Acknowledgement

Thanks to **GOD** almighty for the completion of this work. Only due to his blessings.

I would like to express my deepest gratitude to my advisor, Mr : **D. Mihoubi**, for his invaluable advices and suggestions, I also would like to express my thanks to Mr : **L. Ladjelat**, and Mr : **L. Haboube** for her advices.

I would like to thank my beloved **parents** for their encouragement who are so supportive to me throughout my life. My sisters, brothers deserve my whole-hearted thanks as well, to all **my friends** and **all people** who have helped me during my study. This work is only a begining of my journey.

Contents

Introduction

The theory of finite fields is a branch of modern algebra that has come to the fore in the last 50 years because of its diverse applications in combinatorics, coding theory, cryptology, and the mathematical study of switching circuits, among others.

The origins of the subject reach back into the 17th and 18th centuries, with such eminent mathematicians as Pierre de Fermat (1601-1665), Leonhard Euler (1707-1783), Joseph-Louis Lagrange (1736-1813), and Adrien-Marie Legendre (1752-1833) contributing to the structure theory of special finite fields-namely, the so-called finite prime fields.

The general theory of finite fields may be said to begin with the work of Carl Friedrich Gauss (1777-1855) and Evariste Galois (1811-1832), but it only became of interest for applied mathematicians in recent decades with the emergence of discrete mathematics as a serious discipline.

The goal in this memory is how to construct a finite field of order q, identify the important properties of finite fields, and we describe Berlekamp's algorithm for computing the factorization of a polynomial over finite fields.

This work is devided into four chapters:

- The first chapter provides a reminder of the concepts and notations used for the following: binary operation, groups, rings, fields, vector spaces, field extensions.
- In the second chapter we study the construction of finite fields, where we will see finite fields, characteristic of finite fields, order of finite fields, existence and uniqueness of finite fields, quotient rings of $F[x]$, and representation of elements of finite fields.
- The third chapter examines some important properties of finite fields.
- The fourth chapter, we used some related concepts and notation for factorization of polynomials over finite fields and we describe **Berlekamp's algorithm** for computing

the factorization of a polynomial in $\mathbb{F}_q[x]$ into irreducible factors.

Chapter 1

Preliminaries

The first chapter contains definitions and objects that we use the following:

Binary operation, Groups, Cyclic groups, Subgroups, Rings, Subrings, Ideals, Polynomial rings, Quotient rings, Ring homomorphism, Fields, Subfields, Ideals in $F[x]$, Irreducible polynomials, Vector spaces, Linear independence, Field extensions, Splitting Fields.

1.1 Binary operation

Definition 1.1 *If A is a set, the direct product $A \times A$ consists of all ordered pairs $(a,\ b)$ with $a,\ b$ belongs to A. Here the term ordered pairs we have that $(a_1,\ b_1) = (a_2,\ b_2)$ if and only if $a_1 = a_2$ and $b_1 = b_2$. Using this terminology, a binary operation ,$\circ$, on a set A is just an application from $A \times A$ to A, we denote the image of the pair $(a,\ b)$ under this function by $a \circ b$. In other words, the binary operation $\circ$ assigns to any two elements a and b of A the element $a \circ b$ of A.*

- *Many symbols are used for binary operation; like $+,\ \cdot,\ -,\ \circ,\ *,\ \star,\ldots$*
- *A binary operation on a finite set can often presented conveniently by means of a table.*

1.2 Groups

Definition 1.2 *A non-empty set G is said to be a **group**, together with a binary operation "$\cdot$", which statisfies the following properties:*

(G1) *For all elements x and y of G, $x \cdot y$ is an elements of G (closure);*

(G2) *For all elements x, y and z of G,*

$$(x \cdot y) \cdot z = x \cdot (y \cdot z) \text{ (associativity);}$$

(G3) *There exists an element e of G, called the* ***identity*** *(or* ***unit****) of G, such that for all x in G we have*

$$e \cdot x = x \cdot e = x \text{ (existence of identity);}$$

(G4) *For every x in G there exists an element x^{-1} called the inverse of x, such that*

$$x \cdot x^{-1} = x^{-1} \cdot x = e \text{ (existence of inverse).}$$

We then frequently write $(G, \cdot)$, or simply G, to denote a group.

$(G, \cdot)$ also fulfills the law $x \cdot y = y \cdot x$ for all $x, y \in G$, then $(G, \cdot)$ is called a ***commutative*** *or* ***abelian group****.*

Example 1.3

The following are examples of abelian groups:

1. *$(\mathbb{Z}, +)$, $(\mathbb{R}, +)$, $(\mathbb{C}, +)$ are all abelian groups under addition.*

2. *$(\mathbb{Q}^*, \cdot)$, $(\mathbb{R}^*, \cdot)$, $(\mathbb{C}^*, \cdot)$ are all abelian groups under multiplication.*

Example 1.4 *Let G be the set of complex numbers $\{1, -1, i, -i\}$ and let "$\cdot$" be the standard multiplication of complex numbers. Then $(G, \cdot)$ is an abelian group.*

Table: Group

$\{1, -1, i, -i\}$

$\cdot$	1	-1	i	$-i$
1	1	-1	i	$-i$
-1	-1	1	$-i$	i
i	i	$-i$	-1	1
$-i$	$-i$	i	1	-1

Definition 1.5 *(****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 1.6 *If G is a finite group and $a \in G$, then $a^{|G|} = e$.*

1.2.1 Cyclic groups

Definition 1.7 *A group $(G, \cdot)$ is called **cyclic** if there exists an element $g \in G$ such that $G = \langle g \rangle = \{g^n \mid n \in \mathbb{Z}\}$. The element g is called a **generator** of the cyclic group.*

Every cyclic group is abelian because $g^r \cdot g^s = g^{r+s} = g^s \cdot g^r$.

Example 1.8

1. *The group $(\{1, -1, i, -i\}, \cdot)$ is a cyclic group of order 4 generated by i because $i^0 = 1$, $i^1 = i$, $i^2 = -1$, $i^3 = -i$, $i^4 = 1$, $i^5 = i$, and so on. Hence the group can be written as $(\{1, i, i^2, i^3\}, \cdot)$.*

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

Theorem 1.9 *(**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 1.10 *Let G be a finite abelian group $\neq \{e\}$. Then there are natural numbers s, $d_1, d_2, ..., d_s$ with $d_1 > 1$ and $d_i \mid d_{i+1}$ for $1 \leq i < s$ such that*

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

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

1.2.2 Subgroups

Definition 1.11 *A subset H of a group G is a subgroup of G if H is itself a group with respect to the operation on G.*

Example 1.12

1. *The group of integers with addition is a subgroup of the group of real numbers with addition.*

2. *With multiplication, $\{1, -1\}$ is a subgroup of the group of nonzero real numbers.*

3. Any group is a subgroup of itself.

4. If e is the identity of a group G, then $\{e\}$ is a subgroup of G.

Example 1.13 *The subgroups of $(\mathbb{Z}, +)$ are $(n\mathbb{Z}, +)$ for $n \in \mathbb{Z}$.*

1.3 Rings

Definition 1.14 *A ring $(R, +, \cdot)$ is a non-empty set R , together with two binary operations denoted by "$+$" and "$\cdot$", called **addition** $(+)$ and **multiplication** $(\cdot)$, such that:*

a. *$(R, +)$ is an abelian group.*

b. *The product $x \cdot y$ of any two elements $x, y \in R$ is in R.*

c. *"$\cdot$" is associative that is $(x \cdot y) \cdot z = x \cdot (y \cdot z)$ for all $x, y, z \in R$.*

d. *The distributive laws hold, that for all $x, y, z \in R$ we have*

$$\begin{aligned} \textit{(i)}\ z \cdot (x + y) &= z \cdot x + z \cdot y \qquad \textit{[Left distributive law]} \\ \textit{(ii)}\ (x + y) \cdot z &= x \cdot z + y \cdot z \qquad \textit{[Right distributive law]} \end{aligned}$$

We shall use R as a designation for the ring $(R, +, \cdot)$ and stress that the operations "$+$" and "$\cdot$" are not necessarily the ordinary operations with numbers. In following convention, we use 0 (called the zero element) to denote the identity element of the abelian group R with respect to addition, and the additive inverse of a is denoted by $-a$; also, $a + (-b)$ is abbreviate by $a - b$. Instead of $a \cdot b$ we will usually write ab. As a consequence of the definition of a ring one obtains the general property $a0 = 0a = 0$ for all $a \in R$. This, in turn, implies $(-a)b = a(-b) = -ab$ for all $a, b \in R$.

Definition 1.15

(i) *A ring is called a **ring with identity** or **ring with unity** if the ring has a multiplicative identity-that is, if there is an element 1 such that $a1 = 1a = a$ for all $a \in R$.*

(ii) *A ring R is said to be **commutative ring** if under multiplication*

$$ab = ba \text{ for all } a, b \in R.$$

(iii) *A ring is called an* ***integral domain*** *if it is a commutative ring with identity* $1 \neq 0$ *in which* $ab = 0$ *implies* $a = 0$ *or* $b = 0$.

Example 1.16

1. *The integers under addition and multiplication satisfy all of the axioms above, so that* $(\mathbb{Z}, +, \cdot)$ *is a commutative ring. Also,* $(\mathbb{Q}, +, \cdot)$, $(\mathbb{R}, +, \cdot)$, *and* $(\mathbb{C}, +, \cdot)$ *are all commutative rings.*

2. *Show that* $(\mathbb{Z}/n\mathbb{Z}, +, \cdot)$ *is a commutative ring, where addition and multiplication on congruence classes, modulo* n, *are defined by the equations*

$$[x] + [y] = [x + y] \text{ and } [x] \cdot [y] = [x \cdot y].$$

3. *The functions from the real numbers into the real numbers form a commutative ring with identity under the definitions for* $f + g$ *and* fg *given by* $(f + g)(x) = f(x) + g(x)$ *and* $(fg)(x) = f(x)g(x)$ *for* $x \in \mathbb{R}$.

1.3.1 Subrings

Definition 1.17 *Let* R *be a ring. A non-empty subset* S *of the set* R, *which is itself a ring with respect to the binary operations on* R, *is called a subring of* R.

Example 1.18 *The ring of integers is a subring of the ring of rational numbers. If* R *is any ring, then* R *is a subring and* $\{0\}$ *is a subring.*

1.3.2 Ideals

Definition 1.19 *A non-empty subset* I *of a ring* R *is called an ideal of* R *if the following conditions are satisfied for all* $x, y \in I$ *and* $r \in R$:

a. $(I, +)$ *is a subgroup of* $(R, +)$.

b. $x \cdot r \in I$ *and* $r \cdot x \in I$.

Example 1.20

1. *Every ring R has at least two ideals viz. $\{0\}$ and R. The ideals $\{0\}$ and R are called trivial ideals.*

2. *$n \in \mathbb{N}$, $n\mathbb{Z}$ is an ideal in $(\mathbb{Z}, +, \cdot)$.*

Proposition 1.21 *Let α be an element of a commutative ring R. The set $\{\alpha r \mid r \in R\}$ of all multiples of α is an ideal of R called the principal ideal generated by α. This ideal is denoted by (α) or $\langle\alpha\rangle$.*

Example 1.22 *For any $n \in \mathbb{Z}$, $\langle n\rangle = \{nm : m \in \mathbb{Z}\} = n\mathbb{Z}$ is a principal ideal generated by n in $\mathbb{Z}$.*

Definition 1.23 *A ring R is said to be a principal ideal ring iff every ideal I of R is of the form $I = \langle\alpha\rangle$ for some $\alpha \in R$.*

Example 1.24 *The ring $\mathbb{Z}$ is a principal ideal ring.*

1.3.3 Polynomial rings

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

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

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

The coefficient a_n is called the **leading coefficient**. A polynomial is called **monic** if the leading coefficient is 1. If n is the largest nonnegative number for which $a_n \neq 0$, we say that the **degree** of f is n and write $deg\ f(x) = n$. If no such n exists-that is, if $f = 0$ is the zero polynomial-then the degree of f is defined to be $-\infty$. Polynomials of degree ≤ 0 are called **constant polynomials**. We will denote the set of all polynomials with coefficients in a ring R by $R[x]$. Two polynomials are equal exactly when their corresponding coefficients are equal; that is, if we let

$$\begin{aligned} p(x) &= a_0 + a_1 x + \cdots + a_n x^n \\ q(x) &= b_0 + b_1 x + \cdots + b_m x^m, \end{aligned}$$

then $p(x) = q(x)$ if and only if $a_i = b_i$ for all $i \geq 0$.

For example, $4x^2 - 2$ is a polynomial over $\mathbb{R}$ of degree 2, $ix^4 - (2+i)x^3 + 3x$ is a polynomial over $\mathbb{C}$ of degree 4.

To show that the set of all polynomials forms a **ring**, we must first define addition and multiplication. We define the sum of two polynomials as follows. Let

$$\begin{aligned} p(x) &= a_0 + a_1 x + \cdots + a_n x^n \\ q(x) &= b_0 + b_1 x + \cdots + b_m x^m. \end{aligned}$$

Then the sum of $p(x)$ and $q(x)$ is

$$p(x) + q(x) = c_0 + c_1 x + \cdots + c_k x^k,$$

where $c_i = a_i + b_i$ for each i. We define the product of $p(x)$ and $q(x)$ to be

$$p(x)q(x) = c_0 + c_1 x + \cdots + c_{m+n} x^{m+n},$$

where

$$c_i = \sum_{k=0}^{i} a_k b_{i-k} = a_0 b_i + a_1 b_{i-1} + \cdots + a_{i-1} b_1 + a_i b_0$$

for each i. Notice that in each case some of the coefficients may be zero.

Let p, $q \in R[x]$. We say that p divides q (denoted by $p \mid q$) if $q = p \cdot r$ for some $r \in R[x]$.

Example 1.25 *Suppose that*

$$p(x) = 3 + 0x + 0x^2 + 2x^3 + 0x^4$$

and

$$q(x) = 2 + 0x - x^2 + 0x^3 + 4x^4$$

are polynomials in $\mathbb{Z}[x]$. If the coefficient of some term in a polynomial is zero, then we usually just omit that term. In this case we would write $p(x) = 3 + 2x^3$ and $q(x) = 2 - x^2 + 4x^4$. The sum of these two polynomials is

$$p(x) + q(x) = 5 - x^2 + 2x^3 + 4x^4.$$

The product,

$p(x)q(x) = (3 + 2x^3)(2 - x^2 + 4x^4) = 6 - 3x^2 + 4x^3 + 12x^4 - 2x^5 + 8x^7$,

can be calculated either by determining the c_i's in the definition or by simply multiplying polynomials in the same way as we have always done.

1.3.4 Quotient rings

In this section we continue the discussion of ideals. An ideal of a ring produces a new ring, called a quotient ring, which is closely related to the mother ring in a natural way.

Let $(R, +, \cdot)$ be a ring and I an ideal of R. Then $(I, +)$ is a subgroup of the abelian group $(R, +)$. And hence the quotient group $(R/I, +)$ is defined under usual addition of cosets, i.e., $(a + I) + (b + I) = a + b + I$, $\forall a, b \in R$. In this group, the identity element is the trivial coset I and the inverse of $a + I$ is $-a + I$, $\forall a \in R$.

Theorem 1.26 *Given an ideal I of a ring $(R, +, \cdot)$, the natural (usual) addition and multiplication of cosets, namely, $(a + I) + (b + I) = a + b + I$ and $(a + I)(b + I) = ab + I$ $\forall a, b \in R$, make $(R/I, +, \cdot)$ a ring.*

Definition 1.27 *Given an ideal I of a ring R, the ring R/I is called the quotient ring or factor ring of R by I (or modulo I).*

1.3.5 Ring homomorphism

A morphism between two rings is a function between their underlying sets that preserves the two operations of addition and multiplication and also the element 1. Many authors use the term homomorphism instead of morphism.

Definition 1.28 *Let $(R, +_R, \cdot_R)$ and $(S, +_S, \cdot_S)$ be rings.*

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

(i) $\phi(a +_R b) = \phi(a) +_S \phi(b)$ *for all $a, b \in R$,*

(ii) $\phi(a \cdot_R b) = \phi(a) \cdot_S \phi(b)$ *for all $a, b \in R$, and*

(iii) $\phi(1_R) = 1_S$ *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 $\phi : R \to R$ is called an **automorphism** of R.*

Example 1.29

1. Let R be a ring and I be an ideal.

$$\phi \quad : \quad R \quad \rightarrow \quad R/I, \;\; \phi(r) = r + I$$

is a ring homomorphism.

2. *Let R be a commutative ring and let $a \in R$.*

$$\phi \quad : \quad R[x] \quad \rightarrow \quad R, \;\; \phi(f(x)) = f(a)$$

is a ring homomorphism.

Example 1.30

1. *Let $R = \mathbb{Z}$ and $I = n\mathbb{Z}$ for some $n > 1$. We have that the quotient ring $R/I = \mathbb{Z}/n\mathbb{Z}$ is isomorphic to $\mathbb{Z}_n$(as a ring).*
2. *Let $R = \mathbb{R}[x]$, the ring of polynomials with real coefficients and $I = (x^2+1)R = \{(x^2+1)f : f \in R\}$, the principal ideal of R generated by x^2+1. We have that the quotient ring $R/I = \mathbb{R}[x]/(x^2+1)R$ is isomorphic to $\mathbb{C}$ (complex numbers).*

Definition 1.31 *Let $\phi \quad : \quad R \quad \rightarrow \quad S$ be a ring homomorphism.*
The set $\ker\phi = \{r \in R : \phi(r) = 0_S\}$ is called the kernel of ϕ.

Theorem 1.32 ***(First isomorphism theorem)***
Let R and S be commutative rings and $\phi \quad : \quad R \quad \rightarrow \quad S$ a ring homomorphism. Then:

(i) *$\ker\phi$ is an ideal of R,*

(ii) *The quotient ring $R/\ker\phi$ is isomorphic to $\phi(R)$.*

1.4 Fields

Definition 1.33 *A field consists of a set F and two binary operations "+" (addition) and "·" (multiplication), defined on R, for which the following conditions are satisfied:*

a. $(F, +, \cdot)$ *is a ring.*

b. *Multiplicative commutative: For any* $a, b \in F$, $a \cdot b = b \cdot a$.

c. *Multiplicative identity: There exists* $1 \in F$ *such that* $a \cdot 1 = 1 \cdot a = a$ *for all* $a \in F$.

d. *Multiplicative inverse: If* $a \in F$ *and* $a \neq 0$, *there exists* $b \in F$ *such that* $a \cdot b = b \cdot a = 1$.

Example 1.34

1. *The rings* $(\mathbb{Q}, +, \cdot)$, $(\mathbb{R}, +, \cdot)$, *and* $(\mathbb{C}, +, \cdot)$ *are all fields, but the integers do not form a field.*

2. *The set* $\mathbb{Z}/p\mathbb{Z}$, *where* p *is prime is a field.*

Remark 1.35 *The property appearing in definition 1.15 (iii) namely, that* $ab = 0$ *implie* $a = 0$ *or* $b = 0$ *is expressed by saying that there are no zero divisors. In particular, a field has no zero divisors, for if* $ab = 0$ *and* $a \neq 0$, *then multiplication by* a^{-1} *yields* $b = a^{-1}0 = 0$.

Definition 1.36 *Let* F *be a field and* $f(x)$, $g(x)$, $p(x) \in F[x]$ *with* $p(x)$ *nonzero. Then* $f(x)$ *is congruent to* $g(x)$ *modulo* $p(x)$ *written* $f(x) \equiv g(x) \pmod{p(x)}$ *provided that* $p(x)$ *divides* $f(x) - g(x)$.

If F is again an arbitrary field and $f(x) \in F[x]$, then replacement of the indeterminate x in $f(x)$ by a fixed element of F yields a well-defined element of F.

In detail, if $f(x) = a_0 + a_1x + \cdots + a_nx^n \in F[x]$ and $b \in F$, then replacing x by b we get $f(b) = a_0 + a_1b + \cdots + a_nb^n \in F$. In any polynomial identity in $F[x]$ we can substitute a fixed $b \in F$ for x and obtain valid identity in F (principle of substitution).

Theorem 1.37 ***(Euclidean division)*** *Let* F *be a field and* f, $g \in F[x]$ *with* $g \neq 0$. *Then there exist uniquely determined* q, $r \in F[x]$ *with* $f = gq + r$ *and deg* $r <$ *deg* g.

Definition 1.38 *An element* $b \in F$ *is called a root (or a zero) of the polynomial* $f \in F[x]$ *if* $f(b) = 0$.

Example 1.39

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

2. *The polynomial* $x^2 + 1 \in \mathbb{Q}[x]$ *has no roots in* $\mathbb{Q}$, *but two roots* $\pm\, i \in \mathbb{C}$.

Definition 1.40 *If* $f(x) = a_0 + a_1x + a_2x^2 + \cdots + a_nx^n \in F[x]$, *then the derivative*

$$f' = f'(x) = a_1 + 2a_2x + \cdots + na_nx^{n-1} \in F[x].$$

Theorem 1.41 *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'.

Example 1.42 *Consider the polynomial* $f = x^3 - 7x^2 + 16x - 12 \in \mathbb{Q}[x]$. *It factors as* $(x-2)^2(x-3)$, *so its roots are* 2 *(with multiplicity* 2*) and* 3 *(with multiplicity* 1*). Here,* $f' = 3x^2 - 14x + 16$ *which factors as* $(x-2)(3x-8)$, *so we can verify that* 2 *is also a root of* f'.

We now introduce the notion of greatest common divisor.

Theorem 1.43 *Let* F *be a field and* $f,\ g \in F[x]$ *with* $f \neq 0$ *or* $g \neq 0$. *Then there exists exactly one* $d \in F[x]$ *which enjoys the following properties:*

(i) $d \mid f$ *and* $d \mid g$;

(ii) d *is monic;*

(iii) *if* $c \mid f$ *and* $c \mid g$, *then* $c \mid d$.

For this d there exist $p,\ q \in F[x]$ with $d = pf + qg$.

The polynomial d in (1.43) is called the **greatest common divisor** of f and g, denoted by $\gcd(f,\ g)$.

1.4.1 Subfields

Definition 1.44 *A subfield of a field* F *is a subset of* F *which is itself a field with the same operations as* F.

Example 1.45 $\mathbb{Q}$ *is a subfield of* $\mathbb{R}$, $\mathbb{R}$ *is a subfield of* $\mathbb{C}$.

1.4.2 Ideals in $F[x]$

Let F be a field. Recall that a principal ideal in $F[x]$ is an ideal $\langle f(x)\rangle$ generated by some polynomial $f(x)$; that is,

$$\langle f(x)\rangle = \{f(x)q(x) : q(x) \in F[x]\}.$$

Example 1.46 *The polynomial x^2 in $F[x]$ generates the ideal $\langle x^2\rangle$ consisting of all polynomials with no constant term or term of degree* 1.

Lemma 1.47 *$F[x]$ is a principal ideal ring.*

1.4.3 Irreducible polynomials

Definition 1.48 *A polynomial $p \in F[x]$ is said to be irreducible over F (or irreducible in $F[x]$, or prime in $F[x]$) if p has positive degree and $p = bc$ with b, $c \in F[x]$ implies that either b or c is a constant polynomial.*

Briefly stated, a polynomial of positive degree is irreducible over F if it allows only trivial factorizations. A polynomial in $F[x]$ of positive degree that is not irreducible over F is called reducible over F. The reducibility or irreducibility of a given polynomial depends heavily on the field under consideration. For instance, the polynomial $x^2 - 2 \in \mathbb{Q}[x]$ is irreducible over the field $\mathbb{Q}$ of rational numbers, but $x^2 - 2 = (x + \sqrt{2})(x - \sqrt{2})$ is reducible over the field of real numbers.

Proposition 1.49 *A polynomial f, irreducible over the field F, has a root in F if and only if* $\deg\ f = 1$.

Theorem 1.50 *The polynomial $f \in F[x]$ of degree* 2 *or* 3 *is irreducible in $F[x]$ if and only if f has no root in F.*

Proof. The necessity of the condition was already noted. Conversely, if f has no root in F and were reducible in $F[x]$, we could write $f = gh$ with g, $h \in F$ and $1 \leq \deg(g) \leq \deg(h)$. But $\deg(g) + \deg(h) = \deg(f) \leq 3$, hence $\deg(g) = 1$; that is, $g(x) = ax + b$ with a, $b \in F$, $a \neq 0$. Then $-ba^{-1}$ is a root of g, and so a root of f in F, a contradiction. ■

Example 1.51 *Because of theorem 1.50, the irreducible polynomials in* $\mathbb{Z}/2\mathbb{Z}[x]$ *of degree* 2 *or* 3 *can be obtained by eliminating the polynomials with roots in* $\mathbb{Z}/2\mathbb{Z}$ *from the set of all polynomials in* $\mathbb{Z}/2\mathbb{Z}[x]$ *of degree* 2 *or* 3. *The only irreducible polynomial in* $\mathbb{Z}/2\mathbb{Z}[x]$ *of degree* 2 *is* $f(x) = x^2 + x + 1$, *and the irreducible polynomials in* $\mathbb{Z}/2\mathbb{Z}$ $[x]$ *of degree* 3 *is* $f_1(x) = x^3 + x + 1$ *and* $f_2(x) = x^3 + x^2 + 1$.

Example 1.52 *Consider the polynomial* $x^2 + x + 2$ *in* $\mathbb{Z}/3\mathbb{Z}[x]$. *This polynomial has no roots in* $\mathbb{Z}/3\mathbb{Z}$ *so it is irreducible over* $\mathbb{Z}/3\mathbb{Z}$.

Theorem 1.53 *(**Unique factorization in** $F[x]$) Any polynomial* $f \in F[x]$ *of positive degree can be written in the form*

$$f = ap_1^{e_1} \cdots p_k^{e_k}.$$

where $a \in F$, $p_1, \ldots, p_k$ *are distinct manic irreducible polynomials in* $F[x]$, *and* $e_1, \ldots, e_k$ *are positive integers. Moreover, this factorization is unique apart from the order in which the factors occur.*

1.5 Vector spaces

Definition 1.54 *:*

*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).*

$\mu : F \times V \to V$, *the image of* (α, v) *under* μ *is denoted by* αv, *satisfying the following conditions:*

V(1) $1v = v$, *where* 1 *is the multiplicative identity in* F;

V(2) $(\alpha\beta)v = \alpha(\beta v)$;

V(3) $(\alpha + \beta)v = \alpha v + \beta v$;

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

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

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

and scalar multiplication by

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

Example 1.56 *If F is a field, then $F[x]$ is a vector space over F. The vectors in $F[x]$ are simply polynomials. Vector addition is just polynomial addition. If $\alpha \in F$ and $f(x) \in F[x]$. Then scalar multiplication is defined by $\alpha f(x)$.*

Let V be any vector field over a field F and suppose that v_1, v_2,..., v_n are vectors in V and α_1, α_2,..., α_n are scalars in F. Any vector w in V of the form

$$w = \sum_{i=0}^{n} \alpha_i v_i = \alpha_1 v_1 + \alpha_2 v_2 + \cdots + \alpha_n v_n$$

is called a linear combination of the vectors v_1, v_2,..., v_n. The spanning set of vectors v_1, v_2,..., v_n is the set of vectors obtained from all possible linear combinations of v_1, v_2,..., v_n. If W is the spanning set of v_1, v_2,..., v_n then we often say that W is spanned by v_1, v_2,..., v_n.

1.5.1 Linear independence

Let $S = \{v_1, v_2,\ldots, v_n\}$ be a set of vectors in a vector space V. If there exist scalars α_1, α_2,..., $\alpha_n \in F$ such that not all of the α_i's are zero and

$$\alpha_1 v_1 + \alpha_2 v_2 + \cdots + \alpha_n v_n = 0,$$

then S is said to be **linearly dependent**. If the set S is not linearly dependent, then it is said to be **linearly independent**. More specifically, S is a

$$\alpha_1 v_1 + \alpha_2 v_2 + \cdots + \alpha_n v_n = 0$$

implies that

$$\alpha_1 = \alpha_2 = \cdots = \alpha_n = 0$$

for any set of scalars $\{\alpha_1, \alpha_2, \ldots, \alpha_n\}$.

A set $\{e_1, e_2, \ldots, e_n\}$ of vectors in a vector space V is called a basis for V if $\{e_1, e_2, \ldots, e_n\}$ is a linearly independent set that spans V.

Example 1.57 *The vectors $e_1 = (1, 0, 0)$, $e_2 = (0, 1, 0)$, and $e_3 = (0, 0, 1)$ form a basis for $\mathbb{R}^3$. The set certainly spans $\mathbb{R}^3$, since any arbitrary vector (x_1, x_2, x_3) in $\mathbb{R}^3$ can be written as $x_1e_1 + x_2e_2 + x_3e_3$. Also, none of the vectors e_1, e_2, e_3 can be written as a linear combination of the other two; hence, they are linearly independent.*

- If $\{e_1, e_2, \ldots, e_n\}$ is a basis for a vector space V, then we say that the dimension of V is n and we write $\dim V = n$.

1.6 Field extensions

Definition 1.58

If F and E are fields and $F \subseteq E$, we say that E is an extension of F, and we write $E \leq F$, or sometimes E/F.

If E is an extension of F, then in particular E is an abelian group under addition, and we may multiply the "vector" $x \in E$ by the "scalar" $\lambda \in F$, and the axioms of a vector space are satisfied. Thus if $E \leq F$, then E is a vector space over F. The dimension of this vector space is called the degree of the extension, written $[E : F]$. If $[E : F] = n < \infty$, we say that E is a finite extension of F, or that the extension E/F is finite, or that E is of degree n over F.

Example 1.59 *Let $p(x)$ be a polynomial of degree n irreducible over the field F, so that the quotient ring*

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

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

Example 1.60 *Let $F = \mathbb{R}$, $E = \mathbb{C} = \{x + iy \mid x, y \in \mathbb{R}\}$, so $\dim_{\mathbb{R}}(\mathbb{C}) = 2$ and $\{1, i\}$ is a basis of $\mathbb{C}$. So $[\mathbb{C} : \mathbb{R}] = 2$.*

Theorem 1.61 ***(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 1.62 *(**minimal polynomial**) Let E/F be a field extension, α an element 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 1.63 *x^2+1 is the minimal polynomial of i over $\mathbb{R}$ and $[\mathbb{C}:\mathbb{R}]=2$.*

Proposition 1.64 *A minimal polynomial is irreducible. Let E/F be a field extension over F as above, $\alpha \in E$, and $f \in F[x]$ a minimal polynomial for α. Suppose $f = gh$, where g, $h \in F[x]$ are of lower degree than f. Now $f(\alpha)=0$. Since fields are also integral domains, we have $g(\alpha)=0$ or $h(\alpha)=0$. This contradicts the minimality of the degree of f. Thus minimal polynomials are irreducible.*

For simplicity, we shall use the notation

$$F[\alpha] = \{a_0 + a_1\alpha + \cdots a_n\alpha^n \mid n \in \mathbb{N}_0,\, a_i \in F\}.$$

Proposition 1.65 *Let K be a field extension of F and $\alpha \in K$. Then*

$F(\alpha) = \{f(\alpha)/g(\alpha)$, where $f(x)$, $g(x) \in F[x]$ and $g(\alpha) \neq 0\}$ is the quotient field of $F[\alpha]$.

Definition 1.66 *(**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 1.67 *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 1.68 *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 1.69 *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 1.70 *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 α in K.*

(ii) *If f in (i) is of degree n then, $1, \alpha, \ldots, \alpha^{n-1}$ 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*

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

Remark 1.71 *Every finite extension field E of a field F is an algebraic extension.*

1.6.1 Splitting Fields

Definition 1.72 *Let $f \in K[x]$ be of positive degree and F an extension field of K. Then f is said to split in F if f can be written as a product of linear factors in $F[x]$ that is, if there exist elements $\alpha_1, \alpha_2, \ldots, \alpha_n \in F$ such that*

$$f = a(x - \alpha_1)(x - \alpha_2)\cdots(x - \alpha_n),$$

*where a is the leading coefficient of f. The field F is a **splitting field** of f over K.*

Example 1.73

(1) *$\mathbb{C}$ is a splitting field for $x^2 + 1$ over $\mathbb{R}$;*

(2) *$\mathbb{Q}$ is a splitting field for $x^2 - 4$ over $\mathbb{Q}$.*

Theorem 1.74 *(**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.*

Chapter 2

Construction of finite fields

In this chaptre we investigate the structure of finite fields; these fields are called Galois fields in honor of the mathematician **Evariste Galois** (1811-1832).

We will see the following concepts:

Finite fields, Characteristic of finite fields, Order of finite fields, Existence and uniqueness of finite fields, Quotient rings of $F[x]$, Representation of elements of finite fields.

2.1 Finite fields

Definition 2.1 *A finite field is a field which has a finite number of elements, this number being called the order of the field.*

Example 2.2 *For every prime p, the set* $\mathbb{Z}/p\mathbb{Z} = \{0, 1, \cdots, p-1\}$ *forms a finite field under mod-p addition and multiplication.*

Notation 2.3 *We note that when p is a prime the field* $\mathbb{F}_p$ *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 2.4 *Table* 1 *and* 2 *shows module-*2 *addition and multiplication respectively for* $\mathbb{F}_p$, *here p equals* 2*:-*

Table 1

Modulo-2 addition

+	0	1
0	0	1
1	1	0

Table 2

Modulo-2 multiplication

·	0	1
0	0	0
1	0	1

Example 2.5 *The results for* $\mathbb{F}_3$ *are shown in tables* 3 *and* 4 *where* p *here is equal to* 3*:-*

Table 3

Addition in $\mathbb{F}_3$

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

Table 4

Multiplication in $\mathbb{F}_3$

·	0	1	2
0	0	0	0
1	0	1	2
2	0	2	1

2.1.1 Characteristic of finite fields

Definition 2.6 *A field containing no proper subfields is called a prime field.*

By the above argument, any finite field of orde p*,* p *prime, is a prime field. Another example of a prime field is the field* $\mathbb{Q}$ *of rational numbers.*

For a ring R, an integer $n \geq 1$ and $a \in R$, we denote by na or $n \cdot a$ the element

$$\sum_{i=1}^{n} a = \underbrace{a + a + \cdots + a}_{n}.$$

Definition 2.7 *For any ring* R*, there exists the identity element* 1*. Consider the homomorphism*

$$\begin{array}{rccc} \phi & : & \mathbb{Z} & \longrightarrow & R \\ & & n & \mapsto & n \cdot 1 \end{array}$$

where $n \cdot 1$ *simple means adding* 1*, in* R*,* n *times. And* $\mathbb{Z}$ *being a PID (**principal ideal domain**), the kernel of this map will be of the form* $m\mathbb{Z}$*. This number* m *is called the characteristic of the ring.*

In other words, the characteristic is the smallest positive integer number m such that m times the identity element is zero. For example, the characteristic of the ring $\mathbb{F}_p$ is p for any prime p.

However, it is possible that $m \cdot 1$ will never be zero. For example, take the rings like $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, $\mathbb{Q}[x]$ etc. The corresponding map will hence have a trivial kernel and that is the ideal $0\mathbb{Z}$. Hence the characteristics of these rings is 0 and not infinity. This is just the language. Infact, we shall refer characteristic 0 rings as rings of infinite characteristic.

Here is a trivial lemma.

Lemma 2.8 *Let R be a ring (with identity) of characteristic m and S be a ring that contains R. Then characteristic of S is also m.*

Proof. R has characteristic m implies that $\phi \;:\; \mathbb{Z} \longrightarrow R$ has the kernel as $m\mathbb{Z}$. The homomorphism works just on the identity element of R and hence would be exactly the same on S (since S has to share its identity element with R). Thus, since the homomorphism is the same, the kernel has to be the same. ■

Characteristic of fields

Now, suppose m is the characteristic of any ring R. Then by definition the kernel of the map ϕ is $m\mathbb{Z}$. And by the isomorphism theorem, we know that the following map is injective:

$$\phi \;:\; \mathbb{Z}/m\mathbb{Z} \longrightarrow R$$

And therefore, in a way, a copy of $\mathbb{Z}/m\mathbb{Z}$ is sitting inside R. Thus, $\mathbb{Z}/m\mathbb{Z}$ is a subring of R.

Now let us look at the characteristic of fields instead of rings. Let us take the identity element and just keep adding it. Either, for some m we have $m \cdot 1 = 0$ or it just keeps going on. If it becomes 0, we know that the field has characteristic m. The other case is the characteristic 0 case. Now, can it be possible that m is composite? Suppose $m = pq$ where both $p, q < m$. Since we know that $m \cdot 1 = 0$, this means that $(p \cdot 1) \cdot (q \cdot 1) = pq \cdot 1 = 0$. And by our assumption, we know that neither $p \cdot 1$ nor $q \cdot 1$ is zero; we just showed the existence of zero divisors in a field! That is not possible. Hence summarizing as a theorem:

Theorem 2.9 *Any field F must either have 0 characteristic or a characteristic that is a prime.*

Let us pick any field F whose characteristic is a prime p. We know that if we let 1 'generate' a subfield of its own by just adding itself, it would get to $\mathbb{Z}/p\mathbb{Z}$. Thus for any field of prime characteristic, it should contain $\mathbb{Z}/p\mathbb{Z}$. We shall refer to $\mathbb{Z}/p\mathbb{Z}$ by $\mathbb{F}_p$.

For a field of infinite characteristic (characteristic 0, just language), 1 would keep being added on without ever giving a 0. Thus it would generate the entire set of positive integers. And since additive inverses should exist, the negative integers should also belong to the field. And further, because of the multiplicative inverses, all rational numbers should exist.

Hence, every field either contains $\mathbb{F}_p$ or $\mathbb{Q}$.

Please keep in mind that finite characteristic does not mean finite cardinality. As a counter example, look at the following set:

$$\mathbb{F}_p(X) = \left\{ \frac{f(X)}{g(X)} : f,\, g \in \mathbb{F}_p[X],\, g \neq 0 \right\}$$

that the set of rational functions over one variable. This field has infinite cardinality and since it contains $\mathbb{F}_p$ has characteristic p.

Now let us take any finite field F. Then this field must have characteristic that is not zero. Why? Since if it did have characteristic zero, it would contain $\mathbb{Q}$ and hence be infinite.

- **Since the characteristic of this field is finite, say p, it contains $\mathbb{F}_p$. Recall that if F is a field that contains another field K (in our case $\mathbb{F}_p$), then F is an extension of K.**

Thus, this tells us that any field of characteristic p is a vector space over $\mathbb{F}_p$.

2.1.2 Order of finite fields

Theorem 2.10 *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 $\dim_{F_p}(F : \mathbb{F}_p) = n$ and let $\{\zeta_1, \ldots, \zeta_n\}$ be a basis.

Then every element $a \in F$ can be represented via a linear combination of the basis elements with coefficients in $\mathbb{F}_p$. So there exist $c_1, \ldots, c_n \in F_p$ satisfying $a = c_1\zeta_1 + \cdots + c_n\zeta_n$.

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 $|F| = p^n$. ■

2.1.3 Existence and uniqueness of finite fields

Lemma 2.11 *If F is a finite fields 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.

Proof. The polynomial $x^q - x$ of degree q has at most q roots in F. By (Lemma 3.1) 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 2.11.

Theorem 2.12 *(**Existence and uniqueness of finite fields**) 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 $\mathbb{F}_p$.*

Proof. (Existence) For $q = p^n$ consider $x^q - x$ in $\mathbb{F}_p[x]$. and let F be its splitting field over $\mathbb{F}_p$. This polynomial has q distinct roots in F since its derivative is $qx^{q-1} - 1 = -1$ in $\mathbb{F}_p[x]$ and so can have no common root with $x^q - x$ (compare with theorem (1.41). Let $S = \{a \in F : a^q - a = 0\}$. Then S is a subfield of F since: (i) S contains 0 and 1; (ii) a, $b \in S$ implies by lemma (Freshman's Dream) that $(a - b)^q = a^q - b^q = a - b$, and so $a - b \in S$; (iii) 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 $\mathbb{F}_p$ as a subfield. It follows from lemma 2.11 that F is a splitting field of $x^q - x$ over $\mathbb{F}_p$. Thus the desired result is a consequence of the uniqueness (up to isomorphisms) of splitting fields, which was noted in theorem (1.74). ■

The uniqueness part of theorem 2.12 provides the justification for speaking of the finite field (or the Galois field) with q elements, or of the finite field (or the Galois field) of order q. We shall denote this field by $\mathbb{F}_q$, where it is of course understood that q is a power of the prime characteristic p of $\mathbb{F}_q$. The notation $GF(q)$ is also used by many authors.

Remark 2.13 *For each prime power $q = p^n$ we define $\mathbb{F}_q = \mathbb{F}_{p^n}$ to be the field extension of $\mathbb{F}_p$ generated by adjoining all the roots of $x^q - x$ (the splitting field of $x^q - x$ over $\mathbb{F}_p$).*

2.2 Quotient rings of $F[x]$

If F is a field, the quotient rings of the polynomial ring $F[x]$ form an important class of rings that will be used to construct new fields. Recall that $F[x]$ is a principal ideal ring, so that any quotient ring is of the form $F[x]/(p(x))$. for some polynomial $p(x) \in F[x]$. We now look at the structure of such a quotient ring.

Suppose f is a polynomial of degree k over F. Let $g + (f)$ be an arbitrary element in $F[x]/(f)$. By euclidean division 1.37, we get h, $r \in F[x]$ with $g = hf + r$, where $\deg r < k$. Since $hf \in (f)$, it follows that $g + (f) = r + (f)$. Hence each element of $F[x]/(f)$ can be uniquely expressed in the form

$$a_0 + a_1 x + \cdots + a_{k-1} x^{k-1} + (f), \qquad a_i \in F. \tag{2.2.1}$$

If we identify F with the subring $\{a + (f) \mid a \in F\}$ of $F[x]/(f)$, then the element in (2.2.1) can be written as $a_0 + a_1(x + (f)) + \cdots + a_{k-1}(x + (f))^{k-1}$. If $x + (f) = \alpha$, we can write this uniquely as

$$a_0 + a_1\alpha + \cdots + a_{k-1}\alpha^{k-1} \tag{2.2.2}$$

and we may regard $F[x]/(f)$ as a vector space over F with basis $\{1, \alpha, \alpha^2, \ldots, \alpha^{k-1}\}$.

Since $0 + (f)$ is the zero element of $F[x]/(f)$, we have $\bar{f}(x) = f + (f) = 0 + (f)$, i.e., α is a root of f. Clearly, α is an element in $F[x]/(f)$ but in general not in F. Thus the elements in $F[x]/(f)$ of the form (2.2.2) can be regarded so that α is an element with the property that $f(\alpha) = 0$.

Theorem 2.14 *Let F be a field and $f \in F[x]$ with* deg $f = k$. *Then*

$F[x]/(f) = \{a_0 + a_1\alpha + \cdots + a_{k-1}\alpha^{k-1} \mid a_i \in F\}$ *is a k-dimensional vector space over F with basis $\{1, \alpha, \alpha^2, \ldots, \alpha^{k-1}\}$, where $\alpha = [x] = x + (f)$. We have $f(\alpha) = 0$ and $F[x]/(f)$ is a field iff f is irreducible.*

Example 2.15 *Let F be the field $\mathbb{Z}_2 = \{0, 1\}$; then $f(x) = x^2 + x + 1$. is an irreducible polynomial of degree 2 over $\mathbb{Z}_2$. Hence $\mathbb{Z}_2[x]/(x^2 + x + 1)$ is a field whose elements can be represented in the form $a + b\alpha$, $a, b \in \mathbb{Z}_2$, where α satisfies $\bar{f}(\alpha) = 0$, i.e., $\alpha^2 + \alpha + 1 = 0$, which means that $\alpha^2 = \alpha + 1$, due to $-1 = 1$ in $\mathbb{Z}_2$. Hence $\mathbb{Z}_2[x]/(x^2 + x + 1)$ is a field with four elements:*

$$\mathbb{Z}_2[x]/(x^2 + x + 1) = \{0, 1, \alpha, \alpha + 1\}.$$

For instance, $\alpha \cdot (1 + \alpha) = \alpha + \alpha^2 = \alpha + \alpha + 1 = 1$. The addition and multiplication tables are given by

$+$	0	1	α	$1+\alpha$
0	0	1	α	$1+\alpha$
1	1	0	$1+\alpha$	α
α	α	$1+\alpha$	0	1
$1+\alpha$	$1+\alpha$	α	1	0

$\cdot$	0	1	α	$1+\alpha$
0	0	0	0	0
1	0	1	α	$1+\alpha$
α	0	α	$\alpha+1$	1
$1+\alpha$	0	$1+\alpha$	1	α

2.3 Representation of elements of finite fields

Definition 2.16 *(**Primitive element**) An element α in a finite field $\mathbb{F}_q$ is called a primitive element (or generator) of $\mathbb{F}_q$ if $\mathbb{F}_q = \{0, \alpha, \alpha^2, \ldots, \alpha^{q-1}\}$.*

Theorem 2.17 *Let $\mathbb{F}_q$ be a finite field and $\mathbb{F}_r$ a finite extension field. Then*

$\mathbb{F}_r$ is a simple extension of $\mathbb{F}_q$, i.e $\mathbb{F}_r = \mathbb{F}_q(\beta)$ for some $\beta \in \mathbb{F}_r$.

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

Corollary 2.18 *For every finite field $\mathbb{F}_q$ and every positive integer n there exists an irreducible polynomial in $\mathbb{F}_q[x]$ of degree n.*

Proof. *Let $\mathbb{F}_r$ be the extension field of $\mathbb{F}_q$ of order q^n, so that $[\mathbb{F}_r : \mathbb{F}_q] = n$. By theorem (2.17) we have $\mathbb{F}_r = \mathbb{F}_q(\zeta)$ for some $\zeta \in \mathbb{F}_r$. Then the minimal polynomial of ζ over $\mathbb{F}_q$ is an irreducible polynomial in $\mathbb{F}_q[x]$ of degree n.* ■

Theorem 2.19 *For a prime p and a monic irreducible $f(x)$ in $\mathbb{F}_p[x]$ of degree n, the ring $\mathbb{F}_p[x]/(f(x))$ is a field of order p^n.*

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

$$a_0 + a_1 x + \cdots + a_{n-1}x^{n-1}, \qquad a_i \in \mathbb{F}_p,$$

and there are p^n of these. Since the modulus $f(x)$ is irreducible, the ring $\mathbb{F}_p[x]/(f(x))$ is a field by theorem (2.14). ■

Example 2.20

1. *Two fields of order 8 are $\mathbb{F}_2[x]/(x^3 + x + 1)$ and $\mathbb{F}_2[x]/(x^3 + x^2 + 1)$.*
2. *Two fields of order 9 are $\mathbb{F}_3[x]/(x^2 + 1)$ and $\mathbb{F}_3[x]/(x^2 + x + 2)$.*
3. *The polynomial $x^3 - 2$ is irreducible in $\mathbb{F}_7[x]$, so $\mathbb{F}_7[x]/(x^3 - 2)$ is a field of order 7^3.*

Theorem 2.21 *If $f \in \mathbb{F}_p[x]$ is an irreducible polynomial of degree n then $\mathbb{F}_p[x]/(f) \cong \mathbb{F}_{p^n}$.*

Example 2.22

- $\mathbb{F}_2[x]/(x^3 + x + 1) \cong \mathbb{F}_{2^3}$, $\mathbb{F}_2[x]/(x^3 + x^2 + 1) \cong \mathbb{F}_{2^3}$, *and* $\mathbb{F}_3[x]/(x^2 + x + 2) \cong \mathbb{F}_{3^2}$.
- The results obtained so far make it possible to determine the elements of a finite field. We know that $\mathbb{F}_{p^n}$ is a vector space of dimension n over $\mathbb{F}_p$. Moreover, it is a simple extension of the prime field $\mathbb{F}_p$, say $\mathbb{F}_{p^n} = \mathbb{F}_p(\alpha)$, and any $n + 1$ elements of $\mathbb{F}_{p^n}$ are linearly dependent, so that there are $a_0, a_1, \ldots, a_n \in \mathbb{F}_p$ with $a_0 + a_1\alpha + \cdots + a_n\alpha^n = 0$. This means that α is a root of the polynomial $a_0 + a_1 x + \cdots + a_n x^n$ in $\mathbb{F}_p[x]$. Let f be the minimal polynomial of α, then $\mathbb{F}_{p^n} = \mathbb{F}_p(\alpha) \cong \mathbb{F}_p[x]/(f)$ (by theorem 1.70). In order to obtain the elements of $\mathbb{F}_{p^n}$ explicitly, we determine an irreducible monic polynomial of degree n over $\mathbb{F}_p$ and form $\mathbb{F}_p[x]/(f)$. More generally, to obtain $\mathbb{F}_{q^m}$, $q = p^n$, we find an irreducible, monic polynomial g of degree m over $\mathbb{F}_q$ and form $\mathbb{F}_q[x]/(g)$, which is then isomorphic to $\mathbb{F}_{q^m}$.

Example 2.23 *We determine the elements of* $\mathbb{F}_{2^3}$. *If we regard* $\mathbb{F}_{2^3}$ *as a simple extension of degree* 3 *of the prime field* $\mathbb{F}_2$, *then this extension is obtained by adjoining to* $\mathbb{F}_2$ *a root of an irreducible cubic polynomial over* $\mathbb{F}_2$. *It is easily verified that* x^3+x+1 *and* x^3+x^2+1 *are irreducible over* $\mathbb{F}_2$. *Therefore* $\mathbb{F}_{2^3} \cong \mathbb{F}_2[x]/(x^3+x+1)$ *and also* $\mathbb{F}_{2^3} \cong \mathbb{F}_2[x]/(x^3+x^2+1)$. *Let* α *be a root of* $f(x) = x^3+x+1$, *then* 1, α, α^2 *form a basis of* $\mathbb{F}_{2^3}$ *over* $\mathbb{F}_2$. *The elements of* $\mathbb{F}_{2^3}$ *are of the form*

$$a + b\alpha + c\alpha^2 \qquad \text{for all } a,\ b,\ c \in \mathbb{F}_2 \qquad \text{with } \alpha^3 + \alpha + 1 = 0,$$

We can also use $g(x) = x^3 + x^2 + 1$ *to determine the elements of* $\mathbb{F}_{2^3}$. *Let* β *be a root of* g, *so* $\beta^3 + \beta^2 + 1 = 0$. *It can be easily verified that* $\beta + 1$ *is a root of* f *in* $\mathbb{F}_2[x]/(g)$. *The two fields* $\mathbb{F}_2[x]/(f)$ *and* $\mathbb{F}_2[x]/(g)$ *are splitting fields of* $x^8 - x$ *and are thus isomorphic. Therefore there is an isomorphism* ψ *such that* $\psi(\alpha) = \beta + 1$ *and* ψ *restricted to* $\mathbb{F}_2$ *is the identity mapping. The elements* 1, $\beta+1$, $(\beta+1)^2$ *form a basis of* $\mathbb{F}_2[x]/(g)$ *over* $\mathbb{F}_2$. *Thus the isomorphism* ψ *is given by*

$$\psi(a + b\alpha + c\alpha^2) = a + b(\beta + 1) + c(\beta + 1)^2 \qquad \text{with } a,\ b,\ c \in \mathbb{F}_2.$$

The following addition and multiplication tables of the multiplicative group $\mathbb{F}_2[x]/(x^3 + x^2 + 1)\backslash\{0\}$ *is as follows (*β *is as above):*

$\cdot$	1	β	$\beta+1$	β^2	$\beta^2+\beta$	β^2+1	$\beta^2+\beta+1$
1	1	β	$\beta+1$	β^2	$\beta^2+\beta$	β^2+1	$\beta^2+\beta+1$
β	β	β^2	$\beta^2+\beta$	β^2+1	1	$\beta^2+\beta+1$	$\beta+1$
$\beta+1$	$\beta+1$	$\beta^2+\beta$	β^2+1	1	$\beta^2+\beta+1$	β	β^2
β^2	β^2	β^2+1	1	$\beta^2+\beta+1$	β	$\beta+1$	$\beta^2+\beta$
$\beta^2+\beta$	$\beta^2+\beta$	1	$\beta^2+\beta+1$	β	$\beta+1$	β^2	$\beta+1$
β^2+1	β^2+1	$\beta^2+\beta+1$	β	$\beta+1$	β^2	$\beta^2+\beta$	1
$\beta^2+\beta+1$	$\beta^2+\beta+1$	$\beta+1$	β^2	$\beta^2+\beta$	β^2+1	1	β

$+$	1	β	$\beta+1$	β^2	$\beta^2+\beta$	β^2+1	$\beta^2+\beta+1$
1	0	$\beta+1$	β	β^2+1	$\beta^2+\beta+1$	β^2	$\beta^2+\beta$
β	$\beta+1$	0	1	$\beta^2+\beta$	β^2	$\beta^2+\beta+1$	β^2+1
$\beta+1$	β	1	0	$\beta^2+\beta+1$	β^2+1	$\beta^2+\beta$	β^2
β^2	β^2+1	$\beta^2+\beta$	$\beta^2+\beta+1$	0	β	1	$\beta+1$
$\beta^2+\beta$	$\beta^2+\beta+1$	β^2	β^2+1	β	0	$\beta+1$	1
β^2+1	β^2	$\beta^2+\beta+1$	$\beta^2+\beta$	1	$\beta+1$	0	β
$\beta^2+\beta+1$	$\beta^2+\beta$	β^2+1	β^2	$\beta+1$	1	β	0

Hance

$$\begin{aligned}\mathbb{F}_2[x]/(g) &= \left\{0,\, 1,\, \beta,\, \beta+1,\, \beta^2,\, \beta^2+1,\, \beta^2+\beta,\, \beta^2+\beta+1\right\}\\ &= \left\{0,\, 1,\, \beta,\, \beta^2,\, \beta^3,\, \beta^4,\, \beta^5,\, \beta^6\right\}\end{aligned}$$

with $\beta^3 = \beta^2+1$ *and* $\beta^7 = 1$.

Example 2.24 *Consider the field* $\mathbb{F}_9 = \mathbb{F}_{3^2}$*, which is a vector space of dimension* 2 *over* $\mathbb{F}_3$*. Consider* $f(x) = x^2+x+2$ *in* $\mathbb{F}_3[x]$*. This polynomial has no roots in* $\mathbb{F}_3$ *so it is irreducible over* $\mathbb{F}_3$*.*

Let α *be a root of* f*, so* $\alpha^2+\alpha+2=0$*. Hence* $\alpha^2 = -\alpha-2 = 2\alpha+1$*.*

The nine elements of $\mathbb{F}_9 = \mathbb{F}_3(\alpha)$ *are given in the form* $a\alpha+b$ *with* $a,\, b \in \mathbb{F}_3$*. In detail,* $\mathbb{F}_9 = \mathbb{F}_3[x]/(x^2+x+2) = \{0,\, 1,\, 2,\, \alpha,\, \alpha+1,\, \alpha+2,\, 2\alpha,\, 2\alpha+1,\, 2\alpha+2\}$ *with its natural operations. We can compute the addition and multiplication tables by hand. For example,* $2\alpha(\alpha+2) = 2\alpha^2+4\alpha = 2(2\alpha+1)+\alpha = 2\alpha+2$*.*

Chapter 3

Properties of finite fields

In this chapter, we list some important properties of finite fields.

Lemma 3.1 *For every element β of a finite field $\mathbb{F}_q$ 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 $\mathbb{F}_q$ form a group of order $q-1$ under multiplication. Thus $a^{q-1} = 1$ for all $a \in \mathbb{F}_q$ with $a \neq 0$. and multiplication by a yields the desired result. ■

Definition 3.2 *(**Order**) The order of a nonzero element $\alpha \in \mathbb{F}_q$, denoted by $ord(\alpha)$, is the smallest positive integer k such that $\alpha^k = 1$.*

Example 3.3 *Since there are no linear factors for the polynomial $1 + x^2$ over $\mathbb{F}_3$, $1 + x^2$ is irreducible over $\mathbb{F}_3$. Consider the element α in the field $\mathbb{F}_9 = \mathbb{F}_3(\alpha)$, where α is a root of $1 + x^2$. Then $\alpha^2 = -1$, $\alpha^3 = \alpha(\alpha^2) = -\alpha$ and $\alpha^4 = (\alpha^2)^2 = (-1)^2 = 1$.*

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

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

Lemma 3.4

(i) *The order $ord(\alpha)$ divides $q-1$ for every $\alpha \in \mathbb{F}_q^*$.*

(ii) *For tow nonzero elements α, $\beta \in \mathbb{F}_q^*$, if $gcd(ord(\alpha), ord(\beta)) = 1$, then $ord(\alpha\beta) = ord(\alpha) \times ord(\beta)$.*

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

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

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

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

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

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

Lemma 3.5 *Let F be a field and p a prime. The following are equivalent:*

(i) $m \mid n$;

(ii) $p^m - 1 \mid p^n - 1$;

(iii) $x^m - 1 \mid x^n - 1$.

Theorem 3.6 ***(Subfield Criterion)*** *Let p be a prime and let m, n be natural numbers.*

(i) If $\mathbb{F}_{p^m}$ is a subfield of $\mathbb{F}_{p^n}$, then $m \mid n$.

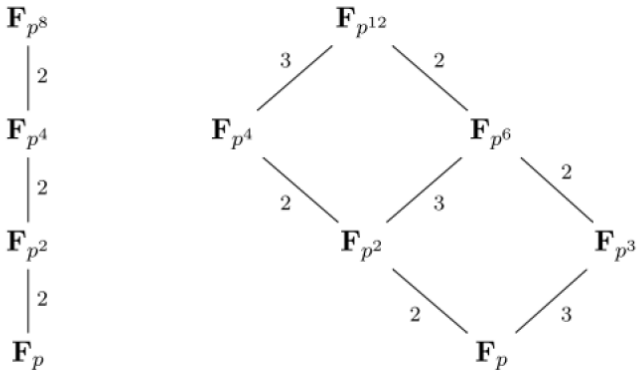
(ii) If $m \mid n$, then $\mathbb{F}_{p^m} \hookrightarrow \mathbb{F}_{p^n}$. There is exactly one subfield of $\mathbb{F}_{p^n}$ with p^m elements.

Proof. (i) Theorem 1.61 implies

$$[\mathbb{F}_{p^n} : \mathbb{F}_P] = [\mathbb{F}_{p^n} : \mathbb{F}_{p^m}][\mathbb{F}_{p^m} : \mathbb{F}_p].$$

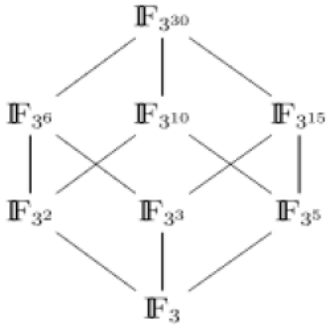
Since the term on the left-hand side is nand the second factor on the right-hand side is m, we have $m \mid n$. (ii) If $m \mid n$, we have $p^m - 1 \mid p^n - 1$, thus (by 3.5) $x^{p^m-1} - 1 \mid x^{p^n-1} - 1$ and $x^{p^m} - x \mid x^{p^n} - x$. The roots of $x^{p^m} - x$ form a subfield of F_{p^n} 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 $\mathbb{F}_{p^n}$. ■

Example 3.7 *In the diagram below are the subfields of* $\mathbb{F}_{p^8}$ *and* $\mathbb{F}_{p^{12}}$.



Example 3.8 *Consider the finite field* $\mathbb{F}_{3^{30}}$. *By theorem (3.6) any subfield* $\mathbb{F}_{3^m}$ *must satisfy* $m \mid 30$ *and thus there are only the following subfields:* $\mathbb{F}_3$, $\mathbb{F}_{3^2}$, $\mathbb{F}_{3^3}$, $\mathbb{F}_{3^5}$, $\mathbb{F}_{3^6}$, $\mathbb{F}_{3^{10}}$, $\mathbb{F}_{3^{15}}$, *and* $\mathbb{F}_{3^{30}}$.

This leads to the following Hasse-diagram:



The following result enunciates a useful property of $\mathbb{F}_q^*$.

With each field F we have a multiplicative group of nonzero elements of F which we will denote by F^*.

Theorem 3.9 *If* G *is a finite subgroup of* F^*, *the multiplicative group of nonzero elements of a field* F, *then* G *is cyclic.*

Proof. Let G be a finite subgroup of F^* with $n = p_1^{e_1} \cdots p_k^{e_k}$ elements, where p_i's are (not necessarily distinct) primes. By the Fundamental Theorem of Finite Abelian Groups,

$$G \cong \mathbb{Z}_{p_1^{e_1}} \times \cdots \times \mathbb{Z}_{p_k^{e_k}}.$$

Let m be the least common multiple of $p_1^{e_1}, \ldots, p_k^{e_k}$. Then G contains an element of order m. Since every α in G satisfies $x^r - 1$ for some r dividing m, α must also be a root of $x^m - 1$.

Since $x^m - 1$ has at most m roots in F, $n \leq m$. On the other hand, we know that $m \leq |G|$; therefore, $m = n$. Thus, G contains an element of order n and must be cyclic. ■

Corollary 3.10 *For every finite field $\mathbb{F}_q$, the multiplicative group $\mathbb{F}_q^*$ of nonzero elements of $\mathbb{F}_q$ is cyclic.*

Definition 3.11 *A generator of the cyclic group $\mathbb{F}_q^*$ is called a primitive element of $\mathbb{F}_q$.*

Remark 3.12 *If α is a root of an irreducible polynomial $f(x)$ of degree m over $\mathbb{F}_p$, and it is also a primitive element of $\mathbb{F}_{p^m} = \mathbb{F}_p[x]/f(x) \cong \mathbb{F}_p[\alpha]$, then every element in $\mathbb{F}_{p^m}$ can be represented both as a polynomial in α and as a power of α, since*

$$\mathbb{F}_{p^m} = \left\{a_0 + a_1\alpha + \cdots + a_{m-1}\alpha^{m-1} \mid a_i \in \mathbb{F}_p\right\} = \left\{0,\ \alpha,\ \alpha^2,\ \ldots,\ \alpha^{p^m-1}\right\}.$$

Addition for the elements of $\mathbb{F}_{p^m}$ is easily carried out if the elements are represented as polynomials in α,

whilst multiplication is easily done if the elements are represented as powers of α.

Example 3.13 *Consider the field $\mathbb{F}_4 = \mathbb{F}_2(\alpha)$, where α is a root of the irreducible polynomial $1 + x + x^2 \in \mathbb{F}_2[x]$. Then we have $\alpha^2 = -(1+\alpha) = 1+\alpha$, $\alpha^3 = \alpha(\alpha^2) = \alpha(1+\alpha) = \alpha + \alpha^2 = \alpha + 1 + \alpha = 1$. Thus, $\mathbb{F}_4 = \{0,\ \alpha,\ 1+\alpha,\ 1\} = \{0,\ \alpha,\ \alpha^2,\ \alpha^3\}$, so α is a primitive element.*

Proposition 3.14

(i) *A nonzero element of $\mathbb{F}_q$ is a primitive element if and only if its order is $q - 1$.*

(ii) *Every finite field has at least one primitive element.*

Example 3.15 *Let α be a root of $1 + x + x^3 \in \mathbb{F}_2[x]$. Hence, $\mathbb{F}_8 = \mathbb{F}_2[\alpha]$ The order of α is a divisor of $8 - 1 = 7$. Thus, $ord(\alpha) = 7$ and α is a primitive element. In fact, any nonzero element in $\mathbb{F}_8$ except 1 is a primitive element, since all the elements like this is not order of 1.*

Definition 3.16 *Let φ be **Euler's phi-function (or the totient function)** where $\varphi(n)$ indicates the number of positive integers less than or equal to n that are relatively prime to n.*

If $n = p_1^{t_1} \ldots p_k^{t_k}$, where p_i are distinct primes, then

$$\varphi(n) = n(1 - \frac{1}{p_1}) \cdots (1 - \frac{1}{p_k}).$$

Remark 3.17 *There are exactly $\varphi(q-1)$ primitive elements of F_q, where φ is the Euler totient function.*

Example 3.18 *$\mathbb{F}_4$ has $\varphi(3) = 2$ primitive elements. Expressing $\mathbb{F}_4$ as $\mathbb{F}_2(\alpha) = \{0,\ 1,\ \alpha,\ 1+\alpha\}$, where $\alpha^2 + \alpha + 1 = 0$, we find that both α and $1+\alpha$ are primitive elements.*

Lemma 3.19 ***(Freshman's Dream)*** *Let p be prime and F is a field (finite or not) of characteristic p. Then*

$$a^{p^n} + b^{p^n} = (a+b)^{p^n}.$$

for all positive integers n.

Proof. We will prove this lemma using mathematical induction on n. We can use the binomial formula to verify the case for $n = 1$; that is,

$$(a+b)^p = \sum_{k=0}^{p} \binom{p}{k}\ a^k b^{p-k}.$$

If $0 < k < p$, then

$$\binom{p}{k} = \frac{p!}{k!(p-k)!}$$

must be divisible by p, since p cannot divide $k!(p-k)!$. Note that F is a field of characteristic p, so all but the first and last terms in the sum must be zero. Therefore,

$$(a+b)^p = a^p + b^p.$$

Now suppose that the result holds for all k, where $1 \le k \le n$. By the induction hypothesis,

$$(a+b)^{p^{n+1}} = ((a+b)^p)^{p^n} = (a^p + b^p)^{p^n} = (a^p)^{p^n} + (b^p)^{p^n} = a^{p^{n+1}} + b^{p^{n+1}}.$$

Therefore, the lemma is true for $n+1$ and the proof is complete. ■

Example 3.20

In a field of characteristic 2, we have

$(a+b)^2 = a^2 + b^2$, $(a+b)^{2^2} = a^{2^2} + b^{2^2}$, $(a+b)^{2^3} = a^{2^3} + b^{2^3}$.

In this section we collect some information about the set of roots of an irreducible polynomial over a finite field.

Lemma 3.21 *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 an extension field of $\mathbb{F}_q$. Then for a polynomial $h \in \mathbb{F}_q[x]$ we have $h(\alpha) = 0$ if and only if f divides h.*

Lemma 3.22 *Let $f \in \mathbb{F}_q[x]$ be an irreducible polynomial over $\mathbb{F}_q$ of degree m. Then $f(x)$ divides $x^{q^n} - x$ if and only if m divides n.*

Proof. Suppose $f(x)$ divides $x^{q^n} - x$. Let α be a root of f in the splitting field of f over $\mathbb{F}_q$. Then $\alpha^{q^n} = \alpha$, so that $\alpha \in \mathbb{F}_{q^n}$. It follows that $\mathbb{F}_q(\alpha)$ is a subfield of $\mathbb{F}_{q^n}$. But since $[\mathbb{F}_q(\alpha) : \mathbb{F}_q] = m$ and $[F_{q^n} : F_q] = n$, theorem (1.61) shows that m divides n.

Conversely, if m divides n, then theorem (3.6) implies that $\mathbb{F}_{q^n}$ contains $\mathbb{F}_{q^m}$ as a subfield. If α is a root of f in the splitting field of f over $\mathbb{F}_q$, then $[\mathbb{F}_q(\alpha) : \mathbb{F}_q] = m$ and so $\mathbb{F}_q(\alpha) = \mathbb{F}_{q^m}$. Consequently, we have $\alpha \in \mathbb{F}_{q^n}$, hence $\alpha^{q^n} = \alpha$. And thus α is a root of $x^{q^n} - x \in \mathbb{F}_q[x]$. We infer then from lemma (3.22) that $f(x)$ divides $x^{q^n} - x$. ■

Theorem 3.23 *If f is an irreducible polynomial in $\mathbb{F}_q[x]$ of degree m. then f has a root α in $\mathbb{F}_{q^m}$ Furthermore, all the roots of f are simple and are given by the m distinct elements α, α^q, α^{q^2},..., $\alpha^{q^{m-1}}$ of $\mathbb{F}_{q^m}$.*

Proof. Let α be a root of f in the splitting field of f over $\mathbb{F}_q$. Then $[\mathbb{F}_q(\alpha) : \mathbb{F}_q] = m$, hence $\mathbb{F}_q(\alpha) = \mathbb{F}_{q^m}$, and in particula $\alpha \in F_{q^m}$. Next we show that if $\beta \in \mathbb{F}_{q^m}$ is a root of f, then β^q is also a root of f. Write $f(x) = a_m x^m + \cdots + a_1 x^1 + a_0$ with $a_i \in \mathbb{F}_q$ for $0 \leq i \leq m$. Then, using lemma (3.1) and lemma 3.19, we get

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

Therefore, the elements α, α^q, α^{q^2},..., $\alpha^{q^{m-1}}$ are roots of f. It remains to prove that these elements are distinct. Suppose, on the contrary, that $\alpha^{q^j} = \alpha^{q^k}$ for some integers j and k with $0 \leq j < k \leq m - 1$. By raising this identity to the power q^{m-k}, we get

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

It follows then from lemma (3.21) that $f(x)$ divides $x^{q^{m-k+j}} - x$. By lemma (3.22) this is only possible if m divide $m - k + j$. But we have $0 < m - k + j < m$. and so we arrive at a contradiction. ■

Definition 3.24 *(**Conjugates**) Let $\mathbb{F}_{q^m}$ be an extension of $\mathbb{F}_q$ and let $\alpha \in \mathbb{F}_{q^m}$. Then the elements α, α^q, α^{q^2},..., $\alpha^{q^{m-1}}$ are called the conjugates of α with respact to $\mathbb{F}_q$.*

Example 3.25 *Let $\alpha \in \mathbb{F}_{16}$ be a root of $f(x) = x^4 + x + 1 \in \mathbb{F}_2[x]$. Then the conjugates of α with respect to $\mathbb{F}_2$ are α, α^2, $\alpha^4 = \alpha + 1$. and $\alpha^8 = \alpha^2 + 1$.*

We next explore the relationship between conjugate elements and certain automorphisms of a finite field.

Definition 3.26 *An automorphism of $\mathbb{F}_{q^m}$ over $\mathbb{F}_q$ is an automorphism θ of $\mathbb{F}_{q^m}$ which fixes the elements of $\mathbb{F}_q$ pointwise. Thus, θ is a one-to-one mapping from $\mathbb{F}_{q^m}$ onto itself with*

$$\theta(\alpha + \beta) = \theta(\alpha) + \theta(\beta)$$

and

$$\theta(\alpha\beta) = \theta(\alpha)\theta(\beta)$$

for all α, $\beta \in \mathbb{F}_{q^m}$ and

$$\theta(\alpha) = \alpha \text{ for all } \alpha \in \mathbb{F}_q.$$

Theorem 3.27 *The distinct automorphisms of $\mathbb{F}_{q^m}$ over $\mathbb{F}_q$ are exactly the mappings θ_0, θ_1,..., θ_{m-1}, defined by*

$$\theta_j(\alpha) = \alpha^{q^j}$$

for $\alpha \in \mathbb{F}_{q^m}$ and $0 \leq j \leq m - 1$.

Proof. For each θ_j and all α, $\beta \in \mathbb{F}_{q^m}$ we obviously have $\theta_j(\alpha\beta) = \theta_j(\alpha)\theta_j(\beta)$, and also $\theta_j(\alpha+\beta) = \theta_j(\alpha)+\theta_j(\beta)$ because of lemma 3.19. Furthermore $\theta_j(\alpha) = 0$ if and only if $\alpha = 0$, θ_j is injective. Since $\mathbb{F}_{q^m}$ is a finite set, θ_j is also surjective, and hence is an automorphism of $\mathbb{F}_{q^m}$. Moreover, we have $\theta_j(\alpha) = \alpha$ for all $\alpha \in \mathbb{F}_q$ by lemma 3.1, and so each θ_j is an automorphism of $\mathbb{F}_{q^m}$ over $\mathbb{F}_q$. The mappings θ_0, θ_1,..., θ_{m-1} are distinct since they attain distinct values for a primitive element of $\mathbb{F}_{q^m}$.

Now suppose that θ is an arbitrary automorphism of $\mathbb{F}_{q^m}$ over $\mathbb{F}_q$. Let β be a primitive element of $\mathbb{F}_{q^m}$ and let $f(x) = x^m + a_{m-1}x^{m-1} + \cdots + a_0 \in \mathbb{F}_q[x]$ be its minimal polynomial over $\mathbb{F}_q$. Then

$$\begin{aligned} 0 &= \theta(\beta^m + a_{m-1}\beta^{m-1} + \cdots + a_0) \\ &= \theta(\beta)^m + a_{m-1}\theta(\beta)^{m-1} + \cdots + a_0, \end{aligned}$$

so that $\theta(\beta)$ is a root of f in $\mathbb{F}_{q^m}$. It follows from theorem 3.23 that $\theta(\beta) = \beta^{q^j}$ for some j, $0 \leq j \leq m-1$.

since θ is a homomorphism, we get then $\theta(\alpha) = \alpha^{q^j}$ for all $\alpha \in \mathbb{F}_{q^m}$. ■

Hence the conjugates of $\alpha \in \mathbb{F}_{q^m}$ are obtained by applying all automorphisms of $\mathbb{F}_{q^m}$ over $\mathbb{F}_q$ to the element α.

Remark 3.28 *The automorphisms of $\mathbb{F}_{q^m}$ over $\mathbb{F}_q$ form a group under composition of mappings, called the Galois group of $\mathbb{F}_{q^m}$ over $\mathbb{F}_q$ and denoted $Gal(\mathbb{F}_{q^m}/\mathbb{F}_q)$. From theorem 3.27, this group of automorphisms is a cyclic group of order m, generated by θ_1.*

Example 3.29 *The field $\mathbb{F}_4 = \{0, 1, \alpha, \alpha^2\}$, with $\alpha^2 = \alpha + 1$, $\alpha^3 = 1$. The automorphisms group of $\mathbb{F}_4$ consists of the identity mapping 1 and the mapping*

$$\theta \;:\; 1 \;\rightarrow\; 1, \qquad \alpha \;\rightarrow\; \alpha^2, \qquad \alpha^2 \;\rightarrow\; \alpha.$$

Clearly $\theta^2 = 1$.

Chapter 4

Factorization of polynomials over finite fields

In this chaptre we describe **Berlekamp's algorithm** for computing the factorization of a polynomial in $\mathbb{F}_q[x]$ into irreducible factors.

Any polynomial $f \in \mathbb{F}_q[x]$ of positive degree has a canonical factorization in $\mathbb{F}_q[x]$ by theorem 1.53. For the discussion of factorization algorithms it will suffice to consider only monic polynomials. Our goal is thus to express a monic polynomial $f \in \mathbb{F}_q[x]$ of positive degree in the form

$$f = f_1^{e_1} \cdots f_k^{e_k},$$

where $f_1, \ldots, f_k$ are distinct manic irreducible polynomials in $\mathbb{F}_q[x]$ and $e_1, \ldots, e_k$ are positive integers.

Next we will introduce the definition of a square-free polynomial. This will prove to be an important part of factoring polynomials over finite fields.

Definition 4.1 *A **square-free** polynomial in $\mathbb{F}_q[x]$ is a monic polynomial of degree ≥ 1 that has no multiple irreducible polynomial factors i.e. $f(x) = \prod_i^n f_i(x)^{e_i}$, where $f_i(x)$ are monic non-trivial irreducible polynomials, is square-free iff $e_i = 1$ for all i.*

Proposition 4.2 *A monic polynomial $f(x) \in \mathbb{F}_q[x]$ is square-free iff $gcd(f(x), f'(x)) = 1$.*

First we will present an algorithm to ensure a polynomial is square-free.

we can proceed as follows: Let $d = \gcd(f,\ f')$.

Case 4.3 : $d = 1$. *Then f is square-free.*

Case 4.4 : $1 \neq d \neq f$. *Then we already have a factor (namely d) of f and we factor d and f/d (which is easier than to factor f).*

Case 4.5 : $d = f$. *Then $f(x) = g \circ x^p = g(x^p)$, where $p =$ characterstic of $\mathbb{F}_q$. In this case, we factor g (which is much easier than to factor f).*

Therefore it suffices to consider the factorization of a monic square-free polynomial $f \in \mathbb{F}_q[x]$. Berlekamp's algorithm is based on some important properties: First we need a generalization of the Chinese Remainder Theorem for integers to the case of polynomials over $\mathbb{F}_q$.

Theorem 4.6 ***(Chinese Remainder Theorem for Polynomials)*** *Let $f_1, \ldots, f_r$ be distinct irreducible polynomials over $\mathbb{F}_q$ and let $g_1, \ldots, g_r$ be arbitrary polynomials over $\mathbb{F}_q$. Then the system of congruences $h \equiv g_i \pmod{f_i}$, $i = 1, 2, \ldots, r$, has a unique solution h modulo $f_1 f_2 \ldots f_r$.*

In trying to factor a square-free polynomial f into distinct monic irreducible divisors f_i over $\mathbb{F}_q$, theorem 4.6 says that we may expect information on f_i if we choose any constants $s_i \in \mathbb{F}_q$ and find h as in 4.6.

Then

$$f_i \mid gcd(f,\ h - s_i)$$

In fact, we shall see that we can find all f_i; among these gcd's. For h we get

$$h^q \equiv s_i^q = s_i \equiv h\ (mod\ f_i).$$

The multinomial theorem in $\mathbb{F}_q[x]$ yields $h^q = h \circ x^q$ and thus

$$h \circ x^q - h \equiv 0\ (mod\ f_i).$$

Since f_i divides f, it is sufficient to find polynomials h with the property

$$h \circ x^q - h \equiv 0\ (mod\ f_i). \tag{4.1}$$

In order to find such polynomials we construct then $n \times n$ matrix ($n = deg\ f$)

$$Q = \begin{pmatrix} q_{0,0} & q_{0,1} & \cdots & q_{0,n-1} \\ \vdots & \cdots & \ddots & \vdots \\ q_{n-1,0} & q_{n-1,1} & \cdots & q_{n-1,n-1} \end{pmatrix}$$

such that the kth row is given as the coefficient vector of the congruence
$x^{q \cdot k} \equiv q_{k,0} + q_{k,1}x + \cdots + q_{k,n-1}x^{n-1} \pmod f$.
A polynomial $h = \sum_{i=0}^{n-1} v_i x^i$ is a solution of (4.1) if and only if

$$(v_0,\, v_1, \ldots,\, v_{n-1}) \cdot Q = (v_0,\, v_1, \ldots,\, v_{n-1}). \tag{4.2}$$

This holds because

$$h = \sum_i v_i x^i = \sum_i \sum_k v_k q_{k,i} x^i = \sum_k v_k x^{qk} = h \circ x^q \equiv h^q\ (mod\ f).$$

The system (4.2) may be written in the equivalent form

$$(v_0,\, v_1, \ldots,\, v_{n-1}) \cdot (Q - I) = (0,\, 0, \ldots,\, 0).$$

The determination of a polynomial h satisfying (4.1) can be regarded as solving the system of linear equations $\mathbf{v} \cdot (Q - I) = 0$, where $\mathbf{v}$ is the coefficient vector of h, $Q = (q_{k,i})$, I is the $n \times n$ identity matrix, and 0 is the n-dimensional zero vector. Finding a suitable his therefore equivalent to determining the null space of $Q - \mathbf{I}$.

Theorem 4.7 $f = \prod_{s \in \mathbb{F}_q} \gcd(h - s,\, f)$.

Proof. Since $h^q - h \equiv 0\ (mod\ f)$, f divides $h^q - h = \prod_{s \in F_q} (h - s)$. Therefore f divides $\prod_{s \in F_q} \gcd(h - s,\, f)$. On the other hand, $\gcd(h - s,\, f)$ divides f. If $s \neq t \in \mathbb{F}_q$, then $h - s$ and $h - t$ are relatively prime, and so are $\gcd(h - s,\, f)$ and $\gcd(h - t,\, f)$.

Thus $\prod_{s \in \mathbb{F}_q} gcd(f,\, h - s)$ divides f. Since both polynomials are monic, they must be equal. ■

Theorem 4.8 *The number of monic distinct irreducible factors f_i of f is equal to the dimension of the null space of the matrix $Q - \mathbf{I}$.*

- Let k be the rank of the matrix $Q - I$. We have $k = n - r$, so that once the rank k is found, we know that the number of distinct monic irreducible factors of f is given by $r = n - k$. On the basis of this information we can already decide if f is irreducible or not. After finding k, we form $r = n - k$. If $r = 1$, we know that f is irreducible over $\mathbb{F}_q$ and the procedure terminates. If $r \geq 2$ we take the polynomial h_2 and compute $\gcd(h_2 - s,\ f)$ for all $s \in \mathbb{F}_q$. If the use of h_2 does not succeed in splitting f into r factors, we compute $\gcd(h_3 - s,\ f)$ for all $s \in \mathbb{F}_q$ and all nontrivial factors g found so far. This procedure is continued until r factors of f are obtained. The process described above must eventually yield all the factors. If the null space has dimension r, then there exists a basis with r monic polynomials $h^{(1)},\ldots,\ h^{(r)}$. We summarize these results.

Theorem 4.9 *(**Berlekamp's Algorithm**) Let $f \in \mathbb{F}_q[x]$ be monic of degree n.*

Stop 1. *Check if f is square-free, i.e., if $gcd(f,\ f') = 1$.*

Stop 2. *If f is square-free, form then $n \times n$ matrix $\mathbf{Q} = (q_{ki})$, defined by*

$$x^{qk} = \sum_{i=0}^{n-1} q_{ki} x^i (\text{mod } f), \qquad 0 \leq k \leq n-1.$$

Stop 3. *Find the null space of $\mathbf{Q} - \mathbf{I}$, determine its rank $n - r$, and find r linearly independent vectors $\mathbf{V}^{(1)},\ldots,\ \mathbf{V}^{(r)}$ such that $\mathbf{V}^{(i)}(\mathbf{Q} - \mathbf{I}) = 0$ for $i = 1, 2, \ldots, r$. The integer r is the number of irreducible factors of f. If $r = 1$, f is irreducible; otherwise go to Step* 4.

Stop 4. *Compute $gcd(f,\ h^{(2)} - s)$ for all $s \in \mathbb{F}_q$, where $h^{(2)} = \sum_i v_i^{(2)} x^i$. This yields a nontrivial decomposition of f into a product of (not necessarily irreducible) factors. If $h^{(2)}$ does not give all r factors of f, then we can obtain further factors by computing $gcd(\ h^{(k)} - s,\ f)$ for all $s \in \mathbb{F}_q$ and for $k = 3,\ 4,\ldots,\ r$. Here $h^{(k)} = \sum_i v_i^{(k)} x^i$. The algorithm ends when all r irreducible factors of f are found.*

Example 4.10

Factor $f(x) = x^8 + x^7 + x^5 + x^4 + x^3 + x + 1$ over $\mathbb{F}_2$ by Berlekamp's algorithm. Since $gcd(f,\ f') = 1$, then f is square-free. We have to comput $x^{2k} \equiv \sum_{i=0}^{7} q_{ki} x^i \pmod f$, $0 \leq k \leq 7$.

This yields the following :

$$\begin{aligned}
x^0 &\equiv 1 \pmod{f(x)} \\
x^2 &\equiv x^2 \pmod{f(x)} \\
x^4 &\equiv x^4 \pmod{f(x)} \\
x^6 &\equiv x^6 \pmod{f(x)} \\
x^8 &\equiv 1 + x + x^3 + x^4 + x^5 + x^7 \pmod{f(x)} \\
x^{10} &\equiv x^8 \cdot x^2 \equiv (1 + x + x^3 + x^4 + x^5 + x^7) \cdot x^2 \pmod{f(x)} \\
&\equiv x^2 + x^3 + x^5 + x^6 + x^7 + x^9 \pmod{f(x)} \\
&\equiv 1 + x^5 \pmod{f(x)} \\
x^{12} &\equiv x^{10} \cdot x^2 \equiv (1 + x^5) \cdot x^2 \pmod{f(x)} \\
&\equiv x^2 + x^7 \pmod{f(x)} \\
x^{14} &\equiv x^{12} \cdot x^2 \equiv (x^2 + x^7) \cdot x^2 \pmod{f(x)} \\
&\equiv x^4 + x^9 \pmod{f(x)} \\
&\equiv 1 + x^2 + x^3 + x^4 + x^6 + x^7 \pmod{f(x)}
\end{aligned}$$

Therefore, the 8×8 *matrix* Q *is given by*

$$Q = \begin{pmatrix}
1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\
1 & 1 & 0 & 1 & 1 & 1 & 0 & 1 \\
1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\
0 & 0 & 1 & 0 & 0 & 0 & 0 & 1 \\
1 & 0 & 1 & 1 & 1 & 0 & 1 & 1
\end{pmatrix}$$

and $Q - \mathbf{I}$ *is given by*

$$Q - \mathbf{I} = \begin{pmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 \\ 1 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 1 & 1 & 0 & 1 & 0 \end{pmatrix}$$

Since, the rank of $Q - \mathbf{I}$ *is* $k = 6$*, and therefore* $f(x)$ *has* $r = 8 - 6 = 2$ *distinct monic irreducible factors. The null space of the matrix* $Q - \mathbf{I}$ *is* $(1, 0, 0, 0, 0, 0, 0, 0)$ *and* $(0, 0, 1, 1, 0, 1, 0, 1)$*. The corresponding polynomials are* $h^{(1)}(x) = 1$ *and* $h^{(2)}(x) = x^2 + x^3 + x^5 + x^7$*. We calculate* $\gcd(h(x)^{(2)} - s,\ f(x))$ *for* $s \in \mathbb{F}_2$ *and obtain* $\gcd(h(x)^{(2)},\ f(x)) = 1 + x^3 + x^4$*,* $\gcd(h(x)^{(2)} - 1,\ f(x)) = 1 + x + x^4$*.*

The desired canonical factorization is therefore

$$f(x) = (x^4 + x + 1)(x^4 + x^3 + 1).$$

Example 4.11 *We want to determine the complete factorization of* $f(x) = x^7 + x^3 + 1$ *over* $\mathbb{F}_2$*.*

Since $gcd(f,\ f') = 1$*, then* f *is square-free.*

We have to comput $x^{2k} \equiv \sum_{i=0}^{6} q_{ki} x^i (\mathrm{mod}\ f), \qquad 0 \leq k \leq 6$*. This yields the following :*

$$\begin{aligned}
x^0 &\equiv 1 \ (\mathrm{mod}\, f(x)) \\
x^2 &\equiv x^2 \ (\mathrm{mod}\, f(x)) \\
x^4 &\equiv x^4 \ (\mathrm{mod}\, f(x)) \\
x^6 &\equiv x^6 \ (\mathrm{mod}\, f(x)) \\
x^8 &\equiv x \cdot x^7 \equiv x(x^3 + 1) \ (\mathrm{mod}\, f(x)) \ \textit{because}\ x^7 \equiv x^3 + 1 \ (\mathrm{mod}\, f(x)) \\
x^{10} &\equiv x^8 \cdot x^2 \equiv x^3 + x^6 \ (\mathrm{mod}\, f(x)) \\
x^{12} &\equiv x^{10} \cdot x^2 \equiv (x^3 + x^6) \cdot x^2 \ (\mathrm{mod}\, f(x)) \\
&\equiv x^5 + x^8 \ (\mathrm{mod}\, f(x)) \\
&\equiv x + x^4 + x^5 \ (\mathrm{mod}\, f(x)).
\end{aligned}$$

Therefore, the 7×7 *matrix* Q *is given by*

$$Q = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 & 1 & 1 & 0 \end{pmatrix}$$

and $Q - \mathbf{I}$ *is given by*

$$Q - \mathbf{I} = \begin{pmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 1 & 1 \end{pmatrix}$$

The matrix $Q - \mathbf{I}$ *has rank* 6 *by following the number of irreducibles factors of* f *is* $7 - 6 = 1$. *Therefore the polynomial* $f(x)$ *is irreducible over* $\mathbb{F}_2$.

.

Conclusion

In this conclusion; we summarize the main results obtained in this work:

We presented initially the definition and some properties on the following concepts:

Binary operation, Groups, Rings, Fields, Vector spaces, Field extensions.

Then, we saw the construction of finite fields, where we prove the order of any finite field has to be power of a prime, we prove existence and uniqueness of finite fields, and we listed some important properties of finite fields.

Finally we describe **Berlekamp's algorithm** for computing the factorization of a polynomial in $\mathbb{F}_q[x]$ into irreducible factors.

Bibliography

[1] **D. P. Acharjya & Sreekumar**. Discrete Mathematics. New Age International, 2005.

[2] **F. J. MacWilliams & N. J. A**. Sloane. The Theory of Error-Correcting Codes. V. 16. North-Holland, 1977.

[3] **Gary L. Mullen & Daniel Panario**. Handbook Of Finite Fields. CRC Press, 2013.

[4] **John R. Durbin**. Modern Algebra: An Introduction. John Wiley & Sons, 2009.

[5] **Mahima Ranjan Adhikari & Avishek Adhikari**. Basic Modern Algebra with Applications. Springer, India, 2014.

[6] **Ramprasad Saptharishi**. Lecture 8: More on Finite Fields, 2007.

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

[8] **Robert B**. **Ash** (2000). Basic Abstract Algebra.

[9] **Rudolf. Lidl & G. Pilz**. Applied Abstract Algebra. Springer-Verlag, New York, 1998.

[10] **Rudolf. Lidl & Harald Niederreiter**. Finite fields. V. 20. Cambridge University Press, 1997.

[11] **Rudolf. Lidl & Harald Niederreiter**. Introduction to finite fields and their applications. Cambridge University Press, 1986.

[12] **San Ling & Chaoping Xing**. Coding Theory: A First Course. Cambridge University Press, 2004.

[13] **Thomas W. Judson**. Abstract Algebra Theory and Applications. Stephen F. Austin State University, 2009.

[14] **William J. Gilbert**. Modern Algebra With Applications. John Wiley & Sons, 2004.