prime subfield of both $\mathbb{Q}$ and $\mathbb{R}$ is $\mathbb{Q}$ itself:*

$$\textit{Prime Subfield}(\mathbb{Q}) = \textit{Prime Subfield}(\mathbb{R}) = \mathbb{Q}.$$

2. *The prime subfield of the field $\mathbb{F}_p(x)$ (rational functions over $\mathbb{F}_p$) is isomorphic to $\mathbb{F}_p$, consisting of the constant polynomials:*

$$\textit{Prime Subfield}(\mathbb{F}_p(x)) \cong \mathbb{F}_p.$$

CHAPTER 2

Algebraic Structures of Finite Fields

IN THIS CHAPTER, we study the **algebraic structures** of finite fields, focusing on their *fundamental properties* and *construction methods*, laying the foundation for their various applications.

2.1 Finite fields

Definition 2.1 *A* finite field *is a field that contains a finite number of elements. A finite field with q elements is denoted by $\mathbb{F}_q$.*

Finite fields are also known as Galois fields, *named in honor of Évariste Galois.*

Example 2.1 *Consider the finite field $\mathbb{F}_5$. It contains exactly 5 elements: $0, 1, 2, 3, 4$.*

Addition and multiplication are performed modulo 5. For instance:

$$2 + 4 \equiv 1 \pmod 5, \quad 3 \cdot 4 \equiv 2 \pmod 5.$$

This field satisfies all field properties: every nonzero element has a multiplicative inverse, such as:

$$3 \cdot 2 \equiv 1 \pmod 5 \Rightarrow 3^{-1} \equiv 2 \pmod 5.$$

2.2 Order of Finite Fields

Theorem 2.1 *If $\mathbb{F}$ is a finite field. Then the number of elements in $\mathbb{F}$ is a prime power, i.e.,*

$$|\mathbb{F}| = p^n,$$

where:

- *p is a prime number (the characteristic of $\mathbb{F}$).*
- *$n \geq 1$ is an integer (the degree of the extension over its prime subfield $\mathbb{F}_p$).*

Proof Consider F as a vector space over the finite field $\mathbb{F}_p$, where $\mathbb{F}_p$ is the field with p elements. Since F is a vector space over $\mathbb{F}_p$, it has a certain dimension, say n. This means that there exists a basis for F consisting of n elements, which we denote by:

$$\{\beta_1, \beta_2, \ldots, \beta_n\}.$$

Any element $a \in F$ can be written as a linear combination of the basis vectors $\beta_1, \beta_2, \ldots, \beta_n$, with coefficients from $\mathbb{F}_p$:

$$a = c_1\beta_1 + c_2\beta_2 + \cdots + c_n\beta_n.$$

Here, each coefficient c_i is an element of $\mathbb{F}_p$, and since there are p possible values for each coefficient, there are p^n distinct combinations of these coefficients. Therefore, the total number of distinct elements in F is p^n.

Example 2.2 *Consider the finite field $\mathbb{F}_5$, also written as $\mathrm{GF}(5)$.*
This field contains exactly 5 elements:

$$\mathbb{F}_5 = \{0, 1, 2, 3, 4\}.$$

Arithmetic in $\mathbb{F}_5$ is done modulo 5.
*Thus, the **order** of the field is:*

$$|\mathbb{F}_5| = 5.$$

2.3 Existence and uniqueness of finite fields

Lemma 2.1 *Let F be a finite field with q elements, and let K be a subfield of F. Then, the polynomial $x^q - x \in K[x]$ factors completely in $F[x]$ as:*

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

Moreover, F is the splitting field of $x^q - x$ over K.

Proof We prove both statements:

1. **Complete factorization:**

- For any $a \in F$, if $a = 0$, then clearly $a^q - a = 0$.
- If $a \neq 0$, since the multiplicative group $F^\times$ has order $q - 1$, by Lagrange's theorem we have $a^{q-1} = 1$, and thus $a^q = a$.
- Therefore, every element of F is a root of $x^q - x$.
- Since $\deg(x^q - x) = q$ and we've found q distinct roots, the polynomial must factor completely as shown.

2. **Splitting field:**

- F contains all roots of $x^q - x$ by part (1).
- No proper subfield of F can contain all roots, because any field containing all roots must contain all of F (as F is generated by these roots).
- Therefore, F is the minimal field over K where $x^q - x$ splits completely.

Theorem 2.2 *(Existence and Uniqueness of Finite Fields) For each prime p and each positive integer n, there is a finite field with order $q = p^n$, which serves as the splitting field of $x^q - x$ over $\mathbb{F}_p$. Any two finite fields with the same size are isomorphic.*

Proof **Existence.** For $q = p^n$, consider the polynomial $x^q - x \in \mathbb{F}_p[x]$, and let F be its splitting field over $\mathbb{F}_p$. This polynomial has exactly q distinct roots in F because its derivative is:

$$\frac{d}{dx}(x^q - x) = qx^{q-1} - 1 = -1 \quad (\text{since } q = 0 \text{ in } \mathbb{F}_p),$$

which has no roots and thus shares no common roots with $x^q - x$.

Define the set $S = \{a \in F \mid a^q - a = 0\}$. Then S is a subfield of F because:

1. S contains 0 and 1.
2. For $a, b \in S$, by the *Freshman's Dream* lemma , $(a - b)^q = a^q - b^q = a - b$, so $a - b \in S$.
3. For $a, b \in S$ with $b \neq 0$, $(ab^{-1})^q = a^q b^{-q} = ab^{-1}$, so $ab^{-1} \in S$.

Since $x^q - x$ splits completely in S (as S contains all its roots), we conclude $F = S$. Thus, F is a finite field with q elements.

Uniqueness. Let F be any finite field with $q = p^n$ elements. Then F has characteristic p and contains $\mathbb{F}_p$ as a subfield. By Lemma 2.1, F is the splitting field of $x^q - x$ over $\mathbb{F}_p$.

2.4 Representation of elements of finite fields

Definition 2.2 *(primitive element) An element α in a finite field $\mathbb{F}_q$ that is not zero is termed a* ***primitive element*** *(or* ***generator****) if its multiplicative order equals $q - 1$. In other words, the powers of α produce every nonzero element of $\mathbb{F}_q$:*

$$\mathbb{F}_q^\times = \{1, \alpha, \alpha^2, \ldots, \alpha^{q-2}\},$$

where $\mathbb{F}_q^\times$ represents the multiplicative group associated with the field $\mathbb{F}_q$.

Example 2.3 *The element 3 is a primitive element of $\mathbb{F}_7$ since it generates all nonzero elements:*

$$3^1 = 3,$$
$$3^2 = 2,$$
$$3^3 = 6,$$
$$3^4 = 4,$$
$$3^5 = 5,$$
$$3^6 = 1.$$

Thus, $\mathbb{F}_7^\times = \{1, 3, 2, 6, 4, 5\}$.

Theorem 2.3 *Let $\mathbb{F}_q$ represent a finite field, and let $\mathbb{F}_r$ denote a finite extension field of $\mathbb{F}_q$. Consequently, $\mathbb{F}_r$ constitutes a simple extension field.*

Proof Let α be a primitive element of the finite field $\mathbb{F}_r$ (which exists by the primitive element theorem for finite fields). We immediately have $\mathbb{F}_q(\alpha) \subseteq \mathbb{F}_r$ since $\alpha \in \mathbb{F}_r$ and $\mathbb{F}_q \subseteq \mathbb{F}_r$.

Moreover, since $\mathbb{F}_r$ contains 0 and all powers α^k for $k = 0, 1, \ldots, r-2$ (because α is primitive), it follows that $\mathbb{F}_r$ also contains all linear combinations of these powers with coefficients in $\mathbb{F}_q$. Therefore, $\mathbb{F}_r \subseteq \mathbb{F}_q(\alpha)$, and we conclude that $\mathbb{F}_r = \mathbb{F}_q(\alpha)$.

Theorem 2.4 *Let α be a nonzero element of order d in a finite field $\mathbb{F}_q$. Then the powers of α*

$$\alpha^d = 1, \quad \alpha, \quad \alpha^2, \quad \ldots, \quad \alpha^{d-1},$$

form a cyclic subgroup of order d of the multiplicative group $\mathbb{F}_q^*$.

Proof Let α be a nonzero element of order d in the multiplicative group $\mathbb{F}_q^*$. The set $\langle\alpha\rangle = \{\alpha^k \mid 0 \leq k \leq d-1\}$ forms a cyclic subgroup of $\mathbb{F}_q^*$ since: (1) closure holds as $\alpha^i \cdot \alpha^j = \alpha^{i+j} = \alpha^{(i+j) \bmod d} \in \langle\alpha\rangle$ for all $0 \leq i, j \leq d-1$; (2) associativity is inherited from $\mathbb{F}_q^*$; (3) the identity $1 = \alpha^0 \in \langle\alpha\rangle$; (4) every α^i has an inverse α^{d-i} because $\alpha^i \cdot \alpha^{d-i} = \alpha^d = 1$. The order of $\langle\alpha\rangle$ is exactly d because α has order d, meaning all α^k are distinct for $0 \leq k \leq d-1$ — if $\alpha^i = \alpha^j$ for

some $i < j$, then $\alpha^{j-i} = 1$ with $0 < j - i < d$, contradicting the minimality of d. Thus, $\langle \alpha \rangle$ is a cyclic subgroup of order d generated by α.

Theorem 2.5 *Let $f \in \mathbb{F}_p[x]$ be an irreducible polynomial of degree n. Then the quotient ring $\mathbb{F}_p[x]/(f)$ is isomorphic to the finite field $\mathbb{F}_{p^n}$. That is,*

$$\mathbb{F}_p[x]/(f) \cong \mathbb{F}_{p^n}.$$

Example 2.4 *Let $\mathbb{F}_2$ and $\mathbb{F}_5$ denote finite fields of orders 2 and 5, respectively. Then:*

1. $\mathbb{F}_2[x]/(x^4 + x + 1) \cong \mathbb{F}_{2^4}$,
2. $\mathbb{F}_5[x]/(x^2 + 2) \cong \mathbb{F}_{5^2}$.

2.5 Properties of finite fields

Lemma 2.2 *For each element α within a finite field $\mathbb{F}_q$ containing q elements, it holds that:*

$$\alpha^q = \alpha.$$

Proof

- **Case $\alpha = 0$:** Trivial since $0^q = 0$.
- **Case $\alpha \neq 0$:** $\mathbb{F}_q^*$ is a multiplicative group of order $q - 1$, so by Lagrange's Theorem,

$$\alpha^{q-1} = 1.$$

  Multiplying by α gives $\alpha^q = \alpha$.

Lemma 2.3 *Let F be a finite field that includes a subfield K consisting of q elements. Thus, F contains q^m elements, with $m = [F : K]$ representing the degree of the field extension F over K.*

Proof Let F be a finite field extension of K, where K has q elements. Since F is a finite-dimensional vector space over K with degree $[F : K] = m$, it admits a basis $\{b_1, b_2, \ldots, b_m\}$

over K. Every element $\alpha \in F$ can be uniquely expressed as a linear combination $\alpha = a_1b_1 + a_2b_2 + \cdots + a_mb_m$, where each coefficient $a_i \in K$. Given that each a_i has q possible values (because $|K| = q$), it follows from the multiplication principle that the total number of distinct elements in F is $q \times q \times \cdots \times q = q^m$. Thus, the order of F is q^m.

Theorem 2.6 *Let F be a finite field. Then:*

1. *The characteristic of F is a prime number p.*
2. *The number of elements in F is p^n, where $n = [F : \mathbb{F}_p]$ is the degree of the field extension F over its prime subfield $\mathbb{F}_p$.*

Proof Given that F is a finite field, it necessarily possesses characteristic p for a certain prime p. The prime subfield of F is isomorphic to $\mathbb{F}_p$, and F constitutes a finite-dimensional vector space over this subfield. If the dimension is n, then F contains precisely p^n elements, since each element can be uniquely represented as a linear combination of n basis vectors with coefficients from $\mathbb{F}_p$.

Theorem 2.7 *Let α be a nonzero element of a finite field $\mathbb{F}_q$. Then:*

$$\alpha^{q-1} = 1.$$

Proof

Let $b_1, b_2, \ldots, b_{q-1}$ enumerate all nonzero elements of $\mathbb{F}_q$. For any nonzero $a \in \mathbb{F}_q$, consider the set $\{a \cdot b_1, a \cdot b_2, \ldots, a \cdot b_{q-1}\}$ obtained by multiplying each b_i by a. These products are all nonzero (since a and b_i are nonzero) and distinct (because $a \cdot b_i = a \cdot b_j$ would imply $b_i = b_j$ by cancellation, contradicting the distinctness of the b_i's). Consequently, the two sets $\{b_i\}_{i=1}^{q-1}$ and $\{a \cdot b_i\}_{i=1}^{q-1}$ contain exactly the same elements, possibly reordered. Taking the product of all elements in each set yields the equality $(a \cdot b_1)(a \cdot b_2) \cdots (a \cdot b_{q-1}) = b_1b_2 \cdots b_{q-1}$, which simplifies to $a^{q-1} \cdot (b_1b_2 \cdots b_{q-1}) = b_1b_2 \cdots b_{q-1}$ using the commutativity and associativity of multiplication in $\mathbb{F}_q$. Since the product $b_1b_2 \cdots b_{q-1}$ is nonzero, we may cancel it from both sides to obtain $a^{q-1} = 1$.

Definition 2.3 *Let β be a nonzero element in a finite field $\mathbb{F}_q$. The **order** of β, denoted by $\mathrm{ord}(\beta)$, is the smallest positive integer k such that:*

$$\beta^k = 1.$$

Example 2.5 *The cubic polynomial $1 + x + x^3$ shows irreducibility over $\mathbb{F}_2$ since it has no roots in this field. In the created field $\mathbb{F}_8 = \mathbb{F}_2(\alpha)$, where α denotes a root of $1 + x + x^3$, we derive the essential relation:*

$$\alpha^3 \equiv 1 + \alpha \pmod 2.$$

Theorem 2.8 *Let α be a nonzero element of the finite field $\mathbb{F}_q$. If $n = \mathrm{ord}(\alpha)$ is the order of α, then n divides $q - 1$.*

Proof Suppose $q - 1$ is not divisible by n. Upon dividing $q - 1$ by n, we obtain:

$$q - 1 = kn + r, \quad \text{where } 1 \leq r < n.$$

Then,

$$a^{q-1} = a^{kn+r} = a^{kn} \cdot a^r.$$

Since $a^{q-1} = 1$ and $a^n = 1$, it follows that $a^r = 1$. This contradicts the minimality of n (as the smallest positive integer for which $a^n = 1$). Therefore, n must divide $q - 1$.

For a finite field $\mathbb{F}_q$, we denote by $\mathbb{F}_q^*$ the multiplicative group of nonzero elements of $\mathbb{F}_q$.

Lemma 2.4 *Let $\mathbb{F}_q$ be a finite field with q elements.*

1. *The order $\mathrm{ord}(\alpha)$ divides $q - 1$ for every $\alpha \in \mathbb{F}_q^*$.*
2. *For any two nonzero elements $\alpha, \beta \in \mathbb{F}_q^*$, if $\gcd\big(\mathrm{ord}(\alpha), \mathrm{ord}(\beta)\big) = 1$, then*

$$\mathrm{ord}(\alpha\beta) = \mathrm{ord}(\alpha) \cdot \mathrm{ord}(\beta).$$

Proof

Let $\alpha \in \mathbb{F}_q^*$ be a non-zero element in a finite field. If $\alpha^m = 1$ for some positive integer m, then the order of α divides m. To see this, apply the division algorithm to write $m =$

$a \cdot \text{ord}(\alpha) + b$ where $0 \leq b < \text{ord}(\alpha)$. Then $1 = \alpha^m = \alpha^b$, which by minimality of $\text{ord}(\alpha)$ implies $b = 0$. Hence $\text{ord}(\alpha)$ divides m, and in particular divides $q-1$ since $\alpha^{q-1} = 1$ for all $\alpha \in \mathbb{F}_q^*$.

Now consider $\alpha, \beta \in \mathbb{F}_q^*$ with $\gcd(\text{ord}(\alpha), \text{ord}(\beta)) = 1$. Let $r = \text{ord}(\alpha) \cdot \text{ord}(\beta)$. We have $(\alpha\beta)^r = \alpha^r \beta^r = 1$, showing that $\text{ord}(\alpha\beta)$ divides r. For the reverse divisibility, let $t = \text{ord}(\alpha\beta)$. From $1 = (\alpha\beta)^{t \cdot \text{ord}(\alpha)} = \beta^{t \cdot \text{ord}(\alpha)}$, we conclude that $\text{ord}(\beta)$ divides $t \cdot \text{ord}(\alpha)$. By Euclid's lemma and the coprimality assumption, $\text{ord}(\beta)$ must divide t. Similarly, $\text{ord}(\alpha)$ divides t, and thus r divides t. Therefore $\text{ord}(\alpha\beta) = r = \text{ord}(\alpha) \cdot \text{ord}(\beta)$

Lemma 2.5 *Let $\mathbb{F}$ be a field and p a prime number. For natural numbers k and ℓ and an indeterminate x, the following are equivalent:*

1. $k \mid \ell$ *(k divides ℓ);*
2. $p^k - 1 \mid p^\ell - 1$*;*
3. $x^k - 1 \mid x^\ell - 1$ *in* $\mathbb{F}[x]$.

Theorem 2.9 *(Subfield Criterion) Let p be a prime number and $k, l \in \mathbb{N}$. The following conditions govern subfield relationships between finite fields:*

1. ***Necessary Condition**: For the containment $\mathbb{F}_{p^k} \subseteq \mathbb{F}_{p^l}$ to hold, the divisibility condition $k \mid l$ must be satisfied.*
2. ***Sufficient Condition**: When k divides l, there exists a canonical embedding $\mathbb{F}_{p^k} \hookrightarrow \mathbb{F}_{p^l}$. Furthermore, this subfield is unique - $\mathbb{F}_{p^l}$ contains precisely one subfield of order p^k.*

Proof **(i)** By Proposition 1.3 (Tower Law for Field Extensions), we have:

$$[\mathbb{F}_{p^l} : \mathbb{F}_p] = [\mathbb{F}_{p^l} : \mathbb{F}_{p^k}][\mathbb{F}_{p^k} : \mathbb{F}_p].$$

- The left-hand side is l (since $[\mathbb{F}_{p^l} : \mathbb{F}_p] = l$).
- The second factor on the right-hand side is k (since $[\mathbb{F}_{p^k} : \mathbb{F}_p] = k$).

Thus, $l = [\mathbb{F}_{p^l} : \mathbb{F}_{p^k}] \cdot k$, which implies $k \mid l$.

(ii) If $k \mid l$, then:

1. $p^k - 1 \mid p^l - 1$ (since $k \mid l$),
2. By Lemma 2.5, $x^{p^k-1} - 1$ divides $x^{p^l-1} - 1$, and hence $x^{p^k} - x$ divides $x^{p^l} - x$.

The roots of $x^{p^k} - x$ form a subfield of $\mathbb{F}_{p^l}$ with p^k elements, which is isomorphic to $\mathbb{F}_{p^k}$.

Uniqueness: There cannot be another distinct subfield with p^k elements, because that would imply more than p^k roots of $x^{p^k} - x$ in $\mathbb{F}_{p^l}$, which is impossible since $\mathbb{F}_{p^l}$ is a field and polynomials have a finite number of roots.

2.6 The Galois group of a finite field

Definition 2.4 *Let L/F be a finite field extension. The **Galois group** of L over F, denoted $Gal(L/F)$, is the set of all field automorphisms of L that fix F elementwise:*

$$Gal(L/F) = \left\{ \sigma : L \to L \;\middle|\; \begin{array}{l} \sigma \text{ is an automorphism,} \\ \\ \sigma(a) = a \text{ for all } a \in F \end{array} \right\}.$$

In other words, $Gal(L/F)$ consists of all automorphisms of L that act as the identity on F.

Proposition 2.1 *$(Gal(L/F), \circ)$ forms a group under composition of automorphisms.*

Proof

To prove that $\mathrm{Gal}(L/F)$ forms a group under composition, we verify the group axioms: The set is closed under composition since for any $\sigma, \tau \in \mathrm{Gal}(L/F)$, the composite $\sigma \circ \tau$ is an automorphism of L that fixes F pointwise, as $(\sigma \circ \tau)(a) = \sigma(\tau(a)) = \sigma(a) = a$ for all $a \in F$. Associativity follows immediately from the associativity of function composition. The identity automorphism id_L serves as the group identity, belonging to $\mathrm{Gal}(L/F)$ since it trivially fixes F. Finally, for any $\sigma \in \mathrm{Gal}(L/F)$, its inverse σ^{-1} is also an F-automorphism because $\sigma^{-1}(a) = \sigma^{-1}(\sigma(a)) = a$ for all $a \in F$, demonstrating the existence of inverses. Thus, $\mathrm{Gal}(L/F)$ satisfies all group axioms.

Lemma 2.6 *Suppose $F \subseteq L$ is a finite field extension, and let $\sigma \in \mathrm{Gal}(L/F)$. Then for any polynomial $h \in F[x_1, \ldots, x_n]$ and any elements $\alpha_1, \ldots, \alpha_n \in L$, it holds that:*

$$\sigma\big(h(\alpha_1, \ldots, \alpha_n)\big) = h\big(\sigma(\alpha_1), \ldots, \sigma(\alpha_n)\big).$$

In particular, when $h \in F[x]$ and $\alpha \in L$, we have:

$$\sigma\big(h(\alpha)\big) = h\big(\sigma(\alpha)\big).$$

Proof This follows immediately because σ preserves addition and multiplication and fixes the coefficients of h (which lie in F).

Proposition 2.2 *Assume $F \subseteq L$ is a finite field extension, and let $\alpha_1, \ldots, \alpha_n$ be algebraic over F. Then for every $\sigma \in \mathrm{Gal}(L/F)$, the following properties hold:*

(i) ***(Roots Are Preserved)*** *Suppose $h \in F[x]$ is a nonconstant polynomial and $\alpha \in L$ satisfies $h(\alpha) = 0$. Then $\sigma(\alpha)$ is also a root of h; that is, $h(\sigma(\alpha)) = 0$.*

(ii) ***(Uniqueness via Generators)*** *If L is generated over F by the elements $\alpha_1, \ldots, \alpha_n$, i.e., $L = F(\alpha_1, \ldots, \alpha_n)$, then the automorphism σ is uniquely determined by its values on these generators.*

Proof

(i) By Lemma 2.6, for $h \in F[x]$ and $h(\alpha) = 0$,

$$0 = \sigma(0) = \sigma(h(\alpha)) = h(\sigma(\alpha)).$$

Thus, $\sigma(\alpha)$ is a root of h and lies in L (since $\sigma\colon L \to L$).

(ii) Since $L = F(\alpha_1, \ldots, \alpha_n)$ is a finite extension, every $\beta \in L$ can be written as

$$\beta = h(\alpha_1, \ldots, \alpha_n).$$

for some $h \in F[x_1, \ldots, x_n]$. By Lemma 2.6,

$$\sigma(\beta) = h(\sigma(\alpha_1), \ldots, \sigma(\alpha_n)).$$

Hence, σ is uniquely determined by $\sigma(\alpha_1), \ldots, \sigma(\alpha_n)$.

Corollary 2.1 *Let $F \subseteq L$ be a finite extension. Then the Galois group $Gal(L/F)$ is finite.*

Proof The finite nature of L/F implies that it is algebraic. The degree of the extension L over F is defined as n. The set of all automorphisms of a field L that preserve the structure of a basis over F is uniquely determined by the way they act on the basis elements. The size of the Galois group of the field extension L/F is less than.

Example 2.6

$$\mathbb{Q} \subset L = \mathbb{Q}(\sqrt{2}).$$

The minimal polynomial of $\sqrt{2}$ over $\mathbb{Q}$ is $x^2 - 2$, which has two roots: $\sqrt{2}$ and $-\sqrt{2}$. Both roots are real, and thus both lie in L. Therefore, there are exactly two automorphisms $\sigma \in \mathrm{Gal}(L/\mathbb{Q})$: the identity id, and the map σ such that $\sigma(\sqrt{2}) = -\sqrt{2}$. Hence,

$$\mathrm{Gal}(L/\mathbb{Q}) \cong \mathbb{Z}/2\mathbb{Z}.$$

2.7 The Frobenius automorphism

Theorem 2.10 *Let $\mathbb{F}$ be a finite field with $q = p^n$ elements (where p is prime). The mapping $\phi\colon \mathbb{F} \to \mathbb{F}$ defined by $\phi(x) = x^p$ is an automorphism of $\mathbb{F}$, called the* Frobenius automorphism.

Theorem 2.11 *The period of ϕ is exactly n.*

Proof Suppose the period of ϕ is m where $m < n$. Then for every element $x \in \mathbb{F}_q$, we have:

$$\phi^m(x) = x^{p^m} = x,$$

which implies that all elements of $\mathbb{F}_q$ satisfy the equation:

$$x^{p^m} - x = 0.$$

However, the polynomial $t^{p^m} - t$ has at most p^m roots in its splitting field. Since $\mathbb{F}_q$ contains p^n elements and $m < n$, we have $p^m < p^n$, leading to a contradiction. Therefore, the minimal such m must be n, proving that the period of ϕ is exactly n.

Theorem 2.12 *Let $\mathbb{F}_q$ be a finite field with $q = p^n$ elements, where p is prime. The only automorphisms of $\mathbb{F}_q$ are the powers of the Frobenius automorphism ϕ, i.e., the automorphisms are given by:*

$$1, \phi, \phi^2, \ldots, \phi^{n-1},$$

where $\phi\colon \mathbb{F}_q \to \mathbb{F}_q$ is defined by $\phi(x) = x^p$.

Proof Let $\mathbb{F}_q = \mathbb{F}_p(\alpha)$ for some primitive element α. Then α is a root of an irreducible polynomial of degree n (since $[\mathbb{F}_q : \mathbb{F}_p] = n$). By the properties of the Frobenius automorphism, there are at most n automorphisms of $\mathbb{F}_q$ over $\mathbb{F}_p$.

The maps $1, \phi, \phi^2, \ldots, \phi^{n-1}$ are distinct automorphisms (since they act differently on α). Since they already provide n automorphisms, there cannot be any others. Thus, $\mathrm{Gal}(\mathbb{F}_q/\mathbb{F}_p)$ is cyclic of order n, generated by ϕ.

CHAPTER 3

Applications of finite field

IN THIS CHAPTER, we will examine specific applications of finite fields in modern mathematics and computer science. Finite fields, also known as Galois fields, play a fundamental role in various theoretical and practical domains due to their unique algebraic properties.

3.1 Linear codes

Definition 3.1 *A linear code of length n over $\mathbb{F}_q$ is a subset of $\mathbb{F}_q^n$ that satisfies the subspace property. The dimension of the vector space C over $\mathbb{F}_q$ is equal to the dimension of the linear code C.*

The codewords in set C can be represented as n-dimensional vectors in the field $\mathbb{F}_q$. The words are constructed using the elements of the finite field $\mathbb{F}_q$. The codes we use are not for covert operations, but for error correction. Simply, if we know that part of the message is going to be garbled en route (through a noisy channel), then we would like an encoding and decoding system that protects the original message from the inevitable errors. We require additional machinery.

Definition 3.2 *Given two vectors, *x* and *y*, from the field $\mathbb{F}_q^n$. For the pair of words x and y, each of length n over the alphabet $\mathbb{F}_q$. The Hamming distance, $d(x, y)$, is the number of positions where x*

and y differ. If $x = x_1 \cdots x_n$ and $y = y_1 \cdots y_n$, then

$$d(x, y) = d(x_1, y_1) + \ldots + d(x_n, y_n),$$

where x_i and y_i are elements of $\mathbb{F}_q$ (words of length 1), and

$$d(x_i, y_i) = \begin{cases} 1 & \text{if } x_i \neq y_i \\ 0 & \text{if } x_i = y_i \end{cases}.$$

For a code C containing at least two words, the (minimum) distance *of C, denoted by $d(C)$, is*

$$d(C) = \min\{d(x, y) : x, y \in C, x \neq y\}.$$

Remark 3.1 *The given definition of distance ensures that our code C adheres to the properties of non-negativity, symmetry, and the triangle inequality, indicating that it resides within a metric space.*

Definition 3.3 *The word $\mathbf{x}$ belongs to the set $\mathbb{F}_q^n$. The* (Hamming) weight *of $\mathbf{x}$, denoted by $\mathrm{wt}(\mathbf{x})$, is defined to be the number of nonzero coordinates in $\mathbf{x}$; i.e., $\mathrm{wt}(\mathbf{x}) = d(\mathbf{x}, \mathbf{0})$, where $\mathbf{0}$ is the zero word.*

Consider a scenario where codewords from a code C are transmitted over a noisy channel. Upon receiving a signal x, we will decode it by selecting the codeword that is closest to it, which is our decoding rule. x is decoded to c_x when the distance between x and c_x is the smallest distance among all possible values of c in C.

A decoding error of at least 'd(C)' will result in the decoding rule producing a different codeword. If a code C can handle errors with a bound v, then we say C is v-error-correcting. The proposition in question is presented here, with its proof left to be proven.

Proposition 3.1 *A code C is v-error-correcting if and only if its distance is at least $2v + 1$.*

To understand encoding and decoding, we must first grasp the concept of duality, which will be crucial for decoding.

Definition 3.4 *The orthogonal complement of the subspace C of $\mathbb{F}_q^n$ is the dual code $C^\perp$.*

Theorem 3.1 *If we let C be a linear code of length n over $\mathbb{F}_q$, then $C^\perp$ is a linear code and $\dim(C) + \dim(C^\perp) = n$.*

Enconding and decoding with a linear code

Definition 3.5 *A generator matrix for a linear code C is a matrix G whose rows are linearly independent vectors that span C. The generator matrix $(I_k|X)$ is said to be in standard form, denoted as $(I_k|X)$.*

The dual code $C^\perp$ is generated by the parity-check matrix H of the code C. A matrix of the form $(Y|I_{n-k})$ is called standard if it is in parity-check form.

Theorem 3.2 *If $G = (I_k|X)$ is the standard form generator matrix of a code C with dimension k and length n and distance d (an $[n, k, d]$ code for short), then a parity-check matrix for C is $H = (-X^T|I_{n-k})$.*

Proof The generator matrix H for the dual code $C^\perp$ is a generator matrix for $C^\perp$ if and only if $HG^T = 0$ when G is a generator matrix for C. The rows of H are linearly independent, as we can see by examining the last $n - k$ coordinates. Given that H meets all the criteria, we can conclude that the task is complete.

Let G be the generator matrix of C, where each row of G is the vector r_i from the chosen basis for G. The vector space C has a dimension of k and a length of n. The codeword $v = uG$ is a valid codeword in the code C for any vector u in $\mathbb{F}_q^k$. For every element *v* in set *C*, it can be expressed uniquely as *v = uG*, where *u* is a vector of length *k* from the field *Fq*. For every word u in the finite field $\mathbb{F}_q^k$, its encoding is $v = uG$.

Remark 3.2 *If a linear code C has a generator matrix G in standard form: $G = (I|X)$, then we have an equally simple form for the parity-check matrix H for C:*

$$H = (-X^T|I).$$

Given the codeword $v = uG$, the message u can be recovered by simply extracting the components (u, uX). The codeword $v = uG$ contains the message u in its first k digits. The remaining $n - k$ digits

are termed check digits. The check digits, despite being redundant, are vital for protecting the message from any unwanted alterations.

A code's usefulness depends on the existence of an efficient decoding method. Group theory principles are necessary for this task.

Definition 3.6 *Let C be a linear code of length n over $\mathbb{F}_q$, and let $u \in \mathbb{F}_q^n$ be any vector of length n; we define the* coset *of C determined by u to be the set $C + u = \{v + u : v \in C\} = u + C$.*

This coset coincides with the usual notion from group theory, if we consider $\mathbb{F}_q^n$ as a finite abelian group under addition and a linear code C of length n over $\mathbb{F}_q$ as a subgroup of $\mathbb{F}_q^n$. The proposition on cosets is straightforward to prove, with brief explanations for each part.

Proposition 3.2 *The code C is an $[n, k, d]$ linear code defined over the finite field $\mathbb{F}_q$. Then,*

(i) every vector of $\mathbb{F}_q^n$ is contained in some coset of C;

(ii) for all $u \in \mathbb{F}_q^n$, $|C + u| = |C| = q^k$;

(iii) for all $u, v \in \mathbb{F}_q^n$, $u \in C + v$ implies that $C + u = C + v$;

(iv) two cosets are either identical or they have empty intersection;

(v) there are q^{n-k} different cosets of C;

(vi) for all $u, v \in \mathbb{F}_q^n$, $u - v \in C$ if and only if u and v are in the same coset.

The crucial element for decoding is the final part of the proposition. If the codeword $\mathbf{v}$ is transmitted and the received word $\mathbf{w}$ is received, the error pattern $\mathbf{e}$ is calculated as $\mathbf{e} = \mathbf{w} - \mathbf{v}$, which falls within the error range $\mathbf{w} + C$. According to Proposition 3.2 (vi), the vectors $\mathbf{e}$ and $\mathbf{w}$ are in the same coset. Now, since error patterns of small weight are most likely, we choose a word $\mathbf{e}$ of least weight in the coset $\mathbf{w} + C$ and conclude that $\mathbf{v} = \mathbf{w} - \mathbf{e}$ was the codeword transmitted. The decoding method performs well for small values of n, but becomes increasingly complex as n increases. We will employ syndromes in the context of cyclic codes.

Definition 3.7 *If C is a $[n, k, d]$-linear code over $\mathbb{F}_q$, then H is a parity-check matrix for C. For any vector $\mathbf{w}$ in $\mathbb{F}_q^n$, the syndrome $S_H(\mathbf{w})$ is the vector obtained by taking the transpose of matrix H and multiplying it with $\mathbf{w}$.*

For ease of notation, we assume the parity-check matrix H is in standard form, and omit the suffix H when clarity is not compromised. This proposition is similar in proof to the previous one.

Proposition 3.3 *For a $[n, k, d]$-linear code C over $\mathbb{F}_q$, let H be a parity-check matrix for C. For $u, v \in \mathbb{F}_q^n$, we have*

(i) $S(u + v) = S(u) + S(v)$;

(ii) $S(u) = 0$ *if and only if* u *is a codeword in* C;

(iii) $S(u) = S(v)$ *if and only if* u *and* v *are in the same coset of* C.

Remark 3.3 *The proposition states that a coset can be identified by its syndrome, and that all words within that coset will exhibit the same syndrome. Every coset is associated with a unique syndrome. For a given $n - k$ dimension, the number of syndromes within $\mathbb{F}_q$ is at most q^{n-k}. The number of cosets, given by Proposition 3.2 (v), implies that there are q^{n-k} distinct syndromes. The vectors in $\mathbb{F}_q^{n-k}$ are identifiable as syndromes.*
We will create a syndrome lookup table next. The table identifies the words with the least weight in a coset and assigns them to their respective syndromes. There is more than one way to construct this table, but if we know the distance d of the code C, then we generate all the error patterns $\mathbf{e}$ with $\mathrm{wt}(\mathbf{e}) \leq \lfloor \frac{d-1}{2} \rfloor$. From the definition of distance, and Proposition 3.2, we know that these error patterns $\mathbf{e}$ have to be coset leaders, so then we simply compute the syndrome $S(\mathbf{e})$ for each of these error patterns. Decoding is easily accomplished with this table.

Decoding procedure using Syndromes

Determine the syndrome, S(w), of the received word w. Locate the coset leader **u** within the syndrome look-up table, where the syndrome of **w** matches the syndrome of **u**. The third step involves substituting **w** with **v** by subtracting **u**.

Here's an example to demonstrate this process.

Example 3.1 *Let $q = 2$ and consider the code $C = \{0000, 1011, 0101, 1110\}$. First, we construct a parity-check matrix H. This is straightforward, since the 2nd and 3rd codewords in C form a basis for the code. Therefore, we have:*

$$G = (I|X) = \begin{pmatrix} 1\ 0\ 1\ 1 \\ 0\ 1\ 0\ 1 \end{pmatrix}, \quad H = (-X^T|I) = \begin{pmatrix} 1\ 0\ 1\ 0 \\ 1\ 1\ 0\ 1 \end{pmatrix}.$$

Next, we construct the syndrome look-up table for the code C:

Coset leader $\mathbf{u}$	*Syndrome* $S(\mathbf{u})$
0000	00
0001	01
0010	10
1000	11

The goal is to decode the vector $\mathbf{w}$ *to the representation 1101. The syndrome, represented by* $S(\mathbf{w})$*, is calculated by multiplying the vector* $\mathbf{w}$ *with the transpose of matrix* H *and obtaining a result of 11. The coset leader is 1000 according to our syndrome lookup table. The codeword 1101 - 1000 was the most likely one sent.*

3.2 Cyclic Codes

Cyclic codes form a subclass of linear codes that can be implemented relatively easily and possess a well-understood mathematical structure.

Definition 3.8 *A subset* S *of* $\mathbb{F}_q^n$ *is cyclic if every possible sequence of elements in* S *can be generated from the initial sequence. A code* C *is cyclic if it forms a cyclic set.*

The sequence $(u_{n-r}, \ldots, u_{n-1}, u_0, u_1, \ldots, u_{n-r-1})$ *is the result of cyclically shifting the sequence* $(u_0, \ldots, u_{n-1})$ *to the left by* r *positions.*

In order to convert the combinatorial structure of cyclic codes into an algebraic one, we consider the following map:

$$\pi : \mathbb{F}_q^n \to \mathbb{F}_q[x]/(x^n - 1), \quad (a_0, a_1, \ldots, a_{n-1}) \mapsto a_0 + a_1 x + \cdots + a_{n-1} x^{n-1}. \tag{3.1}$$

It is clear that this is bijective, and from now on we will sometimes identify $\mathbb{F}_q^n$ *with* $\mathbb{F}_q[x]/(x^n - 1)$*, and*

a codeword $\mathbf{u} = (u_0, u_1, \ldots, u_{n-1})$ *with the polynomial* $u(x) = \sum_{i=0}^{n-1} u_i x^i$. *The ring* $\mathbb{F}_q[x]/(x^n - 1))$ *is known to be a ring by the information provided in 1.2. The definition of the word is provided.*

Definition 3.9 *Let* R *be a commutative ring. For simplicity, we assume all rings considered are commutative; we will not discuss noncommutative rings. A nonempty subset* $I \subseteq R$ *is called an ideal if it satisfies:*

(i) Closure under addition and subtraction: $a + b \in I$ *and* $a - b \in I$ *for all* $a, b \in I$.

(ii) Closure under ring multiplication: $r \cdot a \in I$ *for all* $r \in R$ *and* $a \in I$.

Definition 3.10 *An ideal* I *of a ring* R *is called a principal ideal if there exists an element* $g \in I$ *such that* $I = \langle g \rangle$, *where*

$$\langle g \rangle := \{g \cdot r \mid r \in R\}.$$

The element g *is called a generator of* I, *and we say* I *is generated by* g. *A ring* R *is called a principal ideal ring if every ideal in* R *is principal.*

Example 3.2 *In the ring* $\mathbb{F}_3[x]/(x^4 - 1)$, *the subset*

$$I := \{0, 1 + 2x, x + 2x^3, 1 + x + x^2 + x^3\},$$

is an ideal. In fact, it is a ***principal ideal*** *generated by* $I = \langle 1 + 2x \rangle$, *as demonstrated by:*

$$\begin{aligned}
0 \cdot (1 + 2x) &= 0 \\
1 \cdot (1 + 2x) &= 1 + 2x \\
x \cdot (1 + 2x) &= x + 2x^2 \\
x^2 \cdot (1 + 2x) &= x^2 + 2x^3 \\
x^3 \cdot (1 + 2x) &= x^3 + 2x^4 = x^3 + 2 \quad (\textit{since } x^4 \equiv 1)
\end{aligned}$$

By verifying these products, we confirm that every element in I *can be expressed as* $f(x) \cdot (1 + 2x)$ *for some* $f(x) \in \mathbb{F}_3[x]/(x^4 - 1)$.

Theorem 3.3 *Let I be a nonzero ideal in $\mathbb{F}_q[x]/(x^n-1)$ and let $g(x)$ be a nonzero monic polynomial of minimal degree in I. Then:*

1. *$g(x)$ generates I (i.e., $I = \langle g(x) \rangle$).*
2. *$\mathbb{F}_q[x]/(x^n-1)$ is a principal ideal ring.*
3. *$g(x)$ divides $x^n - 1$.*

Proof For any polynomial $f(x) \in I$, polynomial division yields:

$$f(x) = s(x)g(x) + r(x),$$

where $s(x), r(x) \in \mathbb{F}_q[x]$ with $\deg(r(x)) < \deg(g(x))$. Necessarily $r(x) = 0$, since:

$$r(x) = f(x) - s(x)g(x) \in I,$$

and $g(x)$ has minimal degree in I. Thus $I = \langle g(x) \rangle$.

For the divisibility claim, take $f(x) = x^n - 1$ (the zero element in $\mathbb{F}_q[x]/(x^n-1)$), which must satisfy $x^n - 1 = q(x)g(x)$ for some $q(x) \in \mathbb{F}_q[x]$.

This theorem establishes the fundamental connection between cyclic codes and ideals, which will serve as the foundation for our subsequent development.

Theorem 3.4 *Let π be the linear map defined in Equation (3.1). A nonempty subset $C \subseteq \mathbb{F}_q^n$ is a cyclic code if and only if $\pi(C)$ is an ideal of $\mathbb{F}_q[x]/(x^n-1)$.*

Proof ($\Rightarrow$) Suppose $\pi(C)$ is an ideal. For any $\alpha, \beta \in \mathbb{F}_q \subset \mathbb{F}_q[x]/(x^n-1)$ and $\mathbf{a}, \mathbf{b} \in C$, we have:

$$\alpha\pi(\mathbf{a}) + \beta\pi(\mathbf{b}) \in \pi(C) \Rightarrow \pi(\alpha\mathbf{a} + \beta\mathbf{b}) \in \pi(C).$$

Thus $\alpha\mathbf{a} + \beta\mathbf{b} \in C$, showing C is linear.

For $\mathbf{c} = (c_0, \ldots, c_{n-1}) \in C$, consider:

$$\pi(\mathbf{c}) = \sum_{i=0}^{n-1} c_i x^i \in \pi(C).$$

Since $\pi(C)$ is an ideal:

$$x\pi(\mathbf{c}) \equiv c_{n-1} + c_0 x + \cdots + c_{n-2}x^{n-1} \pmod{x^n - 1}.$$

Thus $(c_{n-1}, c_0, \ldots, c_{n-2}) \in C$, proving cyclicity.

($\Leftarrow$) Suppose C is cyclic. For $\mathbf{f} = (f_0, \ldots, f_{n-1}) \in C$:

$$x\pi(\mathbf{f}) \equiv \pi((f_{n-1}, f_0, \ldots, f_{n-2})) \in \pi(C).$$

By induction, $x^i\pi(\mathbf{f}) \in \pi(C)$ for all $i \geq 0$. Since $\pi(C)$ is a linear space, for any $g(x) = \sum_{i=0}^{n-1} g_i x^i$:

$$g(x)\pi(\mathbf{f}) = \sum_{i=0}^{n-1} g_i(x^i\pi(\mathbf{f})) \in \pi(C).$$

Thus $\pi(C)$ is an ideal.

Definition 3.11 *The unique monic polynomial of minimal degree in an ideal I of $\mathbb{F}_q[x]/(x^n - 1)$ is called the* generator polynomial *of I. For a cyclic code C, the generator polynomial of $\pi(C)$ is also called the* generator polynomial *of C.*

Moreover, every monic divisor of $x^n - 1$ in $\mathbb{F}_q[x]$ serves as the generator polynomial for some cyclic code $C \subseteq \mathbb{F}_q^n$.

Corollary 3.1 *There exists a bijective correspondence between:*

- *The set of cyclic codes in $\mathbb{F}_q^n$, and*
- *The set of monic divisors of $x^n - 1$ in $\mathbb{F}_q[x]$.*

Remark 3.4 *The dimension of a cyclic code is completely determined by the degree of its generator polynomial. Specifically, for a cyclic code $C \subseteq \mathbb{F}_q^n$ with generator polynomial $g(x) \in \mathbb{F}_q[x]$, the code dimension is given by:*

$$\dim(C) = n - \deg(g(x)),$$

where n is the code length and $\deg(g(x))$ represents the polynomial degree.

Example 3.3 *The complete factorization of $x^9 - 1$ in $\mathbb{F}_2[x]$ reveals the structure of all possible binary cyclic codes of length 9:*

$$x^9 - 1 = (1 + x)(1 + x + x^4)(1 + x^3 + x^4).$$

From this factorization, we obtain exactly two distinct $[9, 5]$ cyclic codes:

[label=0.,leftmargin=]The cyclic code generated by $g_1(x) = (1 + x)(1 + x + x^4)$:*

$$C_1 = \langle g_1(x) \rangle = \{000000000,\ 111100010,\ 011110001,\ 101111000,$$

$$010111100,\ 001011110,\ 000101111,\ 100010111,$$

$$110001011,\ 111000101\}.$$

The cyclic code generated by $g_2(x) = (1 + x)(1 + x^3 + x^4)$:

$$C_2 = \langle g_2(x) \rangle = \{000000000,\ 101001100,\ 010100110,\ 001010011,$$

$$100101001,\ 110010100,\ 011001010,\ 101100101,$$

$$010110010,\ 001011001\}.$$

Encoding and Decoding of Cyclic Codes

2. **Theorem 3.5** *Let $g(x) = g_0 + g_1 x + \cdots + g_{n-k} x^{n-k}$ be the generator polynomial of a cyclic code $C \subseteq \mathbb{F}_q^n$ with $\deg(g(x)) = n - k$. Then the matrix*

$$G = \begin{pmatrix} g(x) \\ xg(x) \\ \vdots \\ x^{k-1}g(x) \end{pmatrix} = \begin{pmatrix} g_0 & g_1 & \cdots & g_{n-k} & 0 & 0 & 0 & \cdots & 0 \\ 0 & g_0 & g_1 & \cdots & g_{n-k} & 0 & 0 & \cdots & 0 \\ \vdots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \vdots \\ 0 & \cdots & 0 & g_0 & g_1 & \cdots & \cdots & \cdots & g_{n-k} \end{pmatrix},$$

is a generator matrix for C.

Proof The polynomials $\{g(x), xg(x), \ldots, x^{k-1}g(x)\}$ form a basis for C because:

1. They are linearly independent over $\mathbb{F}_q$.
2. They span the code C (since any codeword can be written as $m(x)g(x)$ for some message polynomial $m(x)$ of degree $< k$).
3. The dimension of C is exactly k.

Thus, their corresponding vectors form a generator matrix for C.

Definition 3.12 *Let $h(x) = \sum_{i=0}^{k} a_i x^i$ be a polynomial of degree k ($a_k \neq 0$) over $\mathbb{F}_q$. We define the* reciprocal polynomial $h^R(x)$ *of $h(x)$ by:*

$$h^R(x) := x^k h\left(\frac{1}{x}\right) = \sum_{i=0}^{k} a_{k-i} x^i.$$

Theorem 3.6 *Let $g(x)$ be the generator polynomial of a q-ary $[n, k]$ cyclic code C. Let $h(x) = (x^n - 1)/g(x)$. Then $h_0^{-1} h^R(x)$ is the generator polynomial of the dual code $C^\perp$, where h_0 is the constant term of $h(x)$.*

Proof Let $g(x) = \sum_{i=0}^{n-1} g_i x^i$ and $h(x) = \sum_{i=0}^{n-1} h_i x^i$. The reciprocal polynomial is:

$$h^R(x) = x^{n-k-1} \sum_{i=0}^{n-1} h_{n-i-1} x^i,$$

where $k = \deg(h(x))$.

Consider the product $g(x)h(x) \equiv 0 \pmod{x^n - 1}$. Expanding this gives:

$$\begin{aligned} g(x)h(x) \equiv & (g_0h_0 + g_1h_{n-1} + \cdots + g_{n-1}h_1) \\ & + (g_0h_1 + g_1h_0 + \cdots + g_{n-1}h_2)x \\ & + (g_0h_2 + g_1h_1 + \cdots + g_{n-1}h_3)x^2 \\ & + \cdots \\ & + (g_0h_{n-1} + g_1h_{n-2} + \cdots + g_{n-1}h_0)x^{n-1} \equiv 0. \end{aligned}$$

This implies that each coefficient must be zero. The coefficients show that:

$$\mathbf{g}_i \cdot (h_{n-1}, h_{n-2}, \ldots, h_1, h_0) = 0,$$

for all $i = 0, 1, \ldots, n-1$, where $\mathbf{g}_i$ is the i-th cyclic shift of $(g_0, g_1, \ldots, g_{n-1})$. Therefore, $(h_{n-1}, h_{n-2}, \ldots, h_0)$ is a codeword of $C^\perp$.

Cyclically shifting this vector by $k+1$ positions gives the vector corresponding to $h^R(x)$, which must also be in $C^\perp$ since $C^\perp$ is cyclic.

As $\deg(h^R(x)) = \deg(h(x)) = k$, the set $\{h^R(x), xh^R(x), \ldots, x^{n-k-1}h^R(x)\}$ forms a basis for $C^\perp$. Thus, the monic polynomial $h_0^{-1}h^R(x)$ is the generator polynomial of $C^\perp$.

Corollary 3.2 *Let C be a $[n, k, d]$ cyclic code with generator polynomial $g(x)$. Let $h(x) = (x^n - 1)/g(x) = h_0 + h_1 x + \cdots + h_k x^k$. Then the matrix*

$$H = \begin{pmatrix} h_k & h_{k-1} & \cdots & h_0 & 0 & 0 & \cdots & 0 \\ 0 & h_k & h_{k-1} & \cdots & h_0 & 0 & \cdots & 0 \\ \vdots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \vdots \\ 0 & \cdots & 0 & h_k & h_{k-1} & \cdots & \cdots & h_0 \end{pmatrix},$$

is a parity-check matrix for C.

Although this matrix is not in standard form, elementary row operations can transform it into the standard form$P = (I_{n-k} \mid M)$. For decoding purposes, we typically work with the standard form parity-check matrix.

Theorem 3.7 *Let $P = (I_{n-k} \mid M)$ be a standard parity-check matrix for a cyclic code $\mathcal{C}$ over $\mathbb{F}_q$, and let $p(x)$ be the generator polynomial of $\mathcal{C}$. For any received vector $\mathbf{v} \in \mathbb{F}_q^n$ with corresponding polynomial representation $v(x)$, the syndrome $\mathbf{s}$ satisfies:*

$$\mathbf{s} \equiv v(x) \pmod{p(x)},$$

where the syndrome is computed as $\mathbf{s} = \mathbf{v}P^\top$.

Proof For the parity-check matrix $P = (I_{n-k} \mid M)$, we associate to each column of M a polynomial of degree at most $n-k-1$, writing:

$$M = \begin{pmatrix} f_0(x) & f_1(x) & \cdots & f_{k-1}(x) \end{pmatrix}.$$

By duality, the matrix $G = (-M^\top \mid I_k)$ generates $\mathcal{C}$. Thus each $x^{n-k+i} - f_i(x)$ corresponds to a codeword in $\mathcal{C}$, and therefore:

$$x^{n-k+i} - f_i(x) = q_i(x)p(x).$$

for some quotient polynomial $q_i(x) \in \mathbb{F}_q[x]/(x^n - 1)$, which implies:

$$f_i(x) \equiv x^{n-k+i} \pmod{p(x)}.$$

For a received vector $\mathbf{v} = (v_0, \ldots, v_{n-1})$ with polynomial representation $v(x) = \sum_{i=0}^{n-1} v_i x^i$, the syndrome polynomial $s(x)$ satisfies:

$$\begin{aligned} s(x) &= \sum_{i=0}^{n-k-1} v_i x^i + \sum_{j=0}^{k-1} v_{n-k+j} f_j(x) \\ &\equiv \sum_{i=0}^{n-1} v_i x^i - \sum_{j=0}^{k-1} v_{n-k+j} q_j(x) p(x) \\ &\equiv v(x) \pmod{p(x)}. \end{aligned}$$

Since $\deg(s(x)) \leq n-k-1$, the result follows.

Remark 3.5 *Theorem 3.7 demonstrates that $v(x) - s(x)$ yields a valid codeword in $\mathcal{C}$, where $s(x)$ is the syndrome of $v(x)$. When the weight condition*

$$\mathrm{wt}(s(x)) \leq \left\lfloor \frac{d(\mathcal{C}) - 1}{2} \right\rfloor,$$

is satisfied, we can unambiguously decode $v(x)$ to $v(x) - s(x)$. However, when this condition fails to hold, more sophisticated decoding machinery becomes necessary.

Lemma 3.1 *Let $\mathcal{C}$ be a q-ary $[n,k]$ cyclic code with generator polynomial $p(x)$. For a received word $v(x)$ with syndrome*

$$s(x) = \sum_{i=0}^{n-k-1} s_i x^i,$$

the syndrome of the cyclically shifted word $xv(x)$ is given by:

$$xs(x) - s_{n-k-1}p(x).$$

Proof By Theorem 6.5, it suffices to show that $xs(x) - s_{n-k-1}p(x)$ is the remainder when dividing $xv(x)$ by $p(x)$. Starting from the division:

$$v(x) = q(x)p(x) + s(x),$$

we multiply by x and rearrange:

$$\begin{aligned} xv(x) &= xq(x)p(x) + xs(x) \\ &= \big(xq(x) + s_{n-k-1}\big)p(x) + \big(xs(x) - s_{n-k-1}p(x)\big), \end{aligned}$$

where we observe that:

- The degree condition $\deg(xs(x) - s_{n-k-1}p(x)) < n-k = \deg(p(x))$ holds.
- The expression $xs(x) - s_{n-k-1}p(x)$ is precisely the remainder.

Definition 3.13 *A* cyclic run of 0 of length ℓ *in an n-tuple is a circular sequence of ℓ consecutive zero components.*

Example: *The vector $\mathbf{e} = (0,0,1,2,0,0,0,1,0,0)$ contains a cyclic run of 0 of length 4 (considering the circular nature of the tuple).*

Decoding algorithm for Cyclic Codes

Let $\mathcal{C}$ be a q-ary $[n,k,d]$-cyclic code with generator polynomial $p(x)$. Let $v(x)$ be a received word with error pattern $e(x)$, where $\mathrm{wt}(e(x)) \leq \lfloor \frac{d-1}{2} \rfloor$ and $e(x)$ has a cyclic run of 0 of length

$\geq k$. The decoding proceeds as:

1. **Syndrome Computation**: Compute syndromes $s_i(x) \equiv x^i v(x) \pmod{p(x)}$ for $i = 0, 1, 2, ...$
2. **Error Location**: Find m such that $\mathrm{wt}(s_m(x)) \leq \lfloor \frac{d-1}{2} \rfloor$.
3. **Error Correction**: Compute $e(x) \equiv x^{n-m} s_m(x) \pmod{x^n - 1}$ and decode to $v(x) - e(x)$.

Proof **Existence of** m: Since $e(x)$ contains a cyclic run of 0 of length $\geq k$, there exists a cyclic shift $x^m e(x) \equiv s_m(x) \pmod{x^n - 1}$ where all non-zero coefficients are confined to the first $n - k$ positions. This shift maintains the weight condition.

Correctness: Let $t(x) \equiv x^{n-m} s_m(x) \pmod{x^n - 1}$. We verify:

$$\begin{aligned} x^m(v(x) - t(x)) &\equiv x^m v(x) - x^n s_m(x) \\ &\equiv s_m(x) - s_m(x) \equiv 0 \pmod{p(x)}. \end{aligned}$$

Since $\gcd(x^m, p(x)) = 1$, we conclude $v(x) - t(x) \in \mathcal{C}$. As both $t(x)$ and $e(x)$ belong to the same coset with weight $\leq \lfloor \frac{d-1}{2} \rfloor$, they must be identical.

Example 3.4 *Consider the binary* $[127]$*-cyclic code generated by* $g(x) = 1 + x^3 + x^5 + x^6 + x^8$*. From the parity-check matrices, we verify that the minimum distance is* 5*. An error pattern with weight at most* 2 *must have a cyclic run of* 0*'s of length at least* 8*. Thus, we can correct such error patterns using the standard decoding procedure. Now, consider the received word:*

$$\begin{aligned} v(x) &= 101110011010001 \\ &= 1 + x^2 + x^3 + x^4 + x^7 + x^8 + x^{10} + x^{14} \end{aligned}$$

We compute the syndromes $s_i(x)$ of $x^i v(x)$ until $vt(s_i(x)) \leq 2$:

i	$s_m(x)$
0	$1 + x^4 + x^6 + x^9$
1	$x + x^5 + x^7 + x^{10}$
2	$1 + x^3 + x^6 + x^8$
3	$x + x^4 + x^7 + x^9$
4	$x^2 + x^5 + x^8 + x^{10}$
5	$1 + x^3 + x^6 + x^9$
6	$x + x^4 + x^7 + x^{10}$
7	$1 + x^6$

We decode $v(x)$ as follows:

$$\begin{aligned} v(x) &\to v(x) + x^7 s_7(x) \\ &= v(x) + x^7(1 + x^6) \\ &= v(x) + x^7 + x^{13} \\ &= 1 + x^2 + x^3 + x^4 + x^8 + x^{10} + x^{13} \\ &= 1011100010100010 \end{aligned}$$

Note: *The parity-check matrix was only used to verify the minimum distance; it was not explicitly required in the decoding procedure.*

General Conclusion

This research has focused on the essential framework of finite fields, how they are constructed, and several significant theoretical and practical uses across different disciplines. It has been demonstrated that finite fields are not just an abstract mathematical subject, but are crucial in the advancement of various modern technologies, especially in fields like information theory, cryptography, and communications.

Even with the considerable advancements achieved in the exploration of finite fields, this area continues to present numerous hopeful opportunities. As applications like artificial intelligence, quantum computing, and future communication networks continue to grow, the necessity for creating new mathematical models grounded in the characteristics of finite fields to aid these technologies becomes more apparent.

Consequently, exploring finite fields and leveraging their applications can be regarded as a crucial foundation for tackling the challenges of the scientific and technological future.

Bibliography

[1] Debbi Islam and Soualmia Said, *Finite Fields and Applications*, Master's thesis in Mathematics, Mohamed Boudiaf University of M'sila, 2024/2025. Available at: https://repository.univ-msila.dz/items/48b0e05d-5d99-4011-8a10-5cf8d97b4882

[2] Dummit, David S. and Richard M. Foote, *Abstract Algebra*, 3rd Edition, University of Vermont, Wiley, 2004. Available at: https://rksmvv.ac.in/wp-content/uploads/2021/04/David_S_Dummit_Richard_M_Foote_Abstract_Algebr_230928_225848.pdf

[3] Durbin, John R., *Modern Algebra: An Introduction*, John Wiley & Sons, 2008.

[4] Forney, David, *Introduction to Finite Fields*, Lecture Notes for Course CS250, Stanford University, Winter 2019. Available at: http://web.stanford.edu/~marykw/classes/CS250_W19/readings/Forney_Introduction_to_Finite_Fields.pdf

[5] Fraleigh, John B., *A First Course in Abstract Algebra*, Pearson Education India, 2003.

[6] Hill, Raymond, *A First Course in Coding Theory*, Oxford University Press, 1986.

[7] Huffman, W. Cary and Vera Pless, *Fundamentals of Error-Correcting Codes*, Cambridge University Press, 2010.

[8] Lang, Serge, *Algebra*, Vol. 211, Springer Science & Business Media, 2012.

[9] Lidl, Rudolf and Harald Niederreiter, *Finite Fields*, No. 20, Cambridge University Press, 1997.

[10] Morandi, Patrick, *Field and Galois Theory*, Vol. 167, Springer Science & Business Media, 2012.

[11] Rota, Gian-Carlo (ed.), *Encyclopedia of Mathematics and its Applications*, Cambridge University Press, 1976.

[12] Shparlinski, Igor E., *Finite Fields: Theory and Applications*, Available at: https://www.researchgate.net/publication/240745769_Finite_Fields_Theory_and_Applications

[13] Stewart, Ian, *Galois Theory*, Chapman and Hall/CRC, 2022.

[14] van Tilborg, Henk C. A., *Coding Theory: A First Course*, 1993.