Let G be a set of elements. A *binary operation* $*$ on G is a *rule* that assigns to each pair of elements a and b a uniquely defined third element $c = a * b$ in G. When such a binary operation $*$ is defined on G, we say that G is *closed* under $*$. For example, let G be the set of all integers and let the binary operation on G be real addition $+$. We all know that, for any two integers i and j in G, $i + j$ is a uniquely defined integer in G. Hence, the set of integers is closed under real addition. A binary operation $*$ on G is said to be *associative* if, for any a, b, and c in G,

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

Now, we introduce a useful algebraic system called a *group*.

Definition 2.1. A set G on which a binary operation $*$ is defined is called a *group* if the following conditions are satisfied:

(i) The binary operation $*$ is associative.

(ii) G contains an element e such that, for any a in G,

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

This element e is called an *identity* element of G.

(iii) For any element a in G, there exists another element a' in G such that

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

The element a' is called an *inverse* of a (a is also an inverse of a').

A group G is said to be *commutative* if its binary operation $*$ also satisfies the following condition: For any a and b in G,

$$a * b = b * a.$$

Example 2.1

Consider the set of two integers, $G = \{0, 1\}$. Let us define a binary operation, denoted by $\oplus$, on G as follows:

$$0 \oplus 0 = 0, \qquad 0 \oplus 1 = 1, \qquad 1 \oplus 0 = 1, \qquad 1 \oplus 1 = 0.$$

This binary operation is called *modulo-2* addition. The set $G = \{0, 1\}$ is a group under modulo-2 addition. It follows from the definition of modulo-2 addition $\oplus$ that G is closed under $\oplus$ and $\oplus$ is commutative. We can easily check that $\oplus$ is associative. The element 0 is the identity element. The inverse of 0 is itself and the inverse of 1 is also itself. Thus, G together with $\oplus$ is a commutative group.

The number of elements in a group is called the *order* of the group. A group of finite order is called a *finite* group. For any positive integer m, it is possible to construct a group of order m under a binary operation which is very similar to real addition.

DEFINITION 6.6 Ring *A* ring *is a triple* $(R, +, \times)$ *consisting of a set* R*, and two operations* $+$ *and* $\times$*, referred to as* addition *and* multiplication*, respectively, which satisfy the following conditions:*

1. associativity of $+$: $a + (b + c) = (a + b) + c$ *for all* $a, b, c \in R$;
2. commutativity of $+$: $a + b = b + a$ *for all* $a, b \in R$;
3. existence of additive identity: *there exists* $0 \in R$ *such that* $0 + a = a$ *and* $a + 0 = a$ *for all* $a \in R$;
4. existence of additive inverses: *for each* $a \in R$ *there exists* $-a \in R$ *such that* $a + (-a) = 0$ *and* $(-a) + a = 0$;
5. associativity of $\times$: $a \times (b \times c) = (a \times b) \times c$ *for all* $a, b, c \in R$;
6. distributivity of $\times$ over $+$: $a \times (b + c) = (a \times b)(a \times c)$ *for all* $a, b, c \in R$.

DEFINITION 6.11 The Cyclic Rings *For every positive integer* p*, there is a ring* $(\mathbb{Z}_p, +, \times)$*, called the* cyclic ring of order p*, with set of elements*

$$Z_p = \{0, 1, \ldots, (p-1)\}$$

and operations $+$ *denoting addition modulo* p*, and* $\times$ *denoting multiplication modulo* p.

EXAMPLE 6.14

The operation tables of the cyclic ring of order 3 are

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

×	0	1	2
0	0	0	0
1	0	1	2
2	0	2	1

$\mathbb{Z}_3$ is a field.

EXAMPLE 6.15

The operation tables of the cyclic ring of order 4 are

+	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

×	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	0	2
3	0	3	2	1

$\mathbb{Z}_4$ is not a field; 2 does not have a multiplicative inverse.

EXAMPLE 6.16

The operation tables of the cyclic ring of order 5 are

+	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

×	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

$\mathbb{Z}_5$ is a field.

The cyclic ring of order p is a field if and only if p is a prime number.

FIELDS

- Let F be a set of elements on which two binary operations, called addition "+" and multiplication "." are defined. The set F together with the two binary operations + and . is the field if the following conditions are satisfied.

1.F is a commutative group under addition +.the identity element with respect to addition is called the *zero element* or the ***additive identity*** *of F* and is denoted by **0**

2.The set of nonzero elements in F is a commutative group under multiplication. The identity elements with respect to multiplication is called the unit element or the **multiplicative identity** of F and is denoted by **1.**

3.Multiplication is distributive over addition; for any three elements a,b and c in F.

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

Basic Properties

- For every element a in the field $a.0=0.a=0$

Proof. First we note that

$$a = a \cdot 1 = a \cdot (1 + 0) = a + a \cdot 0.$$

Adding $-a$ to both sides of the equality above, we have

$$-a + a = -a + a + a \cdot 0$$

$$0 = 0 + a \cdot 0$$

$$0 = a \cdot 0.$$

Similarly, we can show that $0 \cdot a = 0$. Therefore, we obtain $a \cdot 0 = 0 \cdot a = 0$.

- For any two nonzero elements a and b in a field $a.b \neq 0$

Proof :

Non zero elements of a field are closed under multiplication

a.b=0 and a≠0 imply that b=0

Proof. This is a direct consequence of Property II.

- For any 2 elements a and b

-(a.b)=(-a).b=a.(-b)

Proof. $0 = 0 \cdot b = (a + (-a)) \cdot b = a \cdot b + (-a) \cdot b$. Therefore, $(-a) \cdot b$ must be the additive inverse of $a \cdot b$ and $-(a \cdot b) = (-a) \cdot b$. Similarly, we can prove that $-(a \cdot b) = a \cdot (-b)$. Q.E.D.

For a ≠ 0, a.b=a.c implies that b=c

Proof. Since a is a nonzero element in the field, it has a multiplicative inverse a^{-1}. Multiplying both side of $a \cdot b = a \cdot c$ by a^{-1}, we obtain

$$a^{-1} \cdot (a \cdot b) = a^{-1} \cdot (a \cdot c)$$

$$(a^{-1} \cdot a) \cdot b = (a^{-1} \cdot a) \cdot c$$

$$1 \cdot b = 1 \cdot c.$$

Thus, $b = c$. Q.E.D.

Example for modulo 2 addition and multiplication

A very common field in this category is Galois field GF(2) with the set {0, 1} and two operations, addition and multiplication, as shown in Figure.

GF(2) field

GF(2)

{0, 1} + ×

+	0	1
0	0	1
1	1	0

Addition

×	0	1
0	0	0
1	0	1

Multiplication

Example

We can define GF(5) on the set Z_5 (5 is a prime) with addition and multiplication operators as shown in Figure.

GF(5)

{0, 1, 2, 3, 4} + ×

+	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

Addition

×	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

Multiplication

Construction of Galois field GF(2^m)

- Begin with 2 elements 0 and 1 from GF(2) and a new symbol α
- Put a condition on α such that F contains 2^m elements and is closed under multiplication
- Let p(X) be a polynomial of degree m over GF(2).
- Assume $p(\alpha) = 0$
- Since p(X) divides $X^{2^m-1}+1$, $\alpha^{2^m-1}=1$
- Under the conditions $p(\alpha)=0$, F becomes finite and contains the following elements
- $F^* = \{0, 1, \alpha, \alpha^2, \alpha^3, \ldots\ldots \alpha^{2^m-2}\}$
- Example
- Three representations for elements GF(2^m) generated by the primitive polynomial $p(X) = 1+X+X^4$

TABLE 2.8 THREE REPRESENTATIONS FOR THE ELEMENTS OF GF(2^4) GENERATED BY $p(X) = 1 + X + X^4$

Power representation	Polynomial representation	4-Tuple representation (α^0 α^1 α^2 α^3)
0	0	(0 0 0 0)
$1 = \alpha^0$	1	(1 0 0 0)
α	α	(0 1 0 0)
α^2	α^2	(0 0 1 0)
α^3	α^3	(0 0 0 1)
α^4	$1 + \alpha$	(1 1 0 0)
α^5	$\alpha + \alpha^2$	(0 1 1 0)
α^6	$\alpha^2 + \alpha^3$	(0 0 1 1)
α^7	$1 + \alpha + \alpha^3$	(1 1 0 1)
α^8	$1 + \alpha^2$	(1 0 1 0)
α^9	$\alpha + \alpha^3$	(0 1 0 1)
α^{10}	$1 + \alpha + \alpha^2$	(1 1 1 0)
α^{11}	$\alpha + \alpha^2 + \alpha^3$	(0 1 1 1)
α^{12}	$1 + \alpha + \alpha^2 + \alpha^3$	(1 1 1 1)
α^{13}	$1 + \alpha^2 + \alpha^3$	(1 0 1 1)
α^{14}	$1 + \alpha^3$	(1 0 0 1)

15
$\alpha = 1$
$=$

$1+\alpha+\alpha^4 = 0$
$\alpha^4 = 1+\alpha$
$\alpha^5 = \alpha \cdot \alpha^4 = \alpha(1+\alpha) = \alpha+\alpha^2$
$\alpha^6 = \alpha \cdot \alpha^5 = \alpha(\alpha+\alpha^2) = \alpha^2+\alpha^3$

$\alpha^7 = \alpha \cdot \alpha^6 = \alpha(\alpha^2+\alpha^3)$
$= \alpha^3+\alpha^4$
$= \alpha^3 + 1+\alpha$

- Given $GF(2^3)$ for $p(X)=1+X+X^3$
  Find the tuple representation

Solution

$GF(2^3)$ generated by $\mathbf{p}(X) = 1 + X + X^3$

0	0 0 0
1	1 0 0
α	0 1 0
α^2	0 0 1
α^3	1 1 0
α^4	0 1 1
α^5	1 1 1
α^6	1 0 1

THEOREM

Let $f(X)$ be a polynomial with coefficients from GF(2). Let β be an element in an extension field of GF(2). If β is a root of $f(X)$, then for any $l \geq 0$, β^{2^l} is also a root of $f(X)$.

The element β^{2^l} is called a *conjugate* of β.

Minimal Polynomial

- Theorem : the $2^m - 1$ nonzero elements of GF(2^m) form all the roots of $X^{2^m-1}+1$
- Let Φ (X) be the polynomial of **the smallest degree** over GF(2) such that Φ (β) =0 , the polynomial Φ (X) is called minimal polynomial of β

Theorem 2.14. Let $\phi(X)$ be the minimal polynomial of an element β in GF(2^m). Let e be the smallest integer such that $\beta^{2^e} = \beta$. Then

$$\phi(X) = \prod_{i=0}^{e-1} (X + \beta^{2^i}). \tag{2.23}$$

Example 2.7

Consider the Galois field GF(2^4) given by Table 2.8. Let $\beta = \alpha^3$. The conjugates of β are

$$\beta^2 = \alpha^6, \qquad \beta^{2^2} = \alpha^{12}, \qquad \beta^{2^3} = \alpha^{24} = \alpha^9.$$

The minimal polynomial of $\beta = \alpha^3$ is then

$$\phi(X) = (X + \alpha^3)(X + \alpha^6)(X + \alpha^{12})(X + \alpha^9).$$

Multiplying out the right-hand side of the equation above with the aid of Table 2.8, we obtain

$$\begin{aligned}\phi(X) &= [X^2 + (\alpha^3 + \alpha^6)X + \alpha^9][X^2 + (\alpha^{12} + \alpha^9)X + \alpha^{21}] \\ &= (X^2 + \alpha^2 X + \alpha^9)(X^2 + \alpha^8 X + \alpha^6) \\ &= X^4 + (\alpha^2 + \alpha^8)X^3 + (\alpha^6 + \alpha^{10} + \alpha^9)X^2 + (\alpha^{17} + \alpha^8)X + \alpha^{15} \\ &= X^4 + X^3 + X^2 + X + 1.\end{aligned}$$