



PEOPLE'S DEMOCRATIC REPUBLIC OF
ALGERIA
MINISTRY OF HIGHER
EDUCATION AND SCIENTIFIC
RESEARCH

Mohamed Boudiaf University of M'sila
Faculty of Mathematics and Informatics
Department of Mathematics



Master of Mathematics

Domain: Mathematics and Informatics

Specialty: Mathematics

Option: Algebra and Discrete Mathematics

Theme

Finite Fields and Applications

Presented by:

Debbi Islam – Soualmia Said

in front of the jury composed of :

KHADRAOUI ABDELMALEK	M.A.A,	University of M'sila	President.
LADJELAT LAHCENE	M.A.A,	University of M'sila	Supervisor.
DECHOUCHA NOUREDDINE	M.A.A,	University of M'sila	Examinator.

Acknowledgments

First and foremost, i would like to thank "**Allah**" who
blessme to finish this work.

The prophet Muhammad, may Allah bless him and grant him
peace, said, "Allah does not thank the person who does not
thank people".

I am very grateful to my supervisor **Mr. LADJELAT
LAHCENE.**, for his constant support, guidance, helped and
encouraged me .

My since thanks to the presedent of the jury **Mr.
KHADRAOUI ABDELMALEK** to accept this task and to give
interest to my work. Also, my thank **Mr. DACHOUCHA
NOUREDDINE** to accept being the examiner of this thesis .

It is important for to thanks my familly : my parents, my
sisters, and my brothers who have always been an inexhaustible
source of encouraguement .

A big thanks to my freinds, my colleagues and all teatchers of
the mathematics departement for their dedecation and their
generosity .

Dedicaces

I dedicate this thesis to my dear family because they were proud of me and who have always been by my side and have always supported me throughout these long years of study. As a sign of recognition, that they find here, the expression of my deep gratitude for all the efforts and means they have made to see me succeed in my studies .

Notations

$ G $	:	Number of elements in G .
$\mathbb{N}$	:	Natural numbers.
$\mathbb{Z}$	:	Integers numbers.
$\mathbb{R}$	:	Real numbers.
$\mathbb{Q}$	:	Rational numbers.
$\cong$	:	Isomorphism.
$\mathbb{Z}/p\mathbb{Z}$	:	Integers modulo p .
F_q	:	Finite field with q elements and $F_q^* = F_q - \{0\}$
$\text{char}(F)$	:	Characteristic of F .
R/I	:	Quotient ring.
$F[X]$	:	The set of polynomials with coefficients in F .
w_H	:	Hamming weight.
d_H	:	Hamming distance.
$d_{\min}$	:	Minimum distance.
$\deg()$	:	Degree of polynomial.
$U(R) = R^*$	:	The group of unity of a ring R .
$\langle a \rangle$	:	The ideal generated by an element $a \in R$.

$[F : K]$	:	The degree of the extension K/F .
C_n^p	:	The binomial coefficients.
$Gal(L/F)$	:	The Galois group of L over F .
σ_p	:	The Frobenius automorphism.
$\left(\frac{x}{p}\right)$	:	The Legendre's symbol.
F_q^n	:	The n -dimensional vector space over F_q .

Contents

Notations	1
Table of contents	3
Introduction	4
1 Introduction to algebraic structures	7
1.1 Groups	7
1.1.1 Subgroup	9
1.1.2 Cyclic group	10
1.2 Rings	10
1.2.1 Subrings	12
1.2.2 Ideals	13
1.2.3 Polynomial rings	17
1.2.4 Ring homomorphism	18
1.3 Fields	19
1.3.1 Subfields	19
1.3.2 Irreducible polynomials	19
1.3.3 Field extention	20

1.3.4	Characteristic of a fields	23
1.3.5	Splitting field	27
1.4	Vector spaces	28
2	The structure of a finite field	30
2.1	Finite field	30
2.2	Order of finite fields	31
2.3	Existence and uniqueness of finite fields	32
2.4	Representation of element of finite fields	33
2.5	Properties of finite fields	35
2.6	The multiplicative group of a finite field	40
2.7	The Galois group of finite field	40
2.8	The Frobenius automorphism	43
3	Some applications of finite fields	46
3.1	Quadratic residues modulo p	46
3.2	Fermat's Theorem	48
3.3	Wilson's Theorem	49
3.4	Linear codes	50
	Conclusion	54
	Bibliographie	55

Introduction

A field with $q \in \mathbb{N}$ elements is called a finite field of order q . The theory of finite fields is an interesting branch of modern algebra in itself and in other areas. The concept of a finite field first accured by Galois in 1830.

Uses and applications of finite fields are many : in mathematics and other areas such that communieation theory , computer science, statistics... etc.

In this work we present the basic properties of finite fields : thier order, characteristic, constructions, uniqueness and give some of their applications in Number Theory, (Quadratic residue) and in Coding Theory (Error-Block Codes over finite fields).

This work is divided into three chapters as follow :

Chapter one discusses the fondamental algebraic structures needed to understand and construct finite fileds: groups, ring, polynomial ring, quotient ring over an ideal, Euclidean division in a ring.

This chapter is necessary to understand the following chapter.

Chapter two is devoted to the construction and the study of properties of finite fields : their existence, uniqueness and constructions, also it studied their properties with respect to the characteristic (the newton's binomial law)... .

This chapter is the core of this work.

Chapter three is an introduction to some applications of finite fields in different areas : Number Theory, Coding Theory : Using finite fields in quadratic residue,

error-black codes over finite fields ... etc .

Chapter 1

Introduction to algebraic structures

In this chapter, we recall important results about rings, and we study some fundamental properties of polynomial rings, fields, extensions of fields...

1.1 Groups

Definition 1.1.1 (group) *A group $(G, *)$ is a nonempty set G with binary operation denoted by " $*$ ",*

$$*: G \times G \rightarrow G$$

$$(x, y) \rightarrow x * y$$

with the following properties:

1. " $*$ " is associative :

$$(x * y) * z = x * (y * z) \quad \text{for all } x, y, z \in G$$

2. There exists an identity element $e \in G$ for $*$:

$$x * e = e * x = x \quad \text{for all } x \in G$$

3. For each $x \in G$ there is an inverse $y \in G$:

$$x * y = y * x = e \quad \text{for all } x, y \in G$$

A group $(G, *)$ is said to be abelian if the group operation " $*$ " is commutative, i.e, for all $x, y \in G : (x * y = y * x)$.

Example 1.1.1 The following are examples of abelian groups :

- $(\mathbb{Z}, +)(\mathbb{R}, +)(\mathbb{C}, +)$ are all abelian groups under addition.
- $(\mathbb{Q}^*, \times)(\mathbb{R}^*, \times)(\mathbb{C}^*, \times)$ are all abelian groups under multiplication.

Definition 1.1.2 (group of unity) Let $(R, +, \cdot)$ be a ring with unity. we say that $(U, \cdot)$ is called the group of unity for R .

Example 1.1.2

- $U(\mathbb{Z}) = \{1, -1\}$.
- $U(\mathbb{Q}) = \mathbb{Q}^* = \mathbb{Q} - \{0\}$.
- $U(\mathbb{Z}/5\mathbb{Z}) = \{\bar{1}, \bar{2}, \bar{3}, \bar{4}\}$.

Theorem 1.1.1 *For all n in $\mathbb{N}$,*

$$\mathbb{Z}_n^\times = \{k \in \mathbb{Z} : k \prec n \text{ and } \gcd(k, n) = 1\}$$

Definition 1.1.3 (order of a group) *A group is called finite (resp. infinite) if it contains finitely (resp. infinitely) many elements. The number of elements in a finite group is called its order . We shall write $|G|$ for the order of the Finite group G .*

Proposition 1.1.1 *If G is a finite group and $a \in G$, then $a^{|G|} = e$.*

1.1.1 Subgroup

Definition 1.1.4 (Subgroup) *Let $(G, *)$ be a group . a nonempty subset H of group G is called subgroup of G if H is itself a group with respect to the operation on G .*

The following theorem gives a characterization for subgroup :

Theorem 1.1.2 *Let $(G, *)$ be a group , and H a nonempty subset of G , then H is subgroup of G if and only if :*

1. *if $x \in H$ and $y \in H$ then $x * y \in H$;*
2. *if $x \in H$,then $x^{-1} \in H$.*

Example 1.1.3 $(\mathbb{Z}, +)$ is a subgroup of $(\mathbb{R}, +)$.

1.1.2 Cyclic group

Definition 1.1.5 (Cyclic group) *Let $(G, \cdot)$ be a group, then G is called cyclic, if there exists an element $g \in G$, such that $G = \langle g \rangle = \{g^n : n \in \mathbb{Z}\}$, g is called a generator of the group G .*

Example 1.1.4 *The group $(\mathbb{Z}, +)$ is an infinite cyclic group with generator 1 or -1 .*

Theorem 1.1.3 (Fundamental Theorem on Finite Abelian Groups)

Every finite abelian group is isomorphic to the direct product of groups of the type $\mathbb{Z}_{p^k}$ (p prime).

By rearranging the direct factors properly this principal theorem can be written in a different form .

Definition 1.1.6 *Let G be a finite abelian group $\neq e$. Then there are natural numbers $s, d_1, d_2, \dots, d_s$ with $d_1 > 1$ and $d_i \mid d_{i+1}$ for $1 \leq i < s$ such that*

$$G \cong \mathbb{Z}_{d_1} \times \mathbb{Z}_{d_2} \times \dots \times \mathbb{Z}_{d_s}$$

These numbers are uniquely determined by G and are called the elementary divisors of G .

1.2 Rings

Definition 1.2.1 (ring) *A ring $(R, +, \cdot)$ is a set R defined with binary operations $+$ and $\cdot$ with the following properties:*

1. $(R, +)$ is an abelian group.

2. " ." is associative :

$$(x.y).z = x.(y.z) \quad \text{for all } x, y, z \in R$$

3. " ." is distributive with respect " + " :

$$x.(y + z) = x.y + x.z$$

$$(x + y).z = x.z + y.z \quad \text{for all } x, y, z \in R$$

- R is a **ring with unity or identity** , if there is an element $1 \in R$ such that $1.x = x.1$ for each element $x \in R$.

- A ring R is called a **commutative ring** , if the law " ." is commutative , i.e ,

$$x.y = y.x \quad \text{for all } x, y \in R$$

- A commutative ring R with identity is called an **integral domain** if , for every $x, y \in R$ such that $x.y = 0$, either $x = 0$ or $y = 0$.

- A **division ring** is a ring R , with an identity , in which every nonzero element in R is a unit, that is, for each $x \in R$ with $x \neq 0$, there exists a unique element x^{-1} such that $x.x^{-1} = x^{-1}.x = 1$.

- A **commutative division ring** is called a field .

Example 1.2.1

- For all $n \in \mathbb{N}^*$, $(M_n(\mathbb{R}), +, \times)$ is a ring with unity not commutative .
- $(2\mathbb{Z}, +, \times)$ is a ring without unity but commutative .

- For all $n \in \mathbb{N}^*$, $(\mathbb{Z}/n\mathbb{Z}, +, \times)$ is a commutative with unity .
- $(\mathbb{Z}/p\mathbb{Z}, +, \times)$ is a field with p number prime .
- the set of polynomials $R[x]$ in the indeterminate x with coefficients from R is a commutative ring with identity .

1.2.1 Subrings

Definition 1.2.2 (subring) Let $(R, +, \cdot)$ be a ring. a nonempty subset S of R is called a subring of R , and write $S \leq R$, if S itself a ring with respect to the operations on R .

Next, we provide an equivalent definition of the subring.

Theorem 1.2.1 A subset S of the ring R is a subring of R if and only if these conditions are satisfied :

- S is nonempty ;
- $(S, +)$ is a subgroup of R , i.e , $\forall a, b \in S, a - b \in S$;
- for all $x, y \in S$, the product $x \cdot y$ belongs to S .

Example 1.2.2

- $\mathbb{Z} \leq \mathbb{Q}$, $\mathbb{Q} \leq \mathbb{R}$, $2\mathbb{Z} \leq \mathbb{Z}$, $\mathbb{Z}[\sqrt{d}] \leq \mathbb{Q}[\sqrt{d}]$.
- if R is a ring , $\{0\}$ and R are subring for R (trivial subring) .
- $\langle x + 1 \rangle = \{(x + 1)f(x) \mid f \in F[x]\}$ is subring for $F[x]$, when F is commutative field .

1.2.2 Ideals

Definition 1.2.3 (ideal) *A subset I of a commutative ring R is said to be an ideal in R if it satisfies :*

1. *If $a, b \in I$, then $a \pm b \in I$.*
2. *If $a \in I$ and $r \in R$, then $r.a \in I$.*

Example 1.2.3

- *if R is a ring , $\{0\}$ are ideals (trivial) .*
- *$R = \mathbb{Z}$, $I = n\mathbb{Z} = \{nz \mid z \in \mathbb{Z}\}$.*
- *Let F be a commutative field , x undetermined over F and $g \in F[x]$*

$$\begin{aligned}\langle g(x) \rangle &= gF[x] \\ &= \{g.h \mid h \in F[x]\}\end{aligned}$$

is an ideal for $F[x]$.

Quation rings

Definition 1.2.4 (quation ring) *Let I be an ideal of a ring R .*

For $a \in R$, define the subset $a + I$ to be $a + I = \{a + i \mid i \in I\}$.

$(a + I) = (b + I)$ if and only if $(a - b) \in I$.

$$0 + I = 0$$

$$a \sim b \iff a + I = b + I \iff (a - b) \in I$$

$\sim$ is equivalence relation on R ,also $\bar{a} = [a] = a + I$

$$R/\sim = R/I = \{a + I \mid a \in R\}$$

On the set R/I we define two internal laws :

1. addition ,i.e ,

$$(a + I) + (b + I) = (a + b) + I$$

2. multiplication ,i.e ,

$$(a + I).(b + I) = (a.b) + I$$

R/I is called the quotient ring of R with respect to the ideal I or ring of residue classes modulo I .

Remark 1.2.1

- a. $1 + I$ is the multiplicative identity of R/I and $0 + I$ is the additive identity of R/I .
- b. If R is a commutative ring with unity then R/I is also a commutative ring with unity .

Proposition 1.2.1 The set $(\mathbb{Z}/n\mathbb{Z}, +, .)$ is always a commutative ring . It is a field if and only if n is prime .

Principal ideals

Definition 1.2.5 (Principal ideal) An ideal $(I, +, .)$ of the ring $(R, +, .)$ generated by a single element $a \in R$ is called a principal ideal , and is denoted by $\langle a \rangle$ such that

$$I = \langle a \rangle = \{a.r : r \in R\}$$

Example 1.2.4 *The principal ideal of the ring $(\mathbb{Z}, +, \times)$ generated by n is :*

$$I = \langle n \rangle = n\mathbb{Z} \quad \text{for some } n \in \mathbb{N} .$$

Prime ideal

Definition 1.2.6 (Prime ideal) *Let R be a integral domain and let P be an ideal of R . Then P is said to be a prime ideal of R if $\forall a, b \in R$, $ab \in P$ so $a \in P$ or $b \in P$.*

Example 1.2.5 *Let $R = (\mathbb{Z}, +, \times)$ and p be a prim number , then $(p) = p\mathbb{Z}$ is prime ideal .*

Theorem 1.2.2 *Let I be an ideal over a commuative ring with dentity et $I \neq R$, then I is prime $\Leftrightarrow R/I$ is integral domain .*

Proof.

$(\Rightarrow)$

Let I be a prime ideal on a ring R , let $(a + I), (b + I) \in R/I$.

$$\begin{aligned} (a + I), (b + I) = 0 + I &\Leftrightarrow ab + I = 0 + I \\ &\Leftrightarrow ab \in I \\ &\Leftrightarrow a \in I \text{ or } b \in I \\ &\Leftrightarrow a + I = I \text{ or } b + I = I \end{aligned}$$

that s to say R/I ntegral domain .

$(\Leftarrow)$

Let R/I integral domain, and let $a, b \in I$

$$\begin{aligned}
 ab \in I &\implies ab + I = I \\
 &= 0 + I \\
 &= (a + I)(b + I) \\
 &\implies a + I = I \text{ or } b + I = I \\
 &\implies a \in I \text{ or } b \in I \\
 &\implies I \text{ is prime .}
 \end{aligned}$$

■

maximal ideal

Definition 1.2.7 (maximal ideal) *The ideal I of the ring R is called maximal if : $I \neq R$ and if $I \subset j \Rightarrow (I = j \text{ or } j = R)$.*

Example 1.2.6 *Let p be a prime , the ideal $(p) = pZ$ is maximal of Z .*

Theorem 1.2.3 *I is maximal ideal of R if and only if R/I is a field .*

Proof.

$\implies$

Let I is a maximal ideal and let $\bar{J}$ is an ideal of R/I , then $\bar{J} = J/I$ and J are ideals of R

and $I \subset J$, this implies that $J = I$ or $J = R$. So $\bar{J} = I/I = \{\bar{0}\}$ or $\bar{J} = R/I$.

Hence, R/I is a field .

$\Leftarrow$

Let R/I is a field and let J is an ideal on R and $I \subset J$, this implies that $\overline{J} = J/I$ is an ideal on R/I . So, R/I is a field. Therefore, $\overline{J} = J/I = \{0\}$ or $\overline{J} = J/I = R/I$. Thus, $J = I$ or $J = R$. Hence, I is a maximal ideal.

■

Example 1.2.7 $I = nZ$ is maximal on $Z \iff Z/nZ$ is a field $\iff n$ is prime.

In the following theorem, we provide the relationship between the maximal ideal and the prime ideal on the same ring.

Theorem 1.2.4 A maximal ideal I on a ring R is a prime ideal on this ring.

Proof.

I is a maximal ideal $\iff R/I$ is a field $\implies R/I$ is an integral domain $\iff I$ is a prime ideal. ■

1.2.3 Polynomial rings

Let R be a commutative ring with identity. Any expression of the form

$$f(x) = \sum_{i=0}^n a_i x^i = a_0 + a_1 x + a_2 x^2 + \dots + a_n x^n,$$

where $a_i \in R$ and an $a_n \neq 0$, is called a **polynomial** over R with **indeterminate** x . The elements $a_0, a_1, \dots, a_n$ are called the **coefficients** of f .

Definition 1.2.8 (degree of polynomial) Let $f \in R[x]$.

If $f \neq 0$, $f = a_0 + a_1 x^1 + \dots + a_n x^n$, $a_n \neq 0$ the natural "n" is the degree of f and we write $\deg(f) = n$.

Proposition 1.2.2 *Let R be a ring , x indetermined on R and $f, g \in R[x]$*

1. $\deg(f + g) \leq \max(\deg(f), \deg(g))$ with equality if $\deg(f) \neq \deg(g)$.
2. if R is an integral domain , then $\deg(f.g) = \deg(f) + \deg(g)$.

Definition 1.2.9 (euclidean division) *Let F be a field , x indetermined on F and $f, g \in F[x]$ with $g \neq 0$, then there is $(q, r) \in (R[x])^2$ unique such that $f = qg + r$ and $\deg(r) < \deg(g)$.*

1.2.4 Ring homomorphism

Definition 1.2.10 (Ring homomorphism) *Let $(R, +_R, \cdot_R)$ and $(S, +_S, \cdot_S)$ be rings .*

A set map $\phi : R \rightarrow S$ is a (ring) homomorphism if

1. $\phi(a +_R b) = \phi(a) +_S \phi(b)$ for all $a, b \in R$,
2. $\phi(a \cdot_R b) = \phi(a) \cdot_S \phi(b)$ for all $a, b \in R$,
3. $\phi(1_R) = 1_S$ where 1_R and 1_S are the respective identities .

- **A ring isomorphism** is a bijective ring morphism . If there is an isomorphism between the rings R and S , we say R and S are **isomorphic rings** and write $R \cong S$.

- An isomorphism $\phi : R \rightarrow R$ is called an **automorphism** of R .

Example 1.2.8 *Let $R = \mathbb{Z}$ and $I = n\mathbb{Z}$ for some $n \succ 1$. We have that the quotient ring $R/I = \mathbb{Z}/n\mathbb{Z}$ is isomorphic to $\mathbb{Z}_n$ (as a ring) .*

1.3 Fields

Definition 1.3.1 (field) *A field $(F, +, \times)$ is a set F with binary operations addition $+$ and multiplication $\times$, for which the following axioms are satisfied :*

1. *$(F, +)$ is an abelian group (whose identity is 0) under the operation $+$.*
2. *The set $F^* = F - \{0\} = \{a \in F \mid a \neq 0\}$ forms an abelian group (whose identity is 1).*
3. *Distributive law holds : $(a + b) \times c = (a \times c) + (b \times c)$, for all $a, b, c \in F$.*

Example 1.3.1 *The rings $(\mathbb{Q}, +, \times)$, $(\mathbb{R}, +, \times)$ and $(\mathbb{C}, +, \times)$ are commutative fields.*

1.3.1 Subfields

Definition 1.3.2 (subfield) *A subfield S of a field F is a subset of F which is itself a field with the same operations as F .*

Example 1.3.2

- *$(\mathbb{Q}, +, \cdot)$ is a subfield of the field $\mathbb{R}$.*
- *$(\mathbb{R}, +, \cdot)$ is a subfield of the field $\mathbb{C}$.*

1.3.2 Irreducible polynomials

Definition 1.3.3 (irreducible polynomial) *A non constant polynomial $p(x)$ in $F[x]$ is said to be irreducible over F if whenever $p(x) = a(x)b(x)$ with $a(x), b(x) \in F[x]$ then one of $a(x), b(x)$ has degree 0 (i.e., is constant).*

Example 1.3.3 The polynomial $x^2 + 1$ is irreducible over the real field $\mathbb{R}$ not over the complex field $\mathbb{C}$, for there $x^2 + 1 = (x + 1)(x - i)$ where $i^2 = -1$.

Definition 1.3.4 An element $b \in F$ is called a root (or a zero) of the polynomial $f \in F[x]$ if $f(b) = 0$.

Example 1.3.4 The elements $2, 3 \in \mathbb{Q}$ are roots of $x^2 - 5x + 6 \in \mathbb{Q}[x]$.

Theorem 1.3.1 The element $b \in F$ is a multiple root of $f \in F[x]$ if and only if it is a root of both f and f' .

Proposition 1.3.1 A polynomial f , irreducible over the field F , has a root in F if and only if $\deg f = 1$.

Proposition 1.3.2 The ideal $I = \langle p(x) \rangle$ over $F[x]$ is a maximal ideal if and only if $p(x)$ is irreducible over F .

1.3.3 Field extension

If F and K are fields and $F \subset K$, we say that K is an extension of F , and we write $K \supseteq F$, or K/F .

Definition 1.3.5 Let $(F, +, \times)$ be a field . A nonempty subset K of F which is a field with respect to the operations in F is called a subfield of F .In this context , F is called an extension field of K .

A field containing no proper subfields is called a prime field .

Example 1.3.5

- The rational-number field is a proper subfield of the real-number field , and the real-number field is a proper subfield of the complex-number field .

- *The rational-number field is a prime field .*
- *The real- and complex-number fields are extension fields of the rational-number field .*

Definition 1.3.6 (the degree of extension) *Let K be a field and F an extension of K . The degree of F over K denoted by $[F : K]$ is the dimension of F as a vector space over F .*

Example 1.3.6

- *The complex numbers $\mathbb{C}$ are two-dimensional over the real numbers $\mathbb{R}$, because a basis is $\{1, i\}$. Hence $[\mathbb{C} : \mathbb{R}] = 2$.*
- *Let $p(x)$ be a polynomial of degree n irreducible over the field F , so that the quotient ring*

$$K = F[x] / (p(x)) = \{a_0 + a_1x + \dots + a_{n-1}x^{n-1} \mid a_i \in F\}$$

is a field. Then K is an extension field of F .

Theorem 1.3.2 (The degree is multiplicative) *Let L be a finite extension of K and K a finite extension of F . Then L is a finite extension of F and*

$$[L : F] = [L : K][K : F]$$

Definition 1.3.7 (minimal polynomial) *Let E/F be a field extension , an element α of E . The **minimal polynomial** of α is the monic polynomial of least degree among all polynomials in $F[x]$ having α as a root.*

Example 1.3.7 $x^2 + 1$ *is the minimal polynomial of i over $\mathbb{R}$ and $[\mathbb{C} : \mathbb{R}] = 2$.*

Proposition 1.3.3 *Let K be a field extension of F and $\alpha \in K$. Then*

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

is the quotient field of $F[\alpha]$.

Definition 1.3.8 (simple extension) *Let K be a field extension of F . The field K is said to be a **simple extension** of F iff there exists an element α in K such that $K = F(\alpha)$. The element $\alpha \in K$ is said to be a primitive element of the extension and $F(\alpha)$ is said to be generated by F and α .*

Definition 1.3.9 *Let K be a field extension of the field F . Then an element α of K is said to be algebraic over F iff α is a root of some non-null polynomial $f(x)$ in $F[x]$.*

Example 1.3.8 *Both $\sqrt{2}$ and i are algebraic over $\mathbb{Q}$ since they are zeros of the polynomials $x^2 - 2$ and $x^2 + 1$, respectively .*

Definition 1.3.10 *Let K be a field extension of the field F . Then K is said to be an algebraic extension over F iff every element of K is algebraic over F .*

Theorem 1.3.3 *Let K be an extension of F , and let $\alpha \in K$ be algebraic over F . Then:*

- i.** $F(\alpha) = F[\alpha] \cong F[x]/(f)$, where f is a uniquely determined , monic ,irreducible polynomial in $F[x]$ with zero in K .

ii. If f in (i) is of degree n then $1, \alpha, \dots, \alpha^{n-1}$ is a basis of $F(\alpha)$ over F . We have $[F(\alpha) : F] = n$ and each element of $F(\alpha)$ can be uniquely expressed as

$$a_0 + a_1\alpha + \dots + a_{n-1}\alpha^{n-1}; a_i \in F.$$

Remark 1.3.1 Every finite extension field E of a field F is an algebraic extension.

1.3.4 Characteristic of a fields

Definition 1.3.11 (Characteristic of a field) Let $(F, +, \times)$ be a field. The smallest natural number $n \succ 0$ such that

$$n \times 1 = \underbrace{1 + 1 + 1 + \dots + 1}_{n\text{-times}} = 0$$

is called the characteristic of F , denoted by $\text{char}(F) = n$. if no such n exists, we say $\text{char}(F) = 0$.

Theorem 1.3.4 The characteristic of a field is either 0 or a prime number p

Proof. The former possibility can certainly occur : $\mathbb{Q}$, $\mathbb{R}$ and $\mathbb{C}$ are all fields of characteristic 0 Let K be a field and suppose that $\text{char } F = n \neq 0$, where n is not prime.

Then $n = rs$, where $1 < r < n, 1 < s < n$, and the minimal property of n implies that $r1_F \neq 0_F, s1_F \neq 0_F$. On the other hand, we deduce that

$$(r1_F)(s1_F) = (rs)1_F = n1_F = 0_F$$

and this is impossible, since F , being a field, has no zero divisors.

■

Theorem 1.3.5 *Let k be a field . Then k contains a prime subfield $P(k)$ contained in every subfield .*

i. *if $\text{char}(k) = 0$, then $\mathbb{Q}$ is the prime subfield of K .*

ii. *if $\text{char}(k) = p$, then $\mathbb{Z}_p = \mathbb{Z}/p\mathbb{Z}$ is the prime subfield of K .*

$$\underset{\text{prime subfield of } k}{K_0} \subset \dots \subset K_2 \subset \underset{\text{subfield}}{K_1} \subset \underset{\text{field}}{K}$$

Theorem 1.3.6 (Freshman's Dream) *Let F be a field of characteristic p . Then, for all x, y in F ,*

$$(x + y)^p = x^p + y^p$$

Proof. By the binomial theorem, valid in any commutative ring with unity , we have that

$$(x + y)^p = \sum_{r=0}^p C_r^p x^{p-r} y^r \tag{1.1}$$

For $r = 1, \dots, p-1$, the binomial coefficient

$$C_r^p = \frac{p(p-1) \dots (p-r+1)}{r!}$$

is an integer, and so $r!$ divides $p(p-1)\dots(p-r+1)$.

Since p is prime and $r < p$, no factor of $r!$ can be divisible by p . Hence $r!$ divides $(p-1)\dots(p-r+1)$, and so C_r^p is an integer divisible by p . Hence, for $r = 1, \dots, p-1$,

$$C_r^p x^{n-r} y^r = 0$$

and so, in (1.1), only the first and last terms survive .

■

Example 1.3.9

- the characteristic of the ring $\mathbb{Z}_6$ of integers mod $[6]$ is $\text{char}(\mathbb{Z}_6) = 6$, car Since $6(1_K) = 0_K$, and since no positive integer smaller than 6 has this property .
- the multiplication table for $\mathbb{Z}_7$, and list the inverses of all the non-zero elements , Leaving out 0, we have the table :

.	1	2	3	4	5	6
1	1	2	3	4	5	6
2	2	4	6	1	3	5
3	3	6	9	5	1	4
4	4	1	5	2	6	3
5	5	3	1	6	4	2
6	6	5	4	3	2	1

the inverses is :

$$1^{-1} = 1 \quad 2^{-1} = 4 \quad 3^{-1} = 5 \quad 4^{-1} = 2 \quad 5^{-1} = 3 \quad 6^{-1} = 6.$$

- we prove by induction on n , that the binomial theorem ,

$$(a + b)^n = \sum_{r=0}^n C_n^r a^{n-r} b^r$$

is valid in a commutative ring R with unity .

This is certainly true for $n = 1$, since

$$(a + b)^1 = (a + b) = C_1^0 a + C_1^1 b$$

Let $n \geq 1$, and suppose inductively that the theorem is true for n . To show that it is true for $n + 1$ we require the Pascal identity

$$C_n^{r-1} + C_n^r = C_{n+1}^r \quad n \geq r \geq 1$$

whose proof is straightforward. For the induction step, during which we use only operations that are valid in a commutative ring , we have that

$$\begin{aligned} (a + b)^{n+1} &= (a + b)(a + b)^n = (a + b) \left(\sum_{r=0}^n C_n^r a^{n-r} b^r \right) \\ &= (a + b) (a^n + \dots + C_n^{r-1} a^{n-r+1} b^{r-1} + C_n^r a^{n-r} b^r + \dots + b^n) \end{aligned}$$

For $r = 1, 2, \dots, n$, the term in $a^{(n+1)-r}b^r$ is

$$b.C_n^{r-1}a^{n-r+1}b^{r-1} + a.C_n^r a^{n-r}b^r$$

and so the coefficient is

$$C_n^{r-1} + C_n^r = C_{n+1}^r$$

The coefficients of a^{n+1} and b^{n+1} are both 1, and so we conclude that

$$(a + b)^{n+1} = \sum_{r=0}^{n+1} C_{n+1}^r a^{(n+1)-r} b^r$$

Hence, by induction, the result is true for all $n \geq 1$.

- In a field of finite characteristic p , for $(x - y)^p = x^p - y^p$ we have that

$$(x - y)^p = \sum_{r=0}^p C_p^r (-1)^r x^{p-r} y^r = x^p + (-1)^p y^p$$

If p is odd, the result is immediate. If $p = 2$ it seems that $(x - y)^2 = x^2 + y^2$, but $a = -a$ for every a in a field of characteristic 2, and so the result is still true.

1.3.5 Splitting field

Definition 1.3.12 (Splitting field) Let $f \in F[x]$, not necessarily an irreducible polynomial. A splitting field for f over F is an extension field K/F such that

1. f splits completely in K , say $I(x) = (x - \alpha_1) \dots (x - \alpha_n)$ with α_i in K

2. K is generated by the roots: $K = F(\alpha_1, \dots, \alpha_n)$

Example 1.3.10 $\mathbb{Q}(\sqrt{2}, \sqrt{3}) = \mathbb{Q}(\pm\sqrt{2}, \pm\sqrt{3})$ is a splitting field of $(x^2 - 2)(x^2 - 3)$ over $\mathbb{Q}$.

Theorem 1.3.7 (Existence and uniqueness of splitting field) *If K is a field and f any polynomial of positive degree in $K[x]$, then there exists a splitting field of f over K . Any two splitting fields of f over K are isomorphic under an isomorphism which keeps the elements of K fixed and maps roots of f into each other.*

1.4 Vector spaces

Definition 1.4.1 *A vector space or a linear space over a field F is an additive abelian group V together with an external law of composition (called scalar multiplication).*

$\mu : F \times V \rightarrow V$, the image of (u, v) under μ is denoted by uv , satisfying the following conditions :

1. $1v = v$, where 1 is the multiplicative identity in F ;
2. $(\alpha\beta)v = \alpha(\beta v)$;
3. $(\alpha + \beta)v = \alpha v + \beta v$;
4. $\alpha(u + v) = \alpha u + \alpha v, \forall \alpha, \beta \in F$ and $u, v \in V$.

The elements of V are called **vectors** and the elements of the field F are called **scalars**.

Example 1.4.1 *The n -tuples of real numbers, denoted by $\mathbb{R}^n$, form a vector space over $\mathbb{R}$. Given vectors $u = (u_1, \dots, u_n)$*

and $v = (v_1, \dots, v_n)$ in $\mathbb{R}^n$ and α in $\mathbb{R}$, we can define vector addition by

$$u + v = (u_1, \dots, u_n) + (v_1, \dots, v_n) = (u_1 + v_1, \dots, u_n + v_n)$$

and scalar multiplication by

$$\alpha u = \alpha(u_1, \dots, u_n) = (\alpha u_1, \dots, \alpha u_n).$$

Chapter 2

The structure of a finite field

This chapter is of central importance since it contains various fundamental properties and results and a description of methods for constructing with some examples specific to this study .

2.1 Finite field

Definition 2.1.1 (Finite field) *A finite field is a field with a finite number of elements. this number is called the order of the field .*

Example 2.1.1 $(\mathbb{Z}/p\mathbb{Z}, +, \times)$ is a finite field when p is a prime number .

Notation 2.1.1 *We note that when p is a prime the field F_p is the same as (isomorphic to) the ring $\mathbb{Z}_p$ of integers modulo p . The ring $\mathbb{Z}_p$ is also denoted by $\mathbb{Z}/p\mathbb{Z}$.*

Example 2.1.2

- *Tables 1 and 2 show module-2 addition and multiplication respectively for F_p , here p equals 2 :*

+	0	1
0	0	1
1	1	0

.	0	1
0	0	0
1	0	1

- The results for F_3 are shown in tables 3 and 4 where p here is equal to 3 :

+	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

.	0	1	2
0	0	0	0
1	0	1	2
2	0	2	1

Definition 2.1.2 (Galois Field) *The Galois Field $GF(q)$ is the finite field with q elements .*

Example 2.1.3 *The field $GF(11)$ is the finite field of order 11.*

2.2 Order of finite fields

Theorem 2.2.1 *Let F be a finite field of characteristic p . There exists an integer $n \geq 1$ so that $|F| = p^n$.*

Proof. Consider F as vector space over F_p . Let $[F = F_p] = \dim F_p = n$ and let $\{\gamma_1, \dots, \gamma_n\}$ be a basis .

Then every element $a \in F$ can be represented via a linear combination of the basis elements with coefficients in F_p so there exist $c_1, \dots, c_n \in F_p$ satisfying $a = c_1\gamma_1 + \dots + c_n\gamma_n$.

Each c_i can have p different values , since we consider linear combinations over a basis, all these p_n elements in F are distinct . Again by the property of a basis

each element of F can be represented as linear combination this way . Thus $|F| = p^n$

.

■

2.3 Existence and uniqueness of finite fields

Lemma 2.3.1 *If F is a finite field with q elements and K is a subfield of F , then the polynomial $x^q - x$ in $K[x]$ factors in $F[x]$ as*

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

and F is a splitting field of $x^q - x$ over $K[x]$.

Proof. The polynomial $x^q - x$ of degree q has at most q roots in F .

but we know q such roots namely , all the elements of F . Thus the given polynomial splits in F in the indicated manner , and it cannot split in any smaller field . ■

We are now able to prove the main characterization theorem for finite fields, the leading idea being contained in lemma (2.3.1)

Theorem 2.3.1 (Existence and uniqueness of finite field) *For every prime p and every positive integer n there exists a finite field with p^n elements . Any finite field with $q = p^n$ elements is isomorphic to the splitting field of $x^q - x$ over F_p .*

Proof. (Existence) For $q = p^n$ consider $x^q - x$ in $F_p[x]$, and let F be its splitting field over F_p . This polynomial has q distinct roots in F since its derivative is

$qx^{q-1} - 1 = -1$ in $F_q[x]$ and so can have no common root with $x^q - x$.

Let $S = \{a \in F : a^q - a = 0\}$ Then S is a subfield of F since: S contains 0 and 1, $a, b \in S$ implies by lemma (Freshman's Dream) that $(a - b)^q = a^q - b^q = a - b$ and so $a - b \in S$, for $a, b \in S$ and $b \neq 0$ we have $(ab^{-1})^q = a^q b^{-q} = ab^{-1}$ and so $ab^{-1} \in S$. But, on the other hand, $x^q - x$ must split in S since S contains all its roots. Thus $F = S$, and since S has q elements, F is a finite field with q elements.

(Uniqueness) Let F be a finite field with $q = p^n$ elements. Then F has characteristic p and so contains F_p as a subfield. It follows from Lemma (2.3.1) that F is a splitting field of $x^q - x$ over F_p . Thus the desired result is a consequence of the uniqueness (up to isomorphisms) of splitting fields, which was noted in theorem (1.3.7). ■

2.4 Representaion of element of finite fields

Definition 2.4.1 (primitive element) A nonzero element a of a finite field F_q is called a primitive (or generator) element if its multiplicative order is $q - 1$. That is,

$a^{q-1} = 1, a, a^2, \dots, a^{q-2}$ form all the nonzero elements of F_q .

Example 2.4.1 A primitive element of F_5 is 2

$$2^1 = 2, \quad 2^2 = 2 \cdot 2 = 4, \quad 2^3 = 2^2 \cdot 2 = 4 \cdot 2 = 3, \quad 2^4 = 2^3 \cdot 2 = 3 \cdot 2 = 1$$

Theorem 2.4.1 Let F_q be a finite field and F_r a finite extension field of F_q . Then F_r is a simple extension of F_q , i.e., $F_r = F_q(\beta)$ for some $\beta \in F_r$.

Proof. Let α be a primitive element of F_r . We clearly have $F_q(\alpha) \subseteq F_r$. On the other hand, F_r contains 0 and all powers of α , and so all elements of F_r . Therefore $F_r = F_q(\alpha)$. ■

Corollary 2.4.1 *For every finite field F_q and every positive integer n there exists an irreducible polynomial in $F_q[x]$ of degree n .*

Proof. Let F_r be the extension field of F_q of order q^n , so that $[F_r : F_q] = n$. By theorem (2.4.1) we have $F_r = F_q(\gamma)$ for some $\gamma \in F_r$. Then the minimal polynomial of γ over F_q is an irreducible polynomial in $F_q[x]$ of degree n . ■

Theorem 2.4.2 *For a prime p and a monic irreducible $f(x)$ in $F_p[x]$ of degree n , the ring $F_p[x]/(f(x))$ is a field of order p^n .*

Proof. The cosets mod $f(x)$ are represented by remainders

$$a_0 + a_1x + \dots + a_{n-1}x^{n-1} \quad a_i \in F_p$$

and there are p^n of these . Since the modulus $f(x)$ is irreducible, the ring $F_p[x]/(f(x))$ is a field . ■

Example 2.4.2

- Two fields of order 8 are $F_2[x]/(x^3 + x + 1)$ and $F_2[x]/(x^3 + x^2 + 1)$.
- Two fields of order 9 are $F_3[x]/(x^2 + 1)$ and $F_3[x]/(x^2 + x + 2)$.
- The polynomial $x^3 - 2$ is irreducible in $F_7[x]$, so $F_7[x]/(x^3 - 2)$ is a field of order 7^3 .

Theorem 2.4.3

If $f \in F_p[x]$ is an irreducible polynomial of degree n then $F_p[x]/(f) \cong F_{p^n}$.

Example 2.4.3

$F_2[x]/(x^3 + x + 1) \cong F_{2^3}$, $F_2[x]/(x^3 + x^2 + 1) \cong F_{2^3}$, and $F_3[x]/(x^2 + x + 2) \cong F_{3^2}$.

2.5 Properties of finite fields

In this section , we list some important properties of finite fields

Lemma 2.5.1 *For every element β of a finite field F_q with q elements, we have $\beta^q = \beta$.*

Proof. The identity $\beta^q = \beta$ is trivial for $\beta = 0$. On the other hand , the nonzero elements of F_q form a group of order $q - 1$ under multiplication. Thus $a^{q-1} = 1$ for all $a \in F_q$ with $a \neq 0$. and multiplication by a yields the desired result . ■

Lemma 2.5.2 *Let F be a finite field containing a subfield K with q elements. Then F has q^m elements , where $m = [F : K]$.*

Proof. F is a vector space over K , and since F is finite, it is finite-dimensional as a vector space over K . If $[F : K] = m$ then F has a basis over K consisting of m elements, say $b_1, b_2, \dots, b_m$. Thus every element of F can be uniquely represented in the form $a_1 b_1 + a_2 b_2 + \dots + a_m b_m$, where $a_1, a_2, \dots, a_m$ in K . Since each a_i can have q values, F has exactly q^m elements .

■

Theorem 2.5.1 *Let F be a finite field . Then F has p^n elements , where the prime p is the characteristic of F and n is the degree of F over its prime subfield .*

Theorem 2.5.2 *Let a be a nonzero element of a finite field F_q . Then $a^{q-1} = 1$.*

Proof. Let $b_1, b_2, \dots, b_{q-1}$ be the $q - 1$ nonzero elements of F_q . Consider the $q - 1$ elements , $a.b_1, a.b_2, \dots, a.b_{q-1}$, which are nonzero . These $q - 1$ elements must be distinct , otherwise , for some $i \neq j$, $a.b_i = a.b_j$ which implies that $b_i = b_j$ (use the cancelation law) . Therefore , $a.b_1, a.b_2, \dots, a.b_{q-1}$ also form the $q - 1$ nonzero elements of F_q . Hence ,

$$(a.b_1).(a.b_2)...(a.b_{q-1}) = b_1.b_2...b_{q-1}$$

Since the multiplication operation in F_q is associative and commutative , the above equality can be put in the following form :

$$a^{q-1}(b_1.b_2...b_{q-1}) = b_1.b_2...b_{q-1}$$

Since the product of nonzero elements is nonzero , it follows from the cancelation law that $a^{q-1} = 1$. This proves the theorem . ■

Definition 2.5.1 (Order) *The order of a nonzero element $\alpha \in F_q$, denoted by $\text{ord}(\alpha)$, is the smallest positive integer k such that $\alpha^k = 1$.*

Example 2.5.1 *Since there are no linear factors for the polynomial $1 + x^2$ over F_3 , $1 + x^2$ is irreducible over F_3 . Consider the element α in the field $F_9 = F_3(\alpha)$, where α is a root of $1 + x^2$ in some extension of F_q . Then $\alpha^2 = -1$, $\alpha^3 = \alpha(\alpha^2) = -\alpha$ and $\alpha^4 = (\alpha^2)^2 = (-1)^2 = 1$.*

This means that $\text{ord}(\alpha) = 4$.

Theorem 2.5.3 *Let n be the order of a nonzero element a in F_q . Then n divides $q - 1$.*

Proof. Suppose $q - 1$ is not divisible by n . On dividing $q - 1$ by n , we have $q - 1 = kn + r$ where $1 \leq r < n$. Then $a^{q-1} = a^{kn+r} = a^{kn}.a^r$ Since $a^{q-1} = 1$ and $a^n = 1$ we must have $a^r = 1$. This contradicts the fact that n is the smallest positive integer such that $a^n = 1$. Therefore, n must divide $q - 1$. ■

For a finite field F_q we denoted by F_q^* the multiplicative group of nonzero elements of F_q

Lemma 2.5.3

1. The order $\text{ord}(\alpha)$ divides $q - 1$ for every $\alpha \in F_q^*$.
2. For two nonzero elements $\alpha, \beta \in F_q^*$,

if $\gcd(\text{ord}(\alpha), \text{ord}(\beta)) = 1$, then $\text{ord}(\alpha\beta) = \text{ord}(\alpha) \times \text{ord}(\beta)$.

Proof.

1. Let m be a positive integer satisfying $\alpha^m = 1$. Write $m = a.\text{ord}(\alpha) + b$ for some integers $a \geq 0$ and $0 \leq b < \text{ord}(\alpha)$. Then

$$1 = \alpha^m = \alpha^{a.\text{ord}(\alpha)+b} = (\alpha^{\text{ord}(\alpha)})^a . \alpha^b = \alpha^b .$$

This forces $b = 0$; i.e. , $\text{ord}(\alpha)$ is a divisor of m . Since $\alpha^{q-1} = 1$, we obtain $\text{ord}(\alpha) \mid (q - 1)$.

2. Put $r = \text{ord}(\alpha) \times \text{ord}(\beta)$. It is clear that $\alpha^r = 1 = \beta^r$ as both $\text{ord}(\alpha)$ and $\text{ord}(\beta)$ are divisors of r . Thus , $(\alpha\beta)^r = \alpha^r \beta^r = 1$. Therefore , $\text{ord}(\alpha\beta) \leq \text{ord}(\alpha) \times \text{ord}(\beta)$. On the other hand, put $t = \text{ord}(\alpha\beta)$. We have

$$1 = (\alpha\beta)^{t.\text{ord}(\alpha)} = (\alpha^{\text{ord}(\alpha)})^t \beta^{t.\text{ord}(\alpha)} = \beta^{t.\text{ord}(\alpha)} .$$

This implies that $\text{ord}(\beta)$ divides $t.\text{ord}(\alpha)$ by the proof of part (1) , so $\text{ord}(\beta)$ divides t as $\text{ord}(\alpha)$ is a prime to $\text{ord}(\beta)$. In the same way, we can show that $\text{ord}(\alpha)$ divides t . This implies that $\text{ord}(\alpha) \times \text{ord}(\beta)$ divides t . Thus , $\text{ord}(\alpha\beta) = t \geq \text{ord}(\alpha)\text{ord}(\beta)$. The desired result follows .

■

Lemma 2.5.4 *Let F be a field and p a prime and let m, n be natural numbers, x is indeterminate. The following are equivalent*

1. $m \mid n$;
2. $p^m - 1 \mid p^n - 1$;
3. $x^m - 1 \mid x^n - 1$.

Theorem 2.5.4 (Subfield Criterion) *Let p be a prime and let m, n be natural numbers .*

- i. *If F_{p^m} is a subfield of F_{p^n} , then $m \mid n$.*
- ii. *If $m \mid n$, then $F_{p^m} \hookrightarrow F_{p^n}$. There is exactly one subfield of F_{p^n} with p^m elements .*

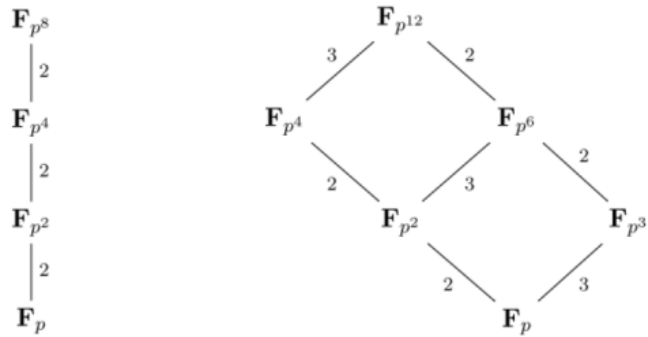
Proof. (i.) Theorem (1.3.2) implies

$$[F_{p^n} : F_p] = [F_{p^n} : F_{p^m}][F_{p^m} : F_p].$$

Since the term on the left-hand side is n and the second factor on the right-hand side is m , we have $m \mid n$. (ii.) If $m \mid n$, we have $p^m - 1 \mid p^n - 1$, thus (lemma 2.5.4) $x^{p^m-1} - 1 \mid x^{p^n-1} - 1$ and $x^{p^m} - x \mid x^{p^n} - x$. The roots of $x^{p^m} - x$ form a subfield of F_{p^n} of order p^m , which is isomorphic to F_{p^m} . There cannot be another subfield with p^m elements, because otherwise there would be more than p^m roots of $x^{p^m} - x$ in F_{p^n} . ■

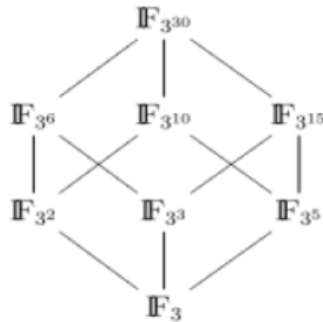
Example 2.5.2

- In the diagram below are the subfields of F_{p^8} and $F_{p^{12}}$.



- Consider the finite field $F_{3^{30}}$. any subfield F_{3^m} must satisfy $m \mid 30$ and thus there are only the following subfields : F_3 , F_{3^2} , F_{3^3} , F_{3^5} , F_{3^6} , $F_{3^{10}}$, $F_{3^{15}}$, and $F_{3^{30}}$.

This leads to the following Hasse-diagram:



2.6 The multiplicative group of a finite field

Theorem 2.6.1 *Let a be a nonzero element of order n in a finite field F_q . Then the powers of a ,*

$$a^n = 1, a, a^2, \dots, a^{n-1},$$

form a cyclic subgroup of the multiplicative group of F_q

Proof. Let $G = \{a^n = 1, a, \dots, a^{n-1}\}$. Since n is the smallest positive integer such that $a^n = 1$, all the elements in G are distinct nonzero elements in the multiplicative group of F_q , denoted by F_q^* . Hence G is a subset of F_q^* . For $1 \leq i, j \leq n$, consider $a^i \cdot a^j$. If $i + j \leq n$, $a^i \cdot a^j = a^{i+j}$, which is an element in G . If $i + j > n$, then $i + j = n + k$ with $1 \leq k < n$. In this case , $a_i \cdot a_j = a^k$, which is an element in G . Therefore , G is closed under the multiplication operation of the field . G contains the identity element 1 of the multiplicative group F_q^* of F_q . For $1 \leq i < n$, a^{n-i} is the multiplicative inverse of the element a^i . The multiplicative inverse of the identity element 1 is itself. So every element in G has a multiplicative inverse . Therefore , G is a subgroup of F_q^* . It follows that G is a cyclic subgroup of F_q^* and a is a generator of G . ■

2.7 The Galois group of finite field

Definition 2.7.1 *Let $F \subset L$ be a finite extension. Then $\text{Gal}(L/F)$ is the set*

$$\{\sigma : L \longrightarrow L \mid \sigma \text{ is an automorphism , } \sigma(a) = a \text{ for all } a \in F\}$$

In other words, $\text{Gal}(L/F)$ consists of all automorphisms of L that are the

identity on F .

Proposition 2.7.1 $(Gal(L/F), \circ)$ is a group under composition .

Proof. First suppose that σ and $\tau \in Gal(L/F)$. Then $\sigma \circ \tau$ is the composition $\sigma \circ \tau$, which is an automorphism because σ, τ are . Also, if $a \in F$, then $\sigma \circ \tau(a) = \sigma(\tau(a)) = \sigma(a) = a$, since σ, τ are the identity on F . Hence composition gives an operation on $Gal(L/F)$, which is associative by standard properties of composition .

The identity map $1_L : L \longrightarrow L$ is an isomorphism that is the identity on F , so that $1_L \in Gal(L/F)$ we can easily check that $\sigma \circ 1_L = \sigma \circ 1_L = \sigma$ for all $\sigma \in Gal(L/F)$.

Thus 1_L is the identity element of $Gal(L/F)$.

Finally, any $\sigma \in Gal(L/F)$ is an automorphism, which means that its inverse $\sigma^{-1} : L \longrightarrow L$ is also an automorphism . Also , if $a \in F$, then $a = \sigma(a)$, which implies $\sigma^{-1}(a) = \sigma^{-1}(\sigma(a)) = a$. This shows that $\sigma^{-1} \in Gal(L/F)$ and completes the proof that $Gal(L/F)$ is a group under composition . ■

Lemma 2.7.1 Let $F \subset L$ be finite , and fix $\sigma \in Gal(L/F)$. Given $h \in F[x_1, \dots, x_n]$ and $\beta_1, \dots, \beta_n$ in L then

$$\sigma(h(\beta_1, \dots, \beta_n)) = h(\sigma(\beta_1), \dots, \sigma(\beta_n)) .$$

In particular , if $h \in F[x]$ and $\beta \in L$, then

$$\sigma(h(\beta)) = h(\sigma(\beta)) .$$

Proof. This follows immediately because σ preserves addition and multiplication and is the identity on the coefficients of h . ■

Proposition 2.7.2 *Let $F \subset L$ be a finite extension, $\alpha_1, \dots, \alpha_n$ are algebraic element over F , and let $\sigma \in \text{Gal}(L/F)$. Then:*

- i. *If $h \in F[x]$ is a nonconstant polynomial with $\alpha \in L$ as a root, then $\sigma(\alpha)$ is also a root of h lying in L .*
- ii. *If $L = F(\alpha_1, \dots, \alpha_n)$, then σ is uniquely determined by its values on $\alpha_1, \dots, \alpha_n$.*

Proof. by Lemma(2.7.1) $h \in F[x]$ and $0 = h(\alpha)$ imply that

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

which shows that $\sigma(\alpha) \in L$ is also a root of h . Part (i.) follows.

Turning to part (ii.), note that $L = F[\alpha_1, \dots, \alpha_n]$, since $L = F(\alpha_1, \dots, \alpha_n)$ is a finite extension of F . Hence any $\beta \in L$ can be written

$$\beta = h(\alpha_1, \dots, \alpha_n)$$

for some polynomial $h \in F[x_1, \dots, x_n]$. by Lemma(2.7.1),

$$\sigma(\beta) = \sigma(h(\alpha_1, \dots, \alpha_n)) = h(\sigma(\alpha_1), \dots, \sigma(\alpha_n))$$

It follows that $\sigma : L \rightarrow L$ is uniquely determined by $\sigma(\alpha_1), \dots, \sigma(\alpha_n)$. ■

Corollary 2.7.1 *Let $F \subset L$ be a finite extension. Then its Galois group $\text{Gal}(L/F)$ is finite.*

Proof. Since $F \subset L$ is finite, $L = F(\alpha_1, \dots, \alpha_n)$ where each α_i is algebraic over F . Now suppose that $\sigma \in \text{Gal}(L/F)$. By part (ii.) of Proposition 15, σ is

uniquely determined by $\sigma(\alpha_1), \dots, \sigma(\alpha_n)$. Furthermore, if $p_i \in F[x]$ is the minimal polynomial of α_i , then part (i.) shows that there are at most $\deg(p_i)$ possibilities for $\sigma(\alpha_i)$. The finiteness of $\text{Gal}(L/F)$ follows immediately. ■

Example 2.7.1 *Consider the extension*

$$\mathbb{Q} \subset L = \mathbb{Q}(\sqrt[3]{2})$$

The minimal polynomial of $\sqrt[3]{2}$ over $\mathbb{Q}$ is $x^3 - 2$, which has roots $\sqrt[3]{2}, \omega\sqrt[3]{2}, \omega^2\sqrt[3]{2}$ where $\omega = \exp(2\pi i/3)$. The last two are not real and hence can't lie in L . Hence every $\sigma \in \text{Gal}(L/\mathbb{Q})$ must satisfy $\sigma(\sqrt[3]{2}) = \sqrt[3]{2}$. Since σ is uniquely determined by $\sigma(\sqrt[3]{2})$, it must be the identity. Thus $\text{Gal}(L/\mathbb{Q}) = \{1_L\}$

2.8 The Frobenius automorphism

Theorem 2.8.1 (The Frobenius automorphism) *Let F be a finite field with q elements. The mapping*

$$\begin{aligned} \varphi : F &\longrightarrow F \\ x &\longrightarrow x^p \end{aligned}$$

is an automorphism of F .

Proof. We already know that the map

$$\varphi : x \longrightarrow x^p$$

is a ring-homomorphism of F into itself. Its kernel is 0 , and since F is finite, the map has to be a bijection , so an automorphism .

The automorphism φ is called the **Frobenius automorphism** of F . It generates a cyclic group , which is finite , because F has only a finite number of elements . Let $q = p^n$. Note that

$$\varphi^n = id$$

Indeed , for any positive integer m

$$\varphi^m(x) = x^{p^m}$$

for all in F . Hence the period of φ divides n , because

$$\varphi^n(x) = x^{p^n} = x^q = x$$

■

Theorem 2.8.2 *The period of φ is exactly n .*

Proof. . Suppose the period is $m \prec n$. Then every element x of F satisfies the equation

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

the polynomial

$$t^{p^m} - 1$$

has at most p^m roots . Hence we cannot have $m \prec n$, as desired . ■

Theorem 2.8.3 *The only automorphisms of F , are the powers of the Frobenius automorphism $1, \varphi, \dots, \varphi^{n-1}$*

Proof. . Let $F_q = F_p(\alpha)$ for some element α , Then α is a root of a polynomial of degree n , if $q = p^n$. Therefore by Theorem (The Frobenius automorphism) there are at most n automorphisms of F_q , over the prime field F_p . Since $1, \varphi, \dots, \varphi^{n-1}$ constitute n distinct automorphisms , there cannot be any others .

■

Chapter 3

Some applications of finite fields

In this chapter , we will discuss some specific applications of finite fields ,
Quadratic residues modulo p , Fermat's Theorem and Linear codes .

3.1 Quadratic residues modulo p

Definition 3.1.1 Let p be a prime number. An element $a \in F_p^*$ from the multiplicative group of the finite field with p -element is called quadratic residue if there exists an element $x \in F_p$ such that

$$x^2 = a \bmod p$$

If there is no such x then a is called a quadratic non-residue .

Example 3.1.1 Let the finite field $\mathbb{Z}/19\mathbb{Z} = \{1, 2, \dots, 18\}$. we have that

$1^2 = 1 \Rightarrow 1 \bmod 19 = 1$	$4^2 = 16 \Rightarrow 16 \bmod 19 = 16$	$7^2 = 49 \Rightarrow 11 \bmod 19 = 11$
$2^2 = 4 \Rightarrow 4 \bmod 19 = 4$	$5^2 = 25 \Rightarrow 6 \bmod 19 = 6$	$8^2 = 64 \Rightarrow 7 \bmod 19 = 7$
$3^2 = 9 \Rightarrow 9 \bmod 19 = 9$	$6^2 = 36 \Rightarrow 17 \bmod 19 = 17$	$9^2 = 81 \Rightarrow 5 \bmod 19 = 5$

The values above are quadratic residues . So the Quadratic residues is 1, 4, 9, 16, 6, 17, 11, 7, 5.
And the Quadratic non residues is 2, 3, 8, 10, 12, 13, 14, 15, 18 .

Remark 3.1.1 The set of quadratic residues of F_p is denoted by $QR(p)$ and the set of quadratic non residues by $QNR(p)$.

Definition 3.1.2 (Legendre symbol) Let p be a prime. Let x be an integer. The *Legendre symbol* is the integer defined as follows :

$$\left(\frac{x}{p}\right) = \begin{cases} 0 & \text{if } p \mid x \\ 1 & \text{if } x \text{ is a QR mod } p \\ -1 & \text{if } x \text{ is a QNR mod } p \end{cases}$$

Example 3.1.2

- 2 is a QR mod 7, since $2 \equiv 3^2 \pmod{7}$. Thus, $\left(\frac{2}{7}\right) = 1$.
- 2 is a QNR mod 5, since the squares in $\mathbb{Z}/5$ are $\bar{0}, \bar{1}, \bar{4}$. Thus, $\left(\frac{2}{5}\right) = -1$.
- -1 is a QR mod 5, since $-1 \equiv 2^2 \pmod{5}$. Thus, $\left(\frac{-1}{5}\right) = 1$.
- -1 is a QNR mod 3. Thus, $\left(\frac{-1}{3}\right) = -1$.

Theorem 3.1.1 Let p be an odd prime , and $a \in F_p^*$ then

$$a \in QR(p) \Leftrightarrow a^{\frac{p-1}{2}} = 1$$

$$a \in QNR(p) \Leftrightarrow a^{\frac{p-1}{2}} = -1$$

Furthermore ,

$$|QR(p)| = |QNR(p)| = \frac{p-1}{2}$$

Proof.

the polynomial $X^{p-1} - 1 = 0$ cannot have more than $p - 1$ roots in F_p . On the other hand it does have $p - 1$ roots F_p^* : i.e, all the element of F_p^* are roots of $X^{p-1} - 1 = 0$.

Consequently, since $X^{p-1} - 1 = \left(X^{\frac{p-1}{2}} - 1\right) \left(X^{\frac{p-1}{2}} + 1\right)$ and the ring of polynomials over F_p has no (non-trivial) zero divisors, again $\left(X^{\frac{p-1}{2}} - 1\right)$ and $\left(X^{\frac{p-1}{2}} + 1\right)$ must have exactly $\frac{p-1}{2}$ root.

If $a = y^2$ is a quadratic residue in F_p then $a^{\frac{p-1}{2}} = y^{p-1} = 1$ by Lagrange's Theorem. Hence, a is a root of $X^{\frac{p-1}{2}} - 1$ implying that $|QR(p)| \leq \frac{p-1}{2}$. On the other hand the polynomial $X^2 - a$ has at most two roots for any quadratic residue a, hence

$$p - 1 = |F_p^*| \leq \sum_{a \in QR(p)} |\{X : X^2 = a\}| \leq 2 |QR(p)|$$

Concluding, $|QR(p)| = \frac{p-1}{2}$ and thus $QR(p)$ must be equal to the set of roots of $\left(X^{\frac{p-1}{2}} - 1\right)$. Then it follows that also $|QNR(p)| = \frac{p-1}{2}$, and $QNR(p)$ must be equal to the set of roots of $\left(X^{\frac{p-1}{2}} + 1\right)$

■

3.2 Fermat's Theorem

Fermat's theorem, sometimes called "Fermat's Little Theorem" to distinguish it from Fermat's Last Theorem about solutions of $x^n + y^n = z^n$, is useful in many places .

Theorem 3.2.1 *If p is prime and $(a, p) = 1$, then $a^{p-1} \equiv 1 [p]$.*

Proof. We know that if the ring $K = \mathbb{Z}/p\mathbb{Z} = \{\bar{0}, \bar{1}, \dots, \overline{p-1}\}$ is a finite field , p is a prime number . We have

$$\begin{aligned} \forall \bar{a} \in (\mathbb{Z}/p\mathbb{Z})^* : (\bar{a})^{p-1} &= \bar{1} \\ \bar{a} \neq \bar{0} &\iff p \nmid a \iff (a, p) = 1 \\ \bar{a} = \bar{0} &\iff a \text{ multiple of } p \iff a \in p\mathbb{Z} \iff p/a \\ (\bar{a})^{p-1} \equiv \bar{1} &\iff a^{p-1} \equiv 1 [p] \end{aligned}$$

■

3.3 Wilson's Theorem

Theorem 3.3.1 *An integer p , $p \geq 2$, is prime if and only if . $(p-1)! \equiv -1 [p]$*

Proof. Let $K = \mathbb{Z}/p\mathbb{Z} = \{\bar{0}, \bar{1}, \dots, \overline{p-1}\}$, p is a prime number . We know that

$$\bar{a} \in \mathbb{Z}/p\mathbb{Z} : \bar{a}^p - a = 0$$

all elements in $\mathbb{Z}/p\mathbb{Z}$ are roots of $x^p - x$, so we have

$$x^p - x = (x - \bar{0}) (x - \bar{1}) \dots (x - \overline{p-1})$$

In the group $((\mathbb{Z}/p\mathbb{Z})^*, \times)$ the multiplicative group of F_q , $x^{p-1} = p-1$

$$x^{p-1} - 1 = (x - \bar{1}) (x - \bar{2}) \dots (x - \overline{p-1})$$

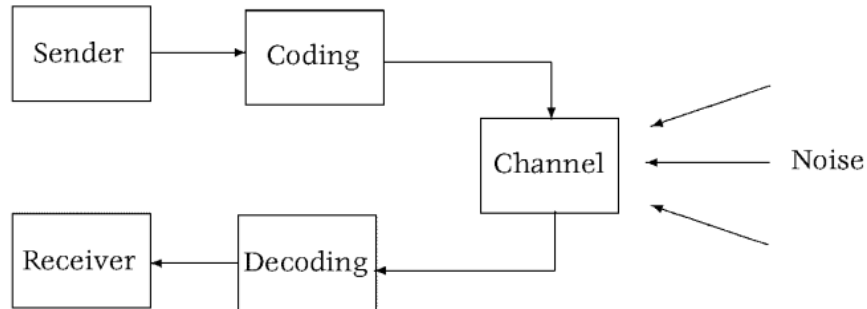
For $x = \bar{0}$

$$\begin{aligned}
 -1 &= (\bar{1}) (\bar{2}) \dots (-(p-1)) \\
 &= (-1)^{p-1} \overline{1 \times 2 \times 3 \times \dots \times (p-1)} \\
 &= (-1)^{p-1} \overline{(p-1)!} \\
 (p-1)! &\equiv -1 [p]
 \end{aligned}$$

■

3.4 Linear codes

The **sender** **encodes** their **message** and sends it through the **channel**, after which the **receiver** **decodes** it to recover the message. However, sometimes **errors** occur due to external **noise** affecting the message, such as weather and channel quality. This necessitates a certain mechanism to ensure the **correct** delivery of the message. The above can be summarized in the following diagram:



A first idea in the coding, is to repeat the message itself a number of times . Suppose **book** was the original message, We "encode" it to **bookbook**, but **book-****look** arrives due to some noise at the fifth position . For this reason, the receiver

and sender create a specific method (**coding error correction**) to ensure that the correct message is received between them .

A **finite field** form the underlying alphabet for coding. Coding consists of transforming a block of k **message symbols** $a_1...a_k$, $a_i \in F_q$, into a **codeword** $x = x_1...x_n$, $x_i \in F_q$ where $n \geq k$. It can also be represented as follows :

$$\begin{aligned} \varphi : \quad F_q^k &\longrightarrow F_q^n \\ (a_1...a_k) &\longrightarrow (x_1...x_n) \end{aligned}$$

φ is encoding mp , F_q^k and F_q^n denote the vector space of all k – *tuples* and n -tuples over the finite field F_q , i.e ,

$$\begin{aligned} F_q^k &= \underbrace{F_q \times F_q \times \dots \times F_q}_{n \text{ times}} \\ &= \{(x_1, x_2, \dots, x_k) \mid x_i \in F_q\} \end{aligned}$$

the same thing for F_q^n . With respect componentwise addition and multiplication by an elements from F_q .

Definition 3.4.1 (Code) Let F_q be a finite field with q elements and $n > 1$ be an integer . A code C of length n is a subset of F_q^n . The size of a code $C \subseteq F_q^n$ is the number of codewords denoted by $|C| = M$.

Example 3.4.1 Let $F_2 = \{0, 1\}$. Then $C = \{1111, 1010, 1110, 0001\}$ is code of length 4 over F_2 .

Definition 3.4.2 (Hamming distance) Let $x = (x_1, x_2, \dots, x_n)$ and $y = (y_1, y_2, \dots, y_n)$, where $x, y \in F_q^n$. A Hamming distance between x and y is the number of position,

in which x and y are different, denoted by $d_H(x, y)$

$$d_H(x, y) = |\{i : 1 \leq i \leq n, x_i \neq y_i\}|.$$

Example 3.4.2 Let $x = 1111$ and $y = 1010$. Then $d_H(x, y) = 2$.

Definition 3.4.3 (Hamming weight) Let $x = (x_1, x_2, \dots, x_n) \in F_q^n$. We defined the Hamming weight of x to be the number of non-zero entries in x . More formally, the Hamming weight of x is

$$w_H(x) = |\{i : x_i \neq 0\}|,$$

and

$$w_H(x) = d_H(x, 0).$$

Example 3.4.3

- Let $x_1 = (1010)$. Then $w_H(1010) = 2$.
- Let $x_2 = (1111)$. Then $w_H(1111) = 4$.

Remark 3.4.1 A minimum weight of the code C is the minimum non-zero weight among all code-words of C ,

$$w_{\min}(C) = \{\min(w_H(c)), 0 \neq c \in C\}$$

Definition 3.4.4 (Minimum distance) The minimum distance of a code C , denoted $d_{\min}(C)$ is defined to be the minimum Hamming distance between two distinct code-words of C

$$d_{\min}(C) = \min\{d_H(c_1, c_2) : c_1, c_2 \in C, c_1 \neq c_2\}.$$

Example 3.4.4

- Let $C = \{000, 110, 011, 101\}$ be a code of F_2^3 . Hence, $d_{\min}(C) = 2$.
- Let $D = \{0001, 0011, 0101, 1100\}$ be a code of F_3^4 . Hence, $d_{\min}(C) = 1$.

Definition 3.4.5 (Linear codes) Let F be a finite field . If the code C is a subspace of F_q^n . Then the code C is said to be a linear code of k -dimension , minimum distance d and length n . The cardinal of C is $|C| = M = q^k$. A q -ary linear code will be referred as an $[n, k, d]_q$ code or $[n, k, d]$ code .

Example 3.4.5 Let C be a linear code of F_3 with parameters $[5, 2, 3]$

$$C = \{00000, 11100, 22200, 00111, 00222, 11211, 22011, 11022, 22122\}.$$

Conclusion

In this work, we have studied the concept of finite fields and we have mentioned some of their applications .

The work is divided in three chapters: an introduction to the necessary background, finite fields with some of their properties, and finally the third chapter giving some of their applications .

Bibliography

- [1] F.Butin, Algebra Polynomials Galois Theory and Applications ,Dover Publications, new yourk ,2017
- [2] G . Mullen & D . Panario, Handbook Of Finite Fields, CRC Press, 2013 .
- [3] J. Durbin. Modern Algebra: An Introduction. John Wiley & Sons, 2009.
- [4] J. Howie . Fields and Galois Theory , Undergraduate Mathematics Series , Springer , (2006).
- [5] K.neal , A cours in number theory and cryptography, Spring-verlage , 1991 .
- [6] L.Ladjelat. Cours d'Anneaux et Extensins,Master 1, AMD, Universite de M'sila , 2022 .
- [7] L.ranz, Error-correcting codes , 2005 .
- [8] R. Lidl & H. Niederreiter. Introduction to finite fields and their applications , Cambridge University Press, 1986.
- [9] R. Lidl & H. Niederreiter. Finite Fields, V, 20, Cambridge University Press, 1997.
- [10] R. Lidl and G. Pilz, Applied abstract algebra, Springer Science and Business Media, 2012.

- [11] T. Judson. Abstract Algebra Theory and Applications, Stephen F, Austin State University, 2009 .
- [12] U. Dudley. A Guide to Elementary Number Theory, The Mathematical Association of America, 2009 .
- [13] W. Huffman and V. Pless, Fundamentals of error-correcting codes, Cambridge University press, 2010 .

الملخص

في هذا العمل قمنا بدراسة مفهوم الحقول المنتهية وبنيتها وبعض من خصائصها . كما تطرقنا الى بعض من تطبيقات الحقول المنتهية في نظريات الأعداد و التشفير .

الكلمات المفتاحية

حلقة , الحقول , الحقول المنتهية , مميز حقل , كثيرات الحدود , مثالي , شفرة مصححة الأخطاء .

Abstract

In this work, we have studied the concept of finite fields, their construction, and some of their properties. We have also discussed some applications of finite fields in number theory and coding theory .

Key words

Ring , fields , finite field , characteristic of a field, polynomial , ideal , error correcting codes.

Résumé

Dans ce travail , nous avons étudié le concept des corps finis, leur construction et certaines de leurs propriétés. Nous avons également discuté de quelques applications des corps finis en théorie des nombres et en théorie du codage.

Mot-clés

Corps , Corps finis , Caractéristique d'un corps, polynome, ideal, codes-correcteurs d'erreurs.