

# Chapter 2

## Finite Fields

### 1. Groups

- A group is an elementary structure, which underlies many other algebraic structures, such as rings, fields, etc.

- Definition:

Let  $G$  be a nonempty set with an algebraic operation  $\circ$  defined for each pair of its element. Then  $G$  is called a group if and only if for all  $a, b, c \in G$ , the operation  $\circ$  satisfies the following four axioms:

(1)  $a \circ b \in G$  (algebraic closure)

(2) There exists an element  $e \in G$  such that

$$e \circ a = a \circ e = a \quad (e \text{ is identity element})$$

(3) There exists an element  $a^{-1} \in G$  such that

$$a \circ a^{-1} = a^{-1} \circ a = e \quad (\text{existence of an inverse element})$$

(4)  $a \circ (b \circ c) = (a \circ b) \circ c$  (associativity)

- If the group  $G$  satisfies  $a \circ b = b \circ a$ ,

then  $G$  is called a commutative or Abelian group.

- A group is denoted by  $(G, \circ)$

- **Examples:**

The set  $I_2 = \{0, 1\}$  with the modulo-2 addition  $\oplus$  is a finite

Abelian group  $(I_2, \oplus)$  of order 2.

## 2. Rings

- **Definition:**

A non-empty set  $R$  with two algebraic operations, written  $*$  (called “multiplication”) and  $+$  (called “addition”), is called a ring if and only if these two operations satisfy the following axioms for all  $a, b, c \in R$ :

(1)  $(R, +)$  is an Abelian group with identity element  $0$ .

(2)  $a * b \in R$  (closed under multiplication)

(3)  $a * (b * c) = (a * b) * c$  (associativity of multiplication)

(4)  $a * (b + c) = a * b + a * c$  and

$(b + c) * a = b * a + c * a$  (distributive laws)

Usually, the ring  $R$  is denoted by  $(R, +, *)$

### 3. Basic Structure of Fields

- Roughly speaking, a field ( 場 ) is a set of elements in which one can perform addition, multiplication, subtraction, and division without leaving the set. Also, in a field, additions and multiplications satisfy the commutative, associative, and distributive laws.

- Definition: ( field )

Let  $F$  be a non-empty set with the two algebraic operations  $+$  and  $*$  defined for each pair of elements. Then  $F$  is a field if and only if the following conditions are satisfied:

- (1)  $(F, +)$  is an Abelian group.

The identity element with respect to addition is called the zero element or the additive identity of  $F$  and is denoted by  $0$ .

- (2)  $(F - \{0\}, *)$  is an Abelian group.

The identity element with respect to multiplication is called the unit element or the multiplicative identity of  $F$  and is denoted by  $1$ .

**(3) For all  $a, b, c \in F$ ,  $a * (b + c) = a * b + a * c$**

**and  $(b + c) * a = b * a + c * a$**

**i.e. multiplication is distributive over addition.**

▪ **Examples:**

**The set of all rational numbers is the rational field. The set of all real numbers is the real-number field. The set of all complex numbers is the complex-number field.**

- **The complex-number field is actually constructed from the real-number by requiring the symbol,  $i = \sqrt{-1}$ , as the root of the irreducible (over the real-number field) polynomial  $x^2 + 1$ , i.e.  $\sqrt{(-1)^2} + 1 = 0$**

**Every complex number is of the form  $a + bi$**

**where  $a$  and  $b$  are real numbers.**

- **The complex-number field contains the real-number field as a subfield. The complex-number is an extension field of the real-number field.**

- Both complex-number field and real-number field have infinite elements.

#### 4. Binary Arithmetic and Field

- Consider the binary set,  $\{0, 1\}$ . Define two binary operations, called addition “+” and multiplication “.” on  $\{0, 1\}$  as follows:

$$\begin{array}{ll} 0 + 0 = 0 & 0 \cdot 0 = 0 \\ 0 + 1 = 1 & 0 \cdot 1 = 0 \\ 1 + 0 = 1 & 1 \cdot 0 = 0 \\ 1 + 1 = 0 & 1 \cdot 1 = 1 \end{array}$$

These two operations are commonly called modulo-2 addition and multiplication, respectively.

- The set  $\{0, 1\}$  together with modulo-2 addition and multiplication is called a binary field, denoted GF(2).

## 5. Vector Space

▪ **Definition:**

Let  $(\bar{V}, +)$  be an Abelian group. Let  $F$  be commutative field with the identity elements,  $0$  and  $1$  for the operators  $+$  and  $*$ , respectively.

A multiplication operation, denoted by  $\cdot$ , between the element in  $F$  and the elements in  $\bar{V}$ , is also defined.

The set  $\bar{V}$  is called a vector space over the field  $F$  if it satisfies the following conditions:

(1) For any element  $a \in F$  and any element  $\bar{v} \in \bar{V}$  one has

$$a \cdot \bar{v} \in \bar{V}$$

(2) (Distributive law)

For any element  $\bar{u}, \bar{v} \in \bar{V}$ , and any elements  $a, b \in F$  one has

$$a \cdot (\bar{u} + \bar{v}) = a \cdot \bar{u} + a \cdot \bar{v}$$

$$(a + b) \cdot \bar{v} = a \cdot \bar{v} + b \cdot \bar{v}$$

(3) (Associative law)

For any  $\bar{v} \in \bar{V}$  and any  $a, b \in F$ , one has

$$(a * b) \cdot \bar{v} = a \cdot (b \cdot \bar{v})$$

(4) For any  $\bar{v} \in \bar{V}$  one has  $1 \cdot \bar{v} = \bar{v}$

- The elements of  $\bar{V}$  are called vectors. The elements of the field  $F$  are called scalars. The addition on  $\bar{V}$  is called vector addition. The multiplication, which maps a scalar in  $F$  and vector in  $\bar{V}$  into a vector in  $\bar{V}$ , is called scalar multiplication. The additive identity (zero) of  $\bar{V}$  is denoted by  $\bar{0}$ .
  
- **Definition** (subspace)

A vector space  $\bar{V}$  over a field  $F$  may contain a subset  $S$  of  $\bar{V}$  which is also a vector space over the field. Such a subset is called a (vector) subspace of  $\bar{V}$ .

## 6. Vector Space over GF(2)

- A binary  $n$ -tuple is an ordered sequence,  $(a_1, a_2, \dots, a_n)$  with components from GF(2), i.e.  $a_i = 1$  or  $0$  for  $1 \leq i \leq n$

There are  $2^n$  distinct binary  $n$ -tuples.

- **Addition operation for any two  $n$ -tuples:**

$$(a_1, a_2, \dots, a_n) + (b_1, b_2, \dots, b_n) = (a_1 + b_1, a_2 + b_2, \dots, a_n + b_n)$$

**The addition of two binary  $n$ -tuples results in a third  $n$ -tuple.**

- **Scalar Multiplication:**

Let  $C \in \text{GF}(2)$ ,  $\bar{a} = (a_1, a_2, \dots, a_n)$  is a binary  $n$ -tuple.

$$\text{Then } c \cdot (a_1, a_2, \dots, a_n) = (ca_1, ca_2, \dots, ca_n)$$

**The scalar multiplication also results in a binary  $n$ -tuple.**

- Let  $V_n$  denote the set of all  $2^n$  binary  $n$ -tuples. The set  $V_n$  together with the addition and scalar multiplication is called a vector space over  $\text{GF}(2)$ .

**The elements in  $V_n$  are called vectors.**

- $V_n$  contains the all-zero  $n$ -tuple  $(0, 0, \dots, 0)$  and

$$(a_1, a_2, \dots, a_n) + (a_1, a_2, \dots, a_n) = (0, 0, \dots, 0)$$

- A subset  $S$  of  $V_n$  is called a subspace of  $V_n$  if

(1) the all-zero vector is in  $S$ .

(2) the sum of two vectors in  $S$  is also a vector in  $S$ .

- **Inner Product:**

The inner product of two vectors,  $\bar{a} = (a_1, a_2, \dots, a_n)$  &

$\bar{b} = (b_1, b_2, \dots, b_n)$  is defined as follows:

$$\bar{a} \cdot \bar{b} = (a_1 b_1 + a_2 b_2 + \dots + a_n b_n)$$

- **Linear Independent:**

A set of vectors,  $\bar{V}_1, \bar{V}_2, \dots, \bar{V}_k$  in  $V_n$  is said to be linearly

independent if  $c_1 \bar{V}_1 + c_2 \bar{V}_2 + \dots + c_k \bar{V}_k \neq 0$

unless all  $c_1, c_2, \dots, c_k$  are the zero elements of GF(2).

- **Dimension of Subspace:**

The subspace formed by the  $2^k$  linearly combinations of  $k$

linearly independent vectors  $\bar{V}_1, \bar{V}_2, \dots, \bar{V}_k$  in  $V_n$  is called a

$k$ -dimensional subspace of  $V_n$ .

These  $k$  vectors are said to span a  $k$ -dimensional subspace of  $V_n$ .

- **Orthogonal:**

Two vectors,  $\bar{a}$  and  $\bar{b}$ , are said to be orthogonal if  $\bar{a} \cdot \bar{b} = 0$

- **Dual space:**

Let  $S$  be a  $k$ -dimensional subspace of  $V_n$ . Let  $S_d$  be the subspace of vectors in  $V_n$  such that, for any  $\bar{a}$  in  $S$  and any  $\bar{b}$  in  $S_d$ ,  $\bar{a} \cdot \bar{b} = 0$

$S_d$  is called the dual space (or null space) of  $S$ . The dimension of  $S_d$  is  $n-k$ .

## 7. Binary Irreducible Polynomials

- A polynomial with coefficients from the binary field GF(2) is called a binary polynomial.

e.g.  $1 + x^2$  and  $1 + x^3 + x^5$  are binary polynomials.

- A binary polynomial  $p(x)$  of degree  $m$  is said to be irreducible if it is not divisible by any binary polynomial of degree less than  $m$  and greater than zero.

e.g.  $1+x+x^2$  ,  $1+x+x^3$  ,  $1+x^2+x^5$  and  $1+x+x^5$

are irreducible polynomials.

- For any positive integer  $m \geq 1$  , there exists at least one irreducible polynomial of degree  $m$ .

- A irreducible polynomial  $p(x)$  of degree  $m$  is said to be primitive if the smallest positive integer  $n$  for which  $p(x)$  divides  $x^n + 1$  is  $n = 2^m - 1$

For example,  $1+x+x^4$  is a primitive polynomial. The smallest positive integer  $n$  for which  $1+x+x^4$  divides  $x^n + 1$  is  $n = 2^4 - 1 = 15$

- For any positive integer  $m$ , there exists a primitive polynomial of degree  $m$

**Example (Lin / Costello page 29)**

| <i>m</i>  | <b>Primitive Polynomial</b>  |
|-----------|------------------------------|
| <i>3</i>  | $1 + x + x^3$                |
| <i>4</i>  | $1 + x + x^4$                |
| <i>5</i>  | $1 + x^2 + x^5$              |
| <i>6</i>  | $1 + x + x^6$                |
| <i>7</i>  | $1 + x^3 + x^7$              |
| <i>8</i>  | $1 + x^2 + x^3 + x^4 + x^8$  |
| <i>9</i>  | $1 + x + x^9$                |
| <i>10</i> | $1 + x + x^{10}$             |
| <i>11</i> | $1 + x^2 + x^{11}$           |
| <i>12</i> | $1 + x + x^4 + x^6 + x^{12}$ |

## 8. Finite Fields

- A field with only a finite number of elements is called a finite field.
  
- Finite fields are also known as Galois field after their discover.
  
- For any positive integer  $m \geq 1$ , there exists a Galois field of  $2^m$  elements, denoted  $\text{GF}(2^m)$ . That is, it is an extension field of  $\text{GF}(2)$ .
  
- Construction of  $\text{GF}(2^m)$ 
  - (1) Begin with a primitive (irreducible) polynomial  $p(x)$  of degree  $m$  with coefficients from the binary field  $\text{GF}(2)$ .
  - (2) Since  $p(x)$  has degree  $m$ , it must have roots somewhere.  
Let  $\alpha$  be the root of  $p(x)$ , i.e.  $p(\alpha) = 0$

(3) Starting from  $\text{GF}(2) = \{0, 1\}$  and  $\alpha$ , we define a multiplication “ $\cdot$ ” to introduce a sequence of powers of  $\alpha$

as follows:

$$0 \cdot 0 = 0$$

$$0 \cdot 1 = 1 \cdot 0 = 0$$

$$1 \cdot 1 = 1$$

$$0 \cdot \alpha = \alpha \cdot 0 = 0$$

$$1 \cdot \alpha = \alpha \cdot 1 = \alpha$$

$$\alpha^2 = \alpha \cdot \alpha$$

$$\alpha^3 = \alpha \cdot \alpha \cdot \alpha$$

$\vdots$

$$\alpha^j = \underbrace{\alpha \cdot \alpha \cdot \dots \cdot \alpha}_{j \text{ times}}$$

and we can see that

$$0 \cdot \alpha^j = \alpha^j \cdot 0 = 0$$

$$1 \cdot \alpha^j = \alpha^j \cdot 1 = \alpha^j$$

$$\alpha^i \cdot \alpha^j = \alpha^{i+j}$$

We now have the following set of elements,

$$F = \{0, 1, \alpha, \alpha^2, \dots\}$$

which is closed under multiplication “ $\cdot$ ”

(4) Since  $\alpha$  is a root of  $p(x)$  and  $p(x)$  divides  $x^{2^m-1} + 1$ ,  $\alpha$  must also be a root of  $x^{2^m-1} + 1$ . Hence  $x^{2^m-1} + 1 = 0$ .

This implies that  $x^{2^m-1} = 1$ . As a result,  $F$  is finite and consists of following elements,

$$F = \{0, 1, \alpha, \alpha^2, \dots, \alpha^{2^m-2}\}$$

(5) Let  $\alpha^0 = 1$ . Multiplication is carried out as follows:

For  $0 \leq i, j \leq 2^m - 1$

$$\alpha^i \cdot \alpha^j = \alpha^{i+j} = \alpha^r$$

Where  $r$  is the remainder resulting from dividing  $i+j$  by

$$2^m - 1. \text{ Since } \alpha^i \cdot \alpha^{2^m-1-i} = \alpha^{2^m-1} = 1$$

$\alpha^{2^m-1-i}$  is called the multiplicative inverse of  $\alpha^i$  and vice versa.

We can also write  $\alpha^{2^m-1-i} = \alpha^{2^m-1} \cdot \alpha^{-i} = \alpha^{-i}$

Thus, we can use  $\alpha^{-i}$  to denote the multiplicative inverse of  $\alpha^i$

The element “1” is called the multiplicative identity (or the unit element).

(6) next, we define “division” as follows:

$$\alpha^i \div \alpha^j = \alpha^i \cdot \alpha^{-j} = \alpha^{i-j}$$

(7) we define “addition” on  $F$  as follows:

For  $0 \leq i \leq 2^m - 2$ , we divide  $X^i$  by  $p(x)$

This results in  $X^i = a(x)p(x) + b(x)$

where  $b(x)$  is the remainder and

$$b(x) = b_0 + b_1x + b_2x^2 + \cdots + b_{m-1}x^{m-1}$$

Replacing  $X$  by  $\alpha$ , we have

$$\begin{aligned}\alpha^i &= a(\alpha)p(\alpha) + b(\alpha) \\ &= b_0 + b_1\alpha + \cdots + b_{m-1}\alpha^{m-1}\end{aligned}$$

This says that each nonzero element in  $F$  can be expressed

as polynomial of  $\alpha$  with degree  $m-1$  or less.

Suppose  $\alpha^i = b_0 + b_1\alpha + \cdots + b_{m-1}\alpha^{m-1}$

$$\alpha^j = c_0 + c_1\alpha + \cdots + c_{m-1}\alpha^{m-1}$$

We define addition “+” as follows:

$$\alpha^i + \alpha^j = (b_0 + c_0) + (b_1 + c_1)\alpha + \cdots + (b_{m-1} + c_{m-1})\alpha^{m-1} = \alpha^k$$

(8) Clearly,  $\alpha^i + \alpha^i = 0$

Thus,  $\alpha^i$  is its own additive inverse.  $-\alpha^i = \alpha^i$

Subtraction is defined as follows:

$$\alpha^i - \alpha^j = \alpha^i + (-\alpha^j) = \alpha^i + \alpha^j$$

Hence, subtraction is the same as addition.

(9) we conclude that  $F = \{0, 1, \alpha, \alpha^2, \dots, \alpha^{2^m-2}\}$  together with the multiplication and addition defined above form a field of  $2^m$  elements.

Such a field is called a Galois field, denoted as  $\text{GF}(2^m)$

Note: the set  $\{1, \alpha, \alpha^2, \dots, \alpha^{m-1}\}$  is called the canonical basis of  $\text{GF}(2^m)$  over  $\text{GF}(2)$

▪ Representation of the elements in  $\text{GF}(2^m)$

There are 3 forms to represent the elements in  $\text{GF}(2^m)$ :

(1) Power form (easier to perform multiplication)

$$\{0, 1, \alpha, \alpha^2, \dots, \alpha^{2^m-2}\}$$

(2) Polynomial form (easier to perform addition)

$$\alpha^j = b_0 + b_1\alpha + \dots + b_{m-1}\alpha^{m-1}$$

(3) Vector form (easier to perform addition)

$$\alpha^j = (b_0, b_1, \dots, b_{m-1})$$

**Example:**

The Galois field  $\text{GF}(2^4)$  generated by  $p(x) = x^4 + x + 1$

| <b>Power Representation</b>     | <b>Polynomial representation</b>                     | <b>4-Tuple representation</b> |
|---------------------------------|--|-------------------------------|
| <b>0</b>                        | <b>0</b>   | <b>(0 0 0 0)</b>              |
| <b>1</b>                        | <b>1</b>   | <b>(1 0 0 0)</b>              |
| <b><math>\alpha</math></b>      | <b><math>\alpha</math></b>                           | <b>(0 1 0 0)</b>              |
| <b><math>\alpha^2</math></b>    | <b><math>\alpha^2</math></b>                         | <b>(0 0 1 0)</b>              |
| <b><math>\alpha^3</math></b>    | <b><math>\alpha^3</math></b>                         | <b>(0 0 0 1)</b>              |
| <b><math>\alpha^4</math></b>    | <b><math>1 + \alpha</math></b>                       | <b>(1 1 0 0)</b>              |
| <b><math>\alpha^5</math></b>    | <b><math>\alpha + \alpha^2</math></b>                | <b>(0 1 1 0)</b>              |
| <b><math>\alpha^6</math></b>    | <b><math>\alpha^2 + \alpha^3</math></b>              | <b>(0 0 1 1)</b>              |
| <b><math>\alpha^7</math></b>    | <b><math>1 + \alpha + \alpha^3</math></b>            | <b>(1 1 0 1)</b>              |
| <b><math>\alpha^8</math></b>    | <b><math>1 + \alpha^2</math></b>                     | <b>(1 0 1 0)</b>              |
| <b><math>\alpha^9</math></b>    | <b><math>\alpha + \alpha^3</math></b>                | <b>(0 1 0 1)</b>              |
| <b><math>\alpha^{10}</math></b> | <b><math>1 + \alpha + \alpha^2</math></b>            | <b>(1 1 1 0)</b>              |
| <b><math>\alpha^{11}</math></b> | <b><math>\alpha + \alpha^2 + \alpha^3</math></b>     | <b>(0 1 1 1)</b>              |
| <b><math>\alpha^{12}</math></b> | <b><math>1 + \alpha + \alpha^2 + \alpha^3</math></b> | <b>(1 1 1 1)</b>              |
| <b><math>\alpha^{13}</math></b> | <b><math>1 + \alpha^2 + \alpha^3</math></b>          | <b>(1 0 1 1)</b>              |
| <b><math>\alpha^{14}</math></b> | <b><math>1 + \alpha^3</math></b>                     | <b>(1 0 0 1)</b>              |

## Historical Notes

- **Galois fields are named in honor of the French mathematician Evariste Galois (1811 – 1832) who was killed in a duel at the age of 20. On the eve of his death, he wrote a letter to his friend in which he gave the results of his theory of algebraic equations, already presented to the Pairs Academy.**

## Remarks

1. **Galois fields are important in the study of cyclic codes, a special class of block codes. In particular, they are used for constructing the well-known random error correcting BCH and Reed-Solomon Codes.**
2.  **$GF(2^m)$  is an extension field of  $GF(2)$ .**
3. **Every Galois field of  $2^m$  elements is generated by a binary primitive polynomial of degree  $m$ .**