INTRODUCTION

In this chapter, we study sets with additional structure, induced by one or more binary operations on the elements of the set. These discrete structures are called as algebraic systems as they obey a set of rules or axioms which are similar to the rules of addition and multiplication of numbers in elementary algebra. Infact many of these structures are prototype models of mathematical systems, with which we are familiar.

We first introduce a general algebraic system and discuss its properties. We then concentrate our attention on some special algebraic systems such as semigroups, groups, rings and fields.

An important application of groups is in coding theory where techniques are developed for detecting and correcting errors in transmitted data. The section on codes discusses some of these techniques in detail.

Besides coding theory, algebraic systems are also widely applied in the design of computer hardware and development of software especially formal language theory and finite state machines.

7.1 ALGEBRAIC SYSTEM

Let us first define an operation on the elements of a set, such that the resulting element is also an element of the set.

7.1.1 Definition

An n-ary operation on a non-empty set A is a function $f : A^n \to A$, A^n being the product set of A.

Observe the following properties that a binary operation must satisfy.

(i) The n-ary operation must be defined for each n-tuple $(a_1, a_2, \ldots, a_n) \in A$.

(ii) Since f is a function, only one element of A should be assigned to each n-tuple of A^n.

If n = 1, f is called **unary,**

if n = 2, f is called **binary,**

if n = 3, f is called **ternary** and so on.

Let us consider the following examples.

Examples

(i) The function $f : Z \to Z$, where

$$f(x) = -x, \text{ is unary,}$$

(ii) $f: Z \times Z \to Z$, defined as

$$f(x, y) = x + y, \text{ is binary,}$$

(iii) $f: Z \times Z \times Z \to Z$, defined as

$$f(x, y, z) = y \text{ if } x \neq 0$$
$$= z \text{ otherwise,}$$

is ternary.

We now proceed to define an algebraic system.

7.1.2 Definition

An algebraic system is an ordered pair (A, F) where

(i) A is a set of elements, called as the **carrier** of the algebra.

(ii) F is a finite set of m-ary operations on the carrier, m being a variable.

In the notation for an algebraic system, the carrier set A is first specified, followed by the elements of F, which are actually listed, viz (A, f_1) or (A, f_1, f_2) etc.

Examples

(i) Let $E = \{0, 2, 4, \ldots\}$. Then E with the binary operation of addition + represents an algebraic system (E, +).

(ii) The set of integers Z with the two binary operations of addition + and multiplication × is an algebraic system, and is denoted as (Z, +, ×).

(iii) The set of real numbers $\mathbb{R}$, with a single unary operation minus – and two binary operations of addition and multiplication is an algebraic system denoted by $(\mathbb{R}, -, +, \times)$.

(iv) For a fixed integer $n > 0$, let $M_n(\mathbb{R})$ denote the set of all $n \times n$ matrices. Then under the binary operation of matrix addition, $M_n(\mathbb{R})$ forms an algebraic system $(M_n(\mathbb{R}), +)$.

Similarly, under matrix multiplication, $(M_n(\mathbb{R}), \times)$ is another algebraic system.

(v) Let P(A) denote the power set of a non-empty set A. Then P(A) together with the set operations of union, intersection and complementation forms an algebraic system $(P(A), \cup, -)$.

(vi) Let $E = \{a, b\}$ be a set of symbols, called as the **alphabets**. A **word** over E is a finite string of symbols a, b, with possible repetitions, e.g. a, aa, abab, etc. Given two words x and y. We can form a new word xy by simply just opposing the symbols of x with those of y in the order xy. For example, if x = aa, y = aba, then xy = aaaba, whereas yx = abaaa. This operation is called as **concatenation**. If E^* denotes the set of all words over E, then concatenation is a binary operation on E^*.

In what follows, we will deal with algebraic systems, having only binary operations.

7.2.1 **D**

A binary operation $*$ on A is said to be **commutative** if $a * b = b * a$, for all elements $a, b \in A$.

Examples

(i) The binary operation of addition on the set of integers is commutative, but the operation of subtraction on the set of integers is not commutative.

(ii) The binary operation of multiplication on the set of integers is commutative.

7.2.2 Definition

A binary operation $*$ on A is said to be **associative** if

$$a * (b * c) = (a * b) * c, \text{ for all elements, } a, b, c \in A.$$

Example

(i) The binary operation of addition on the set of integers is associative, whereas the binary operation of subtraction is not associative.

(ii) The binary operation of multiplication on the set of integers is associative.

7.2.3 Definition

A binary operation $*$ on A is said to satisfy the **idempotent** property if $a * a = a$, for all $a \in A$.

Example

(i) Let L be a lattice with the operators $\wedge$ (meet) and $\vee$ (join). Then $\wedge$ and $\vee$ are binary operations and we know that

$$a \vee a = a,$$

$$a \wedge a = a, \quad \text{for all } a \in A.$$

Hence both $\wedge$ and $\vee$ satisfy the idempotent property.

7.2.4 Tables of Binary Operations

If $A = \{a_1, a_2, \ldots, a_n\}$ is a finite set, we can define a binary operation on A, by means of a table, is shown below. The entry in the i-th row and j-th column denotes the element $a_i * a_j$.

$*$	a_1	a_2	a_j	a_n
a_1				
a_2				
a_i			$a_i * a_j$	
a_n				

Example

Let A = {0, 1} and let × denote multiplication. Then we have the binary table

×	0	1
0	0	0
1	0	1

SOLVED EXAMPLES

1. For each of the following, determine whether $*$ is a binary operation :

   (i) $\mathbb{R}$ is the set of real numbers and $a * b = ab$.

   (ii) Z^+ is the set of positive integers and $a * b = a / b$.

   (iii) On Z^+ where $a * b = a - b$.

   (iv) On $\mathbb{R}$, where $a * b = \min \{a, b\}$.

   (v) On $\mathbb{R}$, where $a * b = a \times |b|$.

   (vi) On Z, where $a * b = a^b$.

Solution :

(i) Yes, since $f : \mathbb{R}^2 \to \mathbb{R}$ defined as $f(a, b) = ab$ is a function, with $a\, b \in \mathbb{R}$.

(ii) No, since $(a, b) \in Z^+ \times Z^+$ does not imply that $a * b = a / b \in Z$

$(1, 2) \in Z^+ \times Z^+$, but $1/2 \notin Z^+$.

(iii) No, since $(1, 2) \in Z^+ \times Z^+$ but

$$1 - 2 = -1 \notin Z^+$$

(iv) Yes, since $*$ is a function, with $\min \{a, b\} \in \mathbb{R}$.

(v) Yes, since $*$ is a function, with $a \times |b| \in \mathbb{R}$.

(vi) No, since $2 * (-1) = 2^{-1} = \frac{1}{2} \notin Z$.

2. For each of the following, determine whether the binary operation $*$ is commutative or associative :

   (i) N is the set of natural numbers and $a * b = a + b + 2$, for $a, b \in N$.

   (ii) On N, where $a * b = \max (a, b)$.

   (iii) On N, where $a * b = \min (a, b)$.

   (iv) On N, where $a * b = \min (a, b + 2)$

   (v) On $\mathbb{R}$, where $a * b = ab + 2b$.

   (vi) On $\mathbb{R}$, where $a * b = ab / 3$.

   (vii) On the set of non-zero real numbers, $a * b = a / b$.

Solution :

(i) $*$ is commutative since $a * b = a + b + 2$ and $b * a = b + a + 2$. Hence both are equal.

$$a * (b * c) = a * (b + c + 2)$$

$$= a + (b + c + 2) + 2 = a + b + c + 4.$$

$$(a * b) * c = (a + b + 2) * c$$

$$= (a + b + 2) + c + 2$$

$$= a + b + c + 4$$

Hence $*$ is associative.

(ii) $a * b = \max(a, b) = \max(b, a) = b * a$. Hence $*$ is commutative.

Let $a, b, c \in N$. Consider $b * c$.

$b * c = \max\{b, c\}$.

$\therefore \quad b * c = b \quad$ if $b \geq c$

or $\quad = c \quad$ if $c \geq b$

Let us suppose $\{b, c\} = b$, so that

$$b * c = b.$$

Then $\quad a * (b * c) = \max\{a, b\}$

$= a \quad$ if $a \geq b$

or $\quad = b \quad$ if $b \geq a$

If $a \geq b$, then $a * (b * c) = a$

Then $\quad a * b = \max\{a, b\} = a.$

Hence $\quad (a * b) * c = \max\{a, c\} = a,$ since $a \geq b$ and $b \geq c$.

Hence if $a \geq b \geq c$, then $(a * b) * c = a * (b * c)$.

Similarly, one can prove $(a * b) * c = a * (b * c)$, for other cases.

Hence $*$ is associative.

(iii) $*$ is commutative as well as associative. Proof is similar to (ii).

(iv) $*$ is not commutative since

$$2 * 3 = \min(2, 5) = 2, \quad \text{whereas}$$

$$3 * 2 = \min(3, 4) = 3.$$

$*$ is also not associative since

$$4 * (3 * 1) = 4 * 3 = 4, \text{ while}$$

$$(4 * 3) * 1 = 4 * 1 = 3.$$

(v) $*$ is not commutative since

$$2 * 3 = 6 + 6 = 12, \text{ while}$$

$$3 * 2 = 6 + 4 = 10$$

Clearly $*$ is also not associative.

(vi) $*$ is commutative and associative.

(vii) $*$ is not commutativ; and $*$ is also not associative since $a * (b * c)$

$$= a * (b/c) = a / b/c = ac / b \text{ ; whereas}$$

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

$$= \frac{a}{bc}$$

3. Let $(A, *)$ be an algebraic system where $*$ is a binary operation such that for any $a, b, \in A$, $a * b = a$.

(i) Show that $*$ is an associative operation.

(ii) Can $*$ ever be a commutative operation ?

Solution :

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

$= a * c = a$. Hence $*$ is associative.

(ii) $*$ is commutative only if $a * b = b * a$, i.e. $a = b$, for all $a, b \in A$. This is possible if A is the singleton set {a} and $a * a = a$, i.e. $*$ is an idempotent operation on A.

4. Let $(A, *)$ be an algebraic system such that for all $a, b, c, d \in A$,

$$a * a = a,$$

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

Show that $a * (b * c) = (a * b) * (a * c)$

Solution : Since $a * a = a$,

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

$$= (a * b) * (a * c)$$ (by the second condition)

5. Let $(A, *)$ be an algebraic system such that for all $a, b \in A$,

$$(a * b) * a = a$$

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

(i) Show that $a * (a * b) = a * b$, for all $a, b, \in A$

(ii) Show that $a * a = (a * b) * (a * b)$, for all $a, b \in A$.

(iii) Show that $a * a = b * b$, for all a, b.

(iv) Show that $a * b = b * a$ iff $a = b$.

(v) Let $(A, *)$ satisfy the additional condition $a * b = (a * b) * b$, for all $a, b \in A$. Show that $*$ is idempotent and commutative.

Solution :

(i) $a * (a * b) = ((a * b) * a) * (a * b)$,

since $a = (a * b) * a$, (by the first condition)

Now let $c = a * b$.

Then RHS $= (c * a) * c = c$ again by the first condition.

Hence $a * (a * b) = a * b$

(ii) $a * a = ((a * b) * a) * a$

$= (c * a) * a$, putting $a * b = c$

$= (a * c) * c$

$= (a * (a * b)) * (a * b)$

$= (a * b) * (a * b)$ (by (i))

(iii) $a * a = (a * b) * (a * b)$ (by (ii))

$= c * c$, where $a * b = c$

$= (c * b) * (c * b)$ (by (ii))

$= ((a * b) * b) * ((a * b) * b)$

$= ((b * a) * a) * ((b * a) * a)$

$= (b * a) * (b * a)$ } (by (ii))

$= b * b$ }

(iv) If $a = b$, $a * b = b * a$.

Conversely, let $a * b = b * a$.

Then $a = (a * b) * a = (b * a) * a$

$= (a * b) * b$ (by given condition)

$= (b * a) * b$

$= b$ (by given condition)

(v) $a * a = (a * a) * a$ (by given condition)

$= a$, since $(a * b) * a = a$ for all $a, b \in A$.

To show $*$ is commutative

$$a * b = (a * b) * b$$

$$= (b * a) * a$$

$$= b * a \quad \text{by given condition.}$$

Hence $*$ is commutative.

6. The following table, of a binary operation $*$ is given. Is $*$ commutative ?

$*$	a	b	c
a	b	c	a
b	c	b	a
c	a	b	c

Solution : From the table,we observe the following :

$$a * b = c, \quad b * a = c$$

$$a * c = a, \quad c * a = a$$

$$b * c = a, \quad c * b = b, \text{ and } a \neq b.$$

Hence $*$ is not commutative.

7. Consider the binary operation $*$ defined on the set A = {a, b, c, d} by the following table :

$*$	a	b	c	d
a	a	c	b	d
b	d	a	b	c
c	c	d	a	a
d	d	b	a	c

Find

(i) $c * d$ and $d * c$

(ii) $b * d$ and $d * b$

(iii) $a * (b * c)$ and $(a * b) * c$

(iv) Is $*$ commutative, associative ?

Solution :

(i) $c * d = a, \quad d * c = a$

(ii) $b * d = c, \quad d * b = b$

(iii) $b * c = b, \quad a * (b * c) = a * b = c$

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

(iv) $*$ is not commutative, since $b * d \neq d * b$.

$*$ is also not associative, since $a * (b * c) \neq (a * b) * c$.

We shall now study some special algebraic systems.

7.3 SEMIGROUPS

Let $(A, *)$ be an algebraic system, with a binary operation $*$ on A. Then $(A, *)$ is called a **semigroup** if $*$ is associative, i.e.

$$a * (b * c) = (a * b) * c, \text{ for all } a, b, c \in A.$$

The semigroup is further said to be commutative if $*$ is commutative.

Examples

(i) $(Z, +)$ is a commutative semigroup.

(ii) $(Z, \times)$ is a commutative semigroup.

(iii) For a non-empty set A, $(P(A), \cup)$ is a commutative semigroup and so is $P(A), \cap)$.

(iv) $(Z, -)$ is not a semigroup, since subtraction is not associative.

7.3.1 Definition

(i) An element e in $(A, *)$ is called as **left identity** element if for each element $x \in A$, $e * x = x$.

(ii) e is called a **right** identity if $x * e = x$, for all $x \in A$.

A semigroup can have more than one left (or right) identity, as seen from the following example.

Example : The algebraic system $(A, *)$ whose table is given below is a semigroup.

*	a	b	c
a	a	b	c
b	a	c	b
c	a	b	c

Since the rows for both the elements a and c are equal to [a b c] it follows that both a and c are left identities. However there is no right identity since none of the columns are equal to [a b c].

7.3.2 Definition

An element e in a semigroup $(A, *)$ is called an **identity** element if $a * e = e * a = a$, for all $a \in A$, i.e. e is both a left identity and right identity. It is clear that e is unique.

Examples

(i) The semigroup $(Z, +)$ has the identity element which is the number 0.

(ii) The semigroup $(Z, \times)$ has the identity element which is the number 1.

(iii) The semigroup $(N, +)$ has no identity element, where the set N is the set of natural numbers, excluding 0.

7.3.3 Definition

A **monoid** is a semigroup $(A, *)$ that has an identity element.

Examples

(i) Let $E = \{0, 2, 4, 6, \ldots\}$. Then $(E, +)$ is a monoid, with the number 0 as the identity element.

(ii) Let E^* be the set of all words over the alphabet set $E = \{a, b\}$. Let concatenation be the binary operation. The empty word Λ is the identity for E^*. Hence E^* under concatenation is a monoid.

7.3.4 Definition

Let $(A, *)$ be an algebraic system, and let B be a subset of A. Then B is said to be closed under $*$, if for any elements $b, c \in B$, $b * c$ is also in B.

7.3.5 Definition

Let $(A, *)$ be a semigroup and let B be a non-empty subset of A, such that B is closed under $*$. Then $(B, *)$ is itself a semigroup and is called a **sub semigroup** of $(A, *)$.

7.3.6 Definitions

Let $(A, *)$ be a monoid, and let B be a non-empty subset of A. Then $(B, *)$ is called a **submonoid** of $(A, *)$ if

(i) B is closed under $*$.

(ii) The identity element $e \in B$.

Example

Let $E = \{0, 2, 4, 6, \ldots\}$. Then $(E, +)$ is a submonoid of $(Z, +)$.

The concepts of semigroups and monoids are used in finite state machines.

7.3.7 Definitions

Let $(A, *)$ be a monoid with identity element e. Let B be a non-empty subset of A. Then the monoid generated by B, denoted by $< B >$ is defined as follows :

(i) $e \in < B >$, and if $b \in B$, then b also is in $< B >$, that is $B \subseteq < B >$.

(ii) $< B >$ is closed under $*$.

(iii) The only elements of $< B >$ are those obtained from steps (i) and (ii).

Examples

1. Find the smallest submonoid of $(Z, +)$ generated by the set $\{-4, 6\}$.

Solution : Let $B = \{-4, 6\}$. Then $< B >$ is obtained as follows :

(i) $0, 6, -4 \in < B >$.

(ii) If $x, y \in < B >$, then $x + y \in < B >$.

(iii) $< B >$ contains only the elements obtained from steps (i) and (ii).

Hence $< B > = \{0, 6, -4, 2, -2, 4, 8, -6, 10, \ldots\}$

$= \{, \ldots -6, -4, -2, 0, 2, 4, 6, 8, 10, \ldots\}$

$=$ set of even integers.

(ii) Let $E = \{a, b\}$ and $B = \{aa, bbb\}$.

Find the submonoid of E^* generated by B.

Solution : $< B > = \{\wedge, aa, bbb, aabbb, bbbaa, aaaa, bbbbbb, \ldots\}$.

(iii) Let $A = \{a, b, c, d\}$ and let C(A) denote the set of all functions on A. Let $f : A \to A$ be defined by the following diagram.

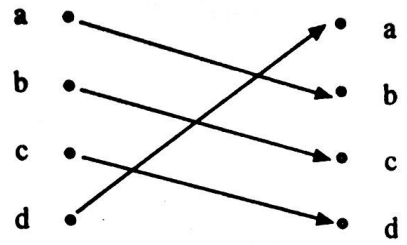

Fig. 7.1

Find the submonoid of (C(A), o), where o denotes composition of functions, generated by f.

Solution : The identity element is 1_A. Consider fof = f^2 which is defined by the following diagram.

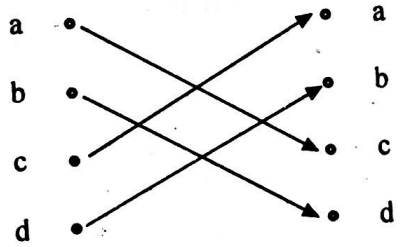

Fig. 7.2

fofof = f^3 is defined as

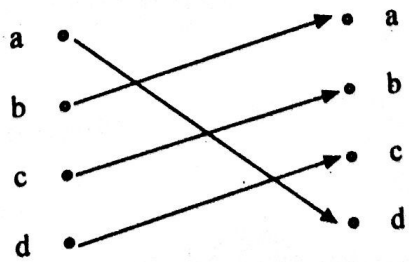

Fig. 7.3

f^4 is defined as

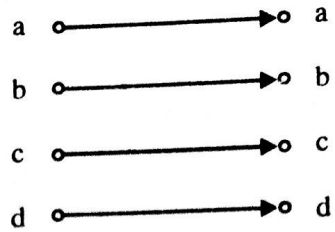

Fig. 7.4

$\therefore \quad f^4 = 1_A$

Hence the submonoid generated by f is the set $\{1_A, f, f^2, f^3\}$.

SOLVED EXAMPLES

1. Show that the set of integers of the form $3m + 1$ is closed under multiplication. Is this set a submonoid of $(Z, \times)$?

Solution : Let $B = \{ n \in Z \mid n = 3m + 1 \}$.

Let $r, s \in B$, then $r = 3m + 1$ and $s = 3n + 1$ for $m, n \in Z$.

then $rs = (3m + 1)(3n + 1)$

$= 9mn + 3n + 3m + 1$

$= 3(m + n + 3mn) + 1$

$= 3t + 1$, where $t = m + n + 3mn$.

Hence B is closed under $\times$.

Since the identity element 1 can be written as $1 = 30 + 1$, $1 \in B$. Hence B is a submonoid of $(Z, \times)$.

2. (i) Determine the submonoid of $(Z, +)$ generated by 6 and 9.

(ii) Submonoid of $(Z, +)$ generated by -3 and 5.

Solution : (i) Let $S = \{6, 9\}$

then $< S > = \{0, 6, 9, 12, 15, 18, 21, 24, \ldots\}$

(ii) Let $S = \{-3, 5\}$

then $< S > = \{0, -3, 5, 2, -1, -2, 4, 7, -4, 1, 3, \ldots\}$

$= \{, \ldots -3, -2, -1, 0, 1, 2, 3, \ldots\}$

$= Z$

3. Let $A = \{a, b\}$. Which of the following tables define a semigroup of A ? Monoid on A ?

(i)

*	a	b
a	a	b
b	a	a

(ii)

*	a	b
a	a	b
b	b	b

(iii)

*	a	b
a	b	a
b	a	b

(iv)

*	a	b
a	a	b
b	b	a

Solution : (i) * is not associative. Consider $b * (a * b) = b * b = a$. On the other hand $(b * a) * b = a * b = b$. Therefore (A, *) is not a semigroup and hence not a monoid.

(ii) $a * (b * b) = a * b = b$

$(a * b) * b = b * b = b$

$a * (a * b) = a * b = b$

$(a * a) * b = a * b = b$

$a * (b * a) = a * b = b$

$(a * b) * a = b * a = b$

Similarly * is associative for the remaining combinations.

The identity element is a. Hence (A, *) is not only a semigroup, but it is also a monoid.

(iii) $a * (a * b) = a * a = b$

$(a * a) * b = b * b = b$

Similarly checking for other combinations, one can show that * is associative. The identity element is b. Hence (A, *) is not only a semigroup, but it is also a monoid.

(iv) $a * (b * a) = a * b = b$

$(a * b) * a = b * a = b$

Similarly one can verify that * is associative for other combinations as well.

Hence (A, *) is a semigroup. Note that $a * b = b = b * a$, and $a * a = a$.

Hence the identity element is a.

Hence (A, *) is also a monoid.

4. Let A = {a, b}. Write the operation table for the semigroup (P(A), ∪).

Solution : $P(A) = \{\phi, A, \{a\}, \{b\}\}$.

Table :

∪	ϕ	A	{a}	{b}
ϕ	ϕ	A	{a}	{b}
A	A	A	A	A
{a}	{a}	A	{a}	A
{b}	{b}	A	A	{b}

5. Prove that the intersection of two subsemigroups of a semigroup (S, *) is a subsemigroup of (S, *).

Solution : Let S_1, S_2 be subsemigroups of S. We have only to show that $S_1 \cap S_2$ is closed under $*$. Let $x, y \in S_1 \cap S_2$. Then $x, y \in S_1$ and $x, y \in S_2$. Since S_1 and S_2 are subsemigroups, $x * y \in S_1$ and $x * y \in S_2$ which means that $x * y \in S_1 \cap S_2$. Hence $S_1 \cap S_2$ is closed under $*$ Therefore $(S_1 \cap S_2, *)$ is a subsemigroup.

6. Prove that the intersection of two submonoids of a monoid $(S, *)$ is a submonoid of $(S, *)$.

Solution : Let S_1 and S_2 be submonoids of S. Then by the above example $(S_1 \cap S_2, *)$ is a subsemigroup. We have only to prove the identity element is in $S_1 \cap S_2$ which is obvious. Hence $(S_1 \cap S_2, *)$ is a submonoid.

7. Show that the set of all idempotents in a commutative monoid S is a submonoid of S.

Solution : Recall an element $x \in S$ is called an idempotent if $x * x = x$. Let T be the set of all idempotents in S. Then $e \in T$ since $e * e = e$. We have only to prove that T is closed under $*$. For $x, y \in T$ consider $(x * y) * (x * y)$.

$$= ((x * y) * x) * y \qquad \text{(by associativity of } *)$$

$$= (y * (x * x)) * y$$

(using both commutativity and associativity)

$$= (y * x) * y$$

$$= x * (y * y)$$

$$= x * y$$

We have thus shown that $x * y$ is an idempotent element, and hence $x * y \in T$. T is therefore closed under $*$ and is hence a submonoid of S.

8. Let Z_n denote the set of integers $\{0,1,2,\ldots, n-1\}$. Let Θ be binary operation on Z_n such that

$$a \Theta b = \text{the remainder of } ab \text{ divided by } n.$$

(i) Construct the table for the operation Θ for $n = 4$.

(ii) Show that (Z_n, Θ) is a semigroup for any n.

Solution : (i) $Z_4 = \{0, 1, 2, 3\}$.

Table

Θ	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	0	2
3	0	3	2	1

(ii) Let $a \Theta b = r$, where

$$ab = pn + r \quad \ldots (1)$$

Then $(a \Theta b) \Theta c = r \Theta c$

$= s$, where $rc = qn + s$ ... (2)

Let $b \Theta c = t$, where $bc = ln + t$ ... (3)

$a \Theta (b \Theta c) = a \Theta t = k$, where $at = mn + k$ ... (4)

We have to prove $s = k$.

Now $a(bc) = aln + at = aln + mn + k$ ... (5)

Also $(ab)c = (pn + r)c = pnc + rc$

$= pnc + qn + s$ ... (6)

Now since equations (5) and (6) are equal, it follows that $k = s$.

Hence $(a \Theta b) \Theta c = a \Theta (b \Theta c)$.

Hence (Z_n, Θ) is a semigroup for any n.

9. Let $(A, *)$ be a semigroup. Let a be an element in A. Consider a binary operation $\square$ on A such that for every $x, y \in A$, $x \square y = x * a * y$.

Show that $\square$ is an associative operation.

Solution: $(x \square y) \square z = (x * a * y) \square z$

$= x * a * y * a * z$

Now $x \square (y \square z) = x \square (y * a * z)$

Hence $(x \square y) \square z = x \square (y \square z)$

therefore $\square$ is an associative operation.

10. Let $(\{a, b\}, *)$ be a semigroup where

$a * a = b$. Show that

(i) $a * b = b * a$

(ii) $b * b = b$.

Solution: (i) $a * b = a * (a * a) = (a * a) * a$ (as $*$ is associative)

$= b * a$

(ii) Since $(A, *)$ is closed under $*$, $a * b = a$ or $a * b = b$.

Let us first assume $a * b = a$.

Then by associativity property of $*$,

$a * (a * b) = (a * a) * b$

$\Rightarrow a * a = b * b$

$\Rightarrow b = b * b$

Next assume $a * b = b$.

Then $a * (a * b) = (a * a) * b$

$\Rightarrow a * b = b * b$

$\Rightarrow b = b * b$

Hence in either case $b * b = b$.

Hence the result is proved.

7.4 GROUPS

A **group** $(G, *)$ is a monoid, with identity e, such that for every element $a \in G$ there exists an element $a^{-1} \in G$, called as the inverse of a, such that $a * a^{-1} = a^{-1} * a = e$.

Thus a group is a set G together with a binary operation $*$ on G such that

(i) $(a * b) * c = a * (b * c)$, for all $a, b, c \in G$ (i.e. $*$ is **Associative**)

(ii) There is a unique element e in G such that $a * e = e * a$, for $a \in G$. (**Identity** element)

(iii) For each $a \in G$, there exists an element $a^{-1} \in G$, such that $a * a^{-1} = a^{-1} * a = e$.

(**Inverse** element)

7.4.1 Definition

A group $(G, *)$ is called an **Abelian** group if $a * b = b * a$, for all $a, b \in G$.

Examples

(i) The set of all integers Z with the operation of addition is a group. The identity element is the number 0 and for every $n \in Z$, its inverse is $(-n)$.

(ii) The set $Q^* = Q - \{0\}$ of non-zero rational numbers is a group under multiplication. The identity element is the number 1 and inverse of each element $p/q \in Q^*$ is q/p.

(iii) The set of all **non zero** real numbers under the operation of multiplication is a group, with the number 1 as the identity element; and inverse of each number a is $1/a$.

The next is a very important example of a group.

(iv) Let n be any positive integer $(n > 0)$. For elements $x, y \in Z$, define a relation $\equiv$ on them as $x \equiv y$ or $x = y \pmod n$ if $x - y$ is divisible by n. The relation is an equivalence relation and for each element $x \in Z$, we obtain the corresponding equivalence class $[x]$.

There are in all n distinct equivalence classes. Let Z_n denote the set of all equivalence classes; Z_n is called as set of **residue classes modulo n**, where $[x] = [y]$ implies $x = y \pmod n$.

For any two elements $[x], [y] \in Z_n$ define $[x] + [y] = [x + y]$. One can easily see that $+$ is both associative and commutative. The identity element is $[0]$, and for each $[x] \in Z_m$, its inverse is $[m - x]$, since $[x] + [m - x] = [x + m - x] = [m] = [0]$. Thus $(Z_m, +)$ is an abelian group.

(v) If p is a prime number, then $Z_p - \{0\} = Z_p^*$ is a multiplicative abelian group where the multiplication $\cdot$ is defined naturally as

$$[x] \cdot [y] = [x \cdot y].$$

However, for a non-prime number Z_m^* is not a group. Consider $Z_4^* = \{[1], [2], [3]\}$. Z_4 is not a group since $[2] \cdot [2] = [4] = [0] \notin Z_4^*$. Hence Z_4^* is not closed under $\cdot$, and therefore it is not a group.

We give below the group tables for Z_3 and Z_4 under $+$.

+	[0]	[1]	[2]
[0]	[0]	[1]	[2]
[1]	[1]	[2]	[0]
[2]	[2]	[0]	[1]

$(Z_3, +)$

+	[0]	[1]	[2]	[3]
[0]	[0]	[1]	[2]	[3]
[1]	[1]	[2]	[3]	[0]
[2]	[2]	[3]	[0]	[2]
[3]	[3]	[0]	[1]	[2]

$(Z_4, +)$

(iv) Let A = {a, b, c} and let F denote the set of functions from A to A, which are given below.

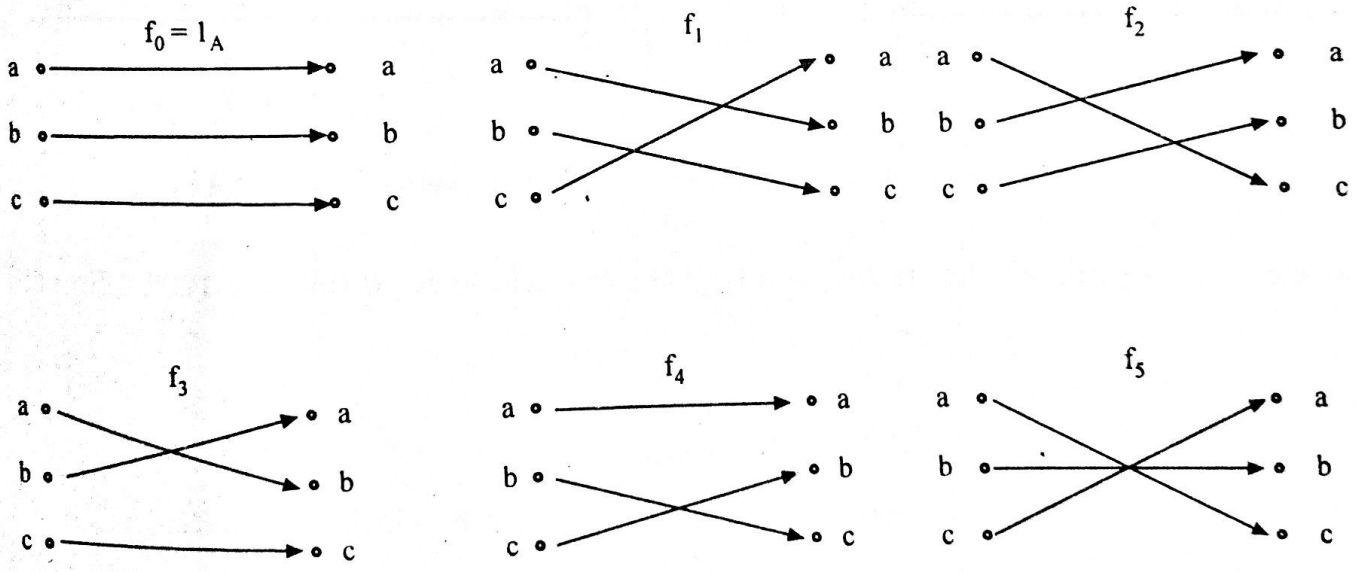

Fig. 7.5

The set (F, •), where • denotes composition forms, a group. The group table is given below.

•	f_0	f_1	f_2	f_3	f_4	f_5
f_0	f_0	f_1	f_2	f_3	f_4	f_5
f_1	f_1	f_2	f_0	f_5	f_3	f_4
f_2	f_2	f_0	f_1	f_4	f_5	f_3
f_3	f_3	f_4	f_5	f_0	f_1	f_2
f_4	f_4	f_5	f_3	f_2	f_0	f_1
f_5	f_5	f_3	f_4	f_1	f_2	f_0

This group is non-abelian, since $f_1 \cdot f_3 = f_5$ and $f_3 \cdot f_1 = f_4$.

(vii) **The Permutation Group (Group of Symmetries of a triangle) :** Consider an equilateral triangle (Fig. 7.6) with vertices 1, 2, 3. Since the triangle is determined by its vertices, a symmetry of the triangle is a **permutation** of the vertices. We describe the various symmetries of this triangle.

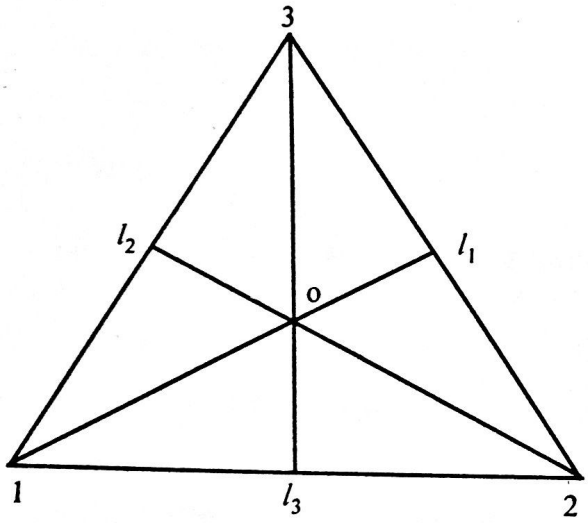

Fig. 7.6

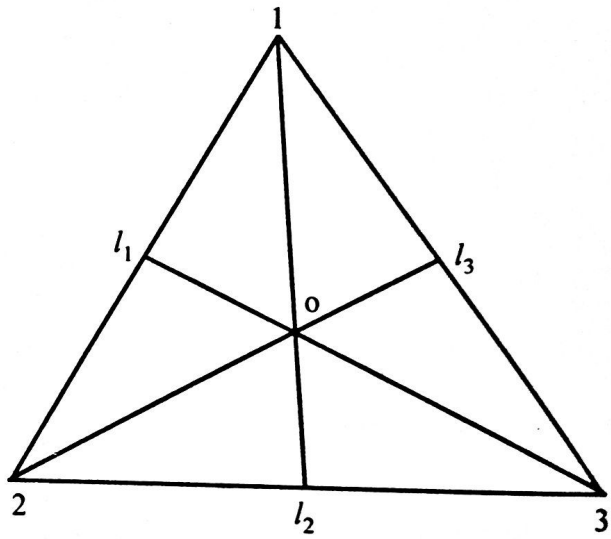

Fig. 7.7

$f_0 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}$ is the identity permutation, that keeps the vertices undisturbed.

Next consider the anti-clockwise rotation f_2 of the triangle about 0 through 120°. (Fig. 7.7). hen

$$f_1 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$$

Next obtain an anti-clockwise rotation f_3 about 0 through 240°, which is the permutation

$$f_2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$$

Finally, there is an anti-clockwise rotation about 360^o which is the same as f_1.

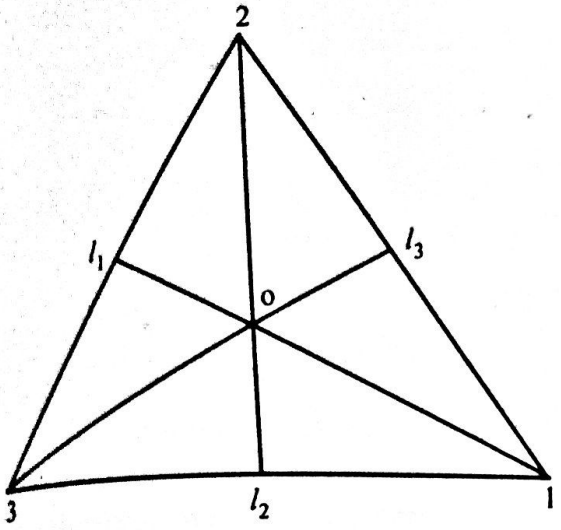

Fig. 7.8

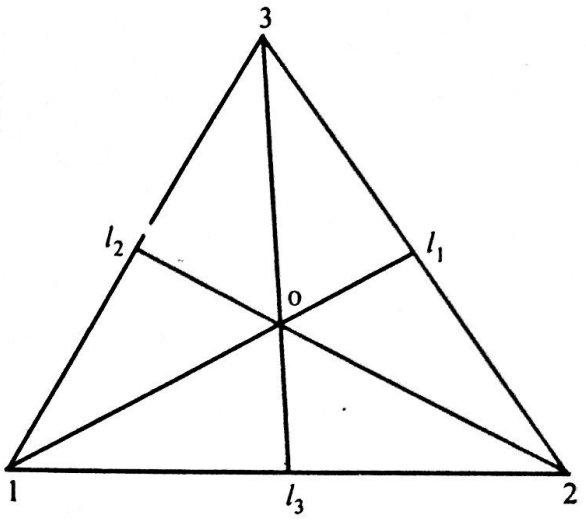

Fig. 7.9

We also obtain three additional symmetries of the triangle g_1, g_2 and g_3 by reflecting about the lines l_1, l_2 and l_3 respectively. We denote these reflections by the following permutations.

$$g_1 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}, \quad g_2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$$

$$g_3 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$$

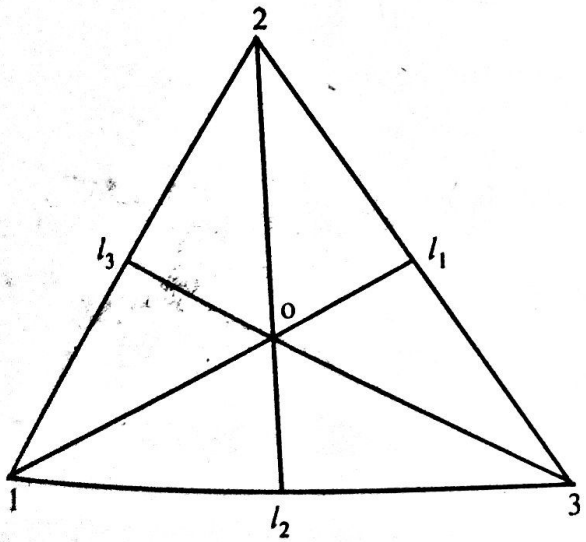

Fig. 7.10

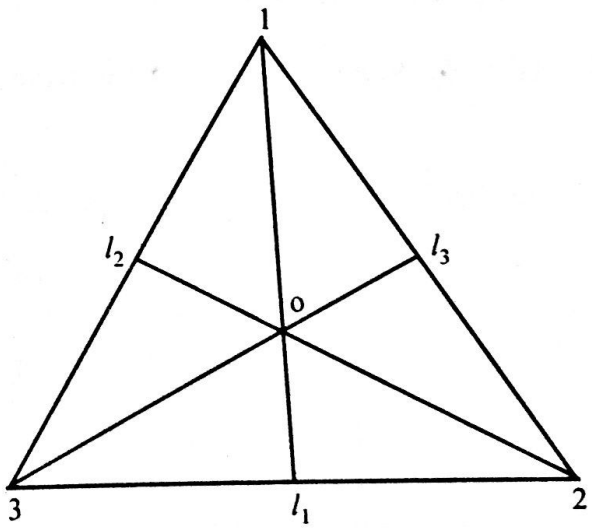

Fig. 7.11

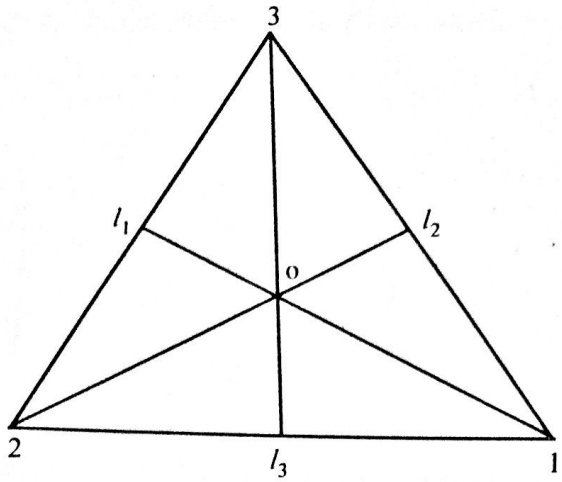

Fig. 7.12

We denote the set of all these permutations by $S_3 = \{f_0, f_1, f_2, g_1, g_2, g_3\}$. S_3 is a non-abelian group of order 6, under composition $\bullet$, with f_1 as the identity element.

$\bullet$	f_0	f_1	f_2	g_1	g_2	g_3
f_0	f_0	f_1	f_2	g_1	g_2	g_3
f_1	f_1	f_2	f_0	g_3	g_1	g_2
f_2	f_2	f_0	f_1	g_2	g_3	g_1
g_1	g_1	g_2	g_3	f_0	f_1	f_2
g_2	g_2	g_3	g_1	f_2	f_0	f_1
g_3	g_3	g_1	g_2	f_1	f_2	f_0

Group table of S_3

(viii) If $(G, *)$ and $(G', *')$ are groups then $(G \times G', \bullet)$ is a group with group operation defined by

$(a_1, b_1) \bullet (a_2, b_2) = (a_1 * a_2, b_1 *' b_2)$, called as the **product** group.

The following is an example of a product group.

Let $G = G' = Z_2$. For simplicity of notation, let us denote the equivalence class [0] by $\bar{0}$ and [1] by $\bar{1}$.

Then the multiplication table for the product group $Z_2 \times Z_2$ is given below.

	$(\bar{0}, \bar{0})$	$(\bar{1}, \bar{0})$	$(\bar{0}, \bar{1})$	$(\bar{1}, \bar{1})$
$(\bar{0}, \bar{0})$	$(\bar{0}, \bar{0})$	$(\bar{1}, \bar{0})$	$(\bar{0}, \bar{1})$	$(\bar{1}, \bar{1})$
$(\bar{1}, \bar{0})$	$(\bar{1}, \bar{0})$	$(\bar{0}, \bar{0})$	$(\bar{1}, \bar{1})$	$(\bar{0}, \bar{1})$
$(\bar{0}, \bar{1})$	$(\bar{0}, \bar{1})$	$(\bar{1}, \bar{1})$	$(\bar{0}, \bar{0})$	$(\bar{1}, \bar{0})$
$(\bar{1}, \bar{1})$	$(\bar{1}, \bar{1})$	$(\bar{0}, \bar{1})$	$(\bar{1}, \bar{0})$	$(\bar{0}, \bar{0})$

7.4.2 Definition

Let $(G, *)$ be a group. The order of G is the cardinality of G, denoted by $|G|$.

Examples

(i) The group $(Z, +)$ is of infinite order.

(ii) The group $(Z_m, +)$ is of finite order viz. m.

7.4.3 Definition

Let $(G, *)$ be a group. Let $a \in G$. The order of a is the **smallest** positive integer n such that $a * a * \ldots * a = a^n = e$. If no such value of n exists for a, then a is said to be of infinite order.

Example

(i) In $(Z, +)$, every number $n \neq 0$ is of infinite order.

(ii) In $(Z_4, +)$, order of [1] is 4, order of [2] is 2, order of [3] is 4.

7.5 BASIC PROPERTIES OF A GROUP

1. Uniqueness of identity and inverse

7.5.1 Theorem

Let $(G, *)$ be a group, then

(i) Identity element e of G is unique.

(ii) Every element $x \in G$ has a unique inverse x^{-1} in G.

Proof : (i) Suppose there exists an element e' is G, with the same property as x. Then $x * e' = e' * x = x$, for all $x \in G$.

In particular, for $x = e$, we have $e * e' = e' * e = e'$. But since e is also an identity,

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

Hence. $$e = e'.$$

(ii) Let an element $y \in G$, such that for all $x \in G$, $x * y = y * x = e$ premultiplying by x^{-1}, we have $x^{-1} * (x * y) = x^{-1} * (y * x) = x^{-1} * e = x^{-1}$. Using the associativity of $*$, we have $(x^{-1} * x) * y = x^{-1}$ which implies $y = x^{-1}$.

Thus the theorem is proved.

Cancellation Laws

7.5.2 Theorem

(i) **Left cancellation law :** For $a \in G$, $a * x = a * y$ implies $x = y$; and

(ii) **Right cancellation law :** For $a \in G$, $x * a = y * a$ implies $x = y$.

Proof : Left as an exercise.

7.6 CYCLIC GROUP

A group $(G, *)$ is said to be a cyclic group if there exists an element $a \in G$ such that every element of G can be written as some power of a, viz a^k, for some integer k. By a^k, we mean $a * a * a \ldots * a$ (k times). We then say that G is generated by a or a is a generator of G.

A cyclic group is abelian, since for any two elements $a^r, a^s \in G$, $a^r * a^s = a^{r+s} = a^{s+r} = a^s * a^r$.

Examples

(i) The group $(Z_2, +)$ is cyclic generated by the equivalence class [1].

In general, the group $(Z_m, +)$ is a cyclic group of order m, generated by [1].

(ii) Let S be the unit circle and let ρ_o be a rotation of the circle through an angle $2\pi/n$. Then the set of rotations $\{\rho_o, \rho_o^2, \rho_o^3, \ldots, \rho_n^n\}$ forms a cyclic group of order n, under the operation composition of functions.

The following theorem is significant, as it describes, completely, the structure of finite cyclic groups.

7.6.1 Theorem

Let G be a cyclic group of order n. Then n is the smallest positive integer such that $a^n = e$, where a is a generator of G.

Proof : Consider the subset $\{a, a^2, \ldots\}$ of G. Since G is finite, the power of a must terminate at some stage. Hence there exists positive integers r and s such that $a^r = a^s$. Assume $r > s$. Then $a^{(r-s)} = e$. Since there exists atleast one element with this property, choose m least such that $a^m = e$. Now $m \leq n$, since otherwise order of g is greater than n. We shall show $m = n$. Suppose $m < n$. Then for any k such that $m < k \leq n$, by division algorithm $k = pm + q$, where $0 \leq q < m$.

Then $a^k = a^{pm+q} = (a^p)^m * a^q = a^q$.

Since $q < m$, $a^q \in \{a, a^2, \ldots, a^m\}$.

Since a is a generator for G, this means $G \subset \{a, a^2, \ldots, a^m\}$, which is absurd. Hence $m \nless n$ and therefore $m = n$.

7.7 SUBGROUPS

Subgroups are subsets of a group G, which inherit the group structure of G.

7.7.1 Definition

Let H be a non-empty subset of a group G. Then H is said to be a **subgroup** of $(G, *)$ if H is itself a group under $*$.

The singleton set $\{e\}$ is a subgroup of G.

The following theorem gives a necessary and sufficient conditions for a subset to be a subgroup.

7.7.2 Theorem

A non-empty subset H of $(G, *)$ is a subgroup iff

(i) $a, b \in H$ implies $a * b \in H$, i.e. H is closed under $*$.

(ii) $a \in H$ implies $a^{-1} \in H$.

Proof : Let H be a subgroup of G, then (i) and (ii) are satisfied.

Conversely, let conditions (i) and (ii) hold. We have to show that H satisfies the group axioms. For $a, b, c \in H$, $a * (b * c) = (a * b) * c$ holds for G and hence for H. Hence the associative law holds for H. Also by condition (ii) every element in H has an inverse in H. It remains to show that the identity element $e \in H$. Now by condition (ii) $a \in H$ implies $a^{-1} \in H$. Hence $a * a^{-1} = a^{-1} * a = e \in H$, by condition (i).

Thus the theorem is proved.

For a finite group however, condition (ii) becomes redundant as proved in the following theorem.

7.7.3 Theorem

If H is a non-empty finite subset of a group G and H is closed under multiplication, then H is a subgroup of G.

Proof : It is enough to show by Theorem 6.9.12 that whenever $a \in H$, $a^{-1} \in H$. Suppose $a \in H$, then $a^2, a^3, \ldots, a^m \in H$, as H is closed under $*$. This means that the infinite set $\{a, a^2, \ldots, a^m, \ldots\}$ is a subset of H, which is finite. This is possible only if the elements are repeated. Hence for some s, t, $s > t$, $a^s = a^t$. By cancellation law, this implies $a^{s-t} = e$. Hence $e \in H$. Since $s-t-1 \geq 0$, $a^{s-t-1} \in H$ and $a^{-1} = a^{s-t-1}$, as $a * a^{s-t-1} = a^{s-t} = e$. Thus $a^{-1} \in H$, completing the proof.

Examples

(i) For a positive integer n, let $H = nZ = \{ nx \mid x \in Z \}$. Then $(H, +)$ is a subgroup of $(Z, +)$.

(ii) Let $H = \{[0], [4]\}$ in $(Z_8, +)$. H is then a subgroup of Z_8.

(iii) Let G be the group of all 2×2 matrices $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ with $ad - bc \neq 0$, under matrix multiplication. Let $H = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix}, ad \neq 0 \right\}$. H is then a subgroup of G.

(iv) Let G be the group of all non-zero complex numbers $a + ib$ (a, b real) under multiplication. Let $H = \{ a + ib \mid a^2 + b^2 = 1 \}$. Then H is a subgroup of G.

7.8 COSETS

In this section, we shall see that a subgroup H defines an equivalence relation on a group G, so that G is partitioned into equivalence classes called as cosets.

7.8.1 Definition

Let $(G, *)$ be a group and let H be a subgroup of G. For $a, b \in G$, we say a is congruent to b modulo H, written as $a \equiv b \bmod H$, if $a * b^{-1} \in H$. One can easily see that the congruence relation is an equivalence relation on G. It therefore partitions G into equivalence classes called as **cosets** of H. The set of these equivalence classes is also called as the **quotient** set of G by H.

7.8.2 Definition

Let H be a subgroup of a group $(G, *)$. For $a \in G$, define

$Ha = \{ h * a \mid h \in H \}$. Then Ha is called a **right coset** of H in G.

Similarly, $aH = \{ a * h \mid h \in H \}$ is called a left coset of H in G.

a is called as the representative element of the coset aH or Ha. If $a \in H$, then $Ha = aH = H$.

Again one can easily show that the cosets are precisely the equivalence classes formed through the congruence relation.

Hence the right cosets of H in G partition G into disjoint subsets. Likewise, the left cosets of H in G yield a partition of G into disjoint subsets.

The concept of cosets as equivalence classes leads to the following theorem, known as Lagrange's theorem, which gives an important relationship between a group and its subgroup.

7.8.3 Theorem (Lagrange)

The order of a subgroup of finite order divides the order of the group.

Proof : Let $(G, *)$ be a finite group of order n and let H be a subgroup of G of order m. Consider a right coset Ha $a \in G$. If $a \in H$, then $Ha = H$, which means that number of elements in Ha is the same as the order of H, which means that m n. Next let $a \in G$ but $a \notin H$. Then for any two distinct elements $h_1, h_2 \in H$, $h_1 * a \neq h_2 * a$. Hence distinct elements in Ha correspond to distinct elements in H and vice versa. This means that each right (left) coset contains exactly m elements. Since the right (left) cosets partition G into disjoint subsets, each containing m elements, it follows that since order of G is n, we must have n/m cosets. This proves that m divides n.

7.8.4 Remarks

From Lagrange's theorem, we deduce the following :

(i) Any group of prime order has only the trivial group {e} as its proper subgroup.

(ii) Consider the permutation group $(S_3, 0)$ described in article 6.6.2, (Example vii) S_3 has subgroups of order 3 and order 2.

Finding these subgroups is left as an exercise.

7.9 NORMAL SUB-GROUPS

We have seen that a subgroup H of G induces an equivalence relation on G, so that G can be partitioned into equivalence classes. Our aim now, is to impose a group structure on the set of equivalence classes, so as to form the quotient group. For this, we must first define the product of two equivalence classes, so that this product is compatible with the group operation on G.

Let H be a subgroup of G, and let Ha, Hb be right cosets of H in G. We want to define Ha * Hb.

A natural way, that suggests itself is Ha * Hb = Hab. However, this definition makes sense only if Ha = aH. Then for $h_1, h_2 \in H$, $(h_1 * a) * (h_2 * b) = h_1 * h_3 * a * b \in Hab$.

Hence subgroups in which the right and left cosets are one and the same form an important class of subgroups called as normal subgroups. More formally, we have the following definition of a normal subgroup.

7.9.1 Definition

A subgroup H of G is said to be a **normal** subgroup of G if for every $a \in G$, aH = Ha.

Examples

(i) A subgroup of an abelian group is normal. For example, nZ is normal in Z (n > 0).

(ii) Consider the symmetric group $(S_3, 0)$, described in article 6.6.2 (Ex. vii). Then $H = \{f_0, g_2\}$ is a subgroup of S_3. But H is not normal in S_3. Consider $f_1 H = \{f_1, g_1\}$. But $Hf_1 = \{f_1, g_3\}$ since $f_1 H \neq H f_1$, it follows that H is not normal in S_3.

However consider $K = \{f_0, f_1, f_2\}$. Note that $f_2 = f_1^2$, so that $K = \{f_0, f_1, f_1^2\}$. One can show that every right coset of K in G is equal to a left coset of K is G and vice versa. Hence k is normal in G.

7.10 QUOTIENT GROUP

Let N be a normal subgroup of G. Then G/N is the set of cosets of N in G.

For two coset elements $g_1 N, g_2 N \in G/N$ define an operation * on G/N as $g_1 N * g_2 N = (g_1 * g_2) N$. Note that the operation * on G/N is induced by the operation * in G. (We use the same symbol for both the operations).

With this operation, G/N is a group, with identity element eN. The inverse of each element $g_1 N$ is naturally $g_1^{-1} N$. The other group axioms, one can easily verify.

7.11 HOMOMORPHISM OF GROUPS

While discussing quotient group, we have implicitly related elements of G and G/H by associating g with g = gH.

In other words, we have defined a function $\phi : G \to G/H$ where

$$\phi(g) = gH.$$

Note that $\phi(g_1 * g_2) = \phi(g_1) * \phi(g_2)$.

A function characterised by this property is defined below.

7.11.1 Definition

Let $(G, *)$ and $(G', *')$ be two semigroups, then a function $\phi : (G, *) \to G', *')$ is called a homomorphism of G and G' if for every $a, b \in G$, $\phi(a * b) = \phi(a) *' \phi(b)$.

In particular if G and G' are groups, then ϕ is called a group homomorphism.

We have the following theorem which shows that under a group homomorphism, identity is mapped onto identity, and inverse onto inverse.

7.11.2 Theorem

Let ϕ be a homomorphism of G into G', where G and G' are groups. Then

(i) $\phi(e) = e'$ is the identity element of G'.

(ii) $\phi(g^{-1}) = \phi(g)^{-1}$, for all $g \in G$.

Proof : For any $g \in G$.

$$\phi(g) * e' = \phi(g) * \phi(e)$$

$$= \phi(g * e) = \phi(e * g) = \phi(g).$$

Similarly one can prove $e' * \phi(g) = \phi(g)$.

Hence e' is the identity element of G'.

(ii) For any $g \in G$, $\phi(g) * \phi(g^{-1})$

$$= \phi(g * g^{-1}) = \phi(e) = e'.$$

Similarly one can prove $\phi(g^{-1}) * \phi(g) = e'$.

Hence $$\phi(g^{-1}) = (\phi(g))^{-1}$$

7.11.3 Definition

Let $\phi : G \to G'$ be a homomorphism of semigroups (or groups). Then ϕ is called an **isomorphism** if ϕ is one-one and onto (i.e. injective as well as surjective).

If $G' = G$, then ϕ is called an automorphism.

Examples

The homomorphism $\phi : Z \to Z$ such that $\phi(n) = -n$ is an automorphism of the group (Z, +).

(i) Define $\phi : Z \to Z_m$, where $\phi(n) = [n]$. Then ϕ is a homomorphism of groups (Z, +) and $(Z_m, +)$.

(ii) The mapping $\pi : Z \to Z\,|_{mZ}$, where $\pi(n) =$ coset $n + mZ$ is a homomorphism.

(iii) The following example plays an important role in the transmission of information in coded form, in coding theory.

Consider $\phi : Z_2 \times Z_2 \to Z_2 \times Z_2 \times Z_2$ given by $\phi(a, b) = (a, b, a + b)$.

Note that $\phi(0, 0) = (0, 0, 0)$, $\phi(1, 0) = (1, 0, 1)$, $\phi(0, 1) = (0, 1, 1)$, $\phi(1, 1) = (1, 1, 0)$. Clearly ϕ is one-one and onto. Hence ϕ is an isomorphism.

(iv) Let $Z_5^* = Z_5 - \{0\}$. Then Z_5^* is a group under multiplication.

Consider the group $(Z_4, +)$ and define a mapping $\phi : (Z_4, +) \to (Z_5^*, \times)$ as $\phi([0]) = [1]$, $\phi([1]) = [2]$, $\phi([3]) = [3]$, $\phi([2]) = [4]$.

Obviously, ϕ is one-one and onto mapping. One can also verify that ϕ is a homomorphism by the following method :

Consider the group tables of $(Z_4, +)$ and $(Z_5^*, \times)$.

$(Z_4, +)$

+	[0]	[1]	[2]	[3]
[0]	[0]	[1]	[2]	[3]
[1]	[1]	[2]	[3]	[0]
[2]	[2]	[3]	[0]	[1]
[3]	[3]	[0]	[1]	[2]

$(Z_5^*, \times)$

×	[1]	[2]	[3]	[4]
[1]	[1]	[2]	[3]	[4]
[2]	[2]	[4]	[1]	[3]
[3]	[3]	[1]	[4]	[2]
[4]	[4]	[3]	[2]	[1]

In $(Z_4, +)$ replace [0] by [1], [1] by [2], [2] by [4] and rewrite the table as

+	[1]	[2]	[4]	[3]
[1]	[1]	[2]	[4]	[3]
[2]	[2]	[4]	[3]	[1]
[4]	[4]	[3]	[1]	[2]
[3]	[3]	[1]	[2]	[4]

Then change + to × and rearrange the rows and columns, so that we obtain

×	[1]	[2]	[3]	[4]
[1]	[1]	[2]	[3]	[4]
[2]	[2]	[4]	[1]	[3]
[4]	[3]	[1]	[4]	[2]
[3]	[4]	[3]	[2]	[1]

This table is same as $(Z_5^*, \times)$. Hence it follows that $(Z_5^*, \times)$ is isomorphic to $(Z_4, +)$.

(v) Let $(A, *)$ be the semigroup whose table of operation is given below.

*	a	b	c	d
a	a	b	c	d
b	b	a	a	c
c	b	d	d	c
d	a	b	c	d

Then the function $f : A \to A$ given by

$$f(a) = d$$
$$f(b) = c$$
$$f(c) = b$$
$$f(d) = a.$$

is an automorphism of $(A, *)$. f is one-one and onto and one can verify that for any elements $x, y \in A$ $f(x * y) = f(x) * f(y)$. For example $f(a * b) = f(b) = c$ by definition of f, and $f(a) * f(b) = d * c = c$.

SOLVED EXAMPLES

1. In each of the following determine whether the set together with the binary operation is a group. If it is a group, determine if it is abelian, specify the identity and inverse of an element a.

(i) Z, where $*$ is ordinary multiplication.

(ii) Z, where $*$ is subtraction.

(iii) Q, the set of all rational numbers under the operation of addition.

(iv) Q, the set of all rational numbers under the operation of multiplication.

(v) $\mathbb{R}$, under the operation of multiplication.

Solution : (i) $(Z, *)$ is not a group since the inverses of elements of Z do not exist in Z.

(ii) $*$ is not associative, hence $(Z, *)$ is not a group.

(iii) $(Q, +)$ is an abelian group, with 0 as the identity element.

(iv) $(Q, \times)$ is not a group since the element 0 does not possess an inverse.

(v) $(\mathbb{R}, \times)$ is not a group, since the element 0 does not possess an inverse.

2. Let $A = \{a, b, c, d\}$ be a group under the operation $*$ defined in the table given below. Find the identity element of the group and find the inverse of each element in the group. Solve the equation $b * x = d$.

*	a	b	c	d
a	c	d	a	b
b	d	a	b	c
c	a	b	c	d
d	b	c	d	a

Solution : Identity element is c, since $a * c = c * a = a$, $b * c = c * b = b$, $c * c = c$, $d * c = c * d = d$.

Since $a * a = c$ a is the inverse of itself. $b * d = c = d * b$. Hence inverse of b is d, and inverse of d is b. Since $b * a = d$, $x = a$.

3. Solve the following equations in $(Z_{12}, +)$

(i) $[5] + x = [2]$, (ii) $[7] + x = [5]$.

Solution : $Z_{12} = \{[0], [1], [2], \ldots\ldots, [11]\}$ identity element is the equivalence class $[0]$.

(i) $[5] + x = [2]$

$\Rightarrow$ $[5] + x = [14]$, since for any element $[y] \in Z_{12} > [y] = [y + 12]$

$\therefore$ $x = [14] - [5] = [9]$

(ii) $[7] + x = [5]$

$\Rightarrow$ $[7] + x = [17]$

$\Rightarrow$ $x = [17 - 7] = [10]$

4. Find the order and inverse of each element in $(Z_{12}, +)$.

Solution : The following table gives the elements and their inverses.

Element	Inverse
[0]	[0]
[1]	[11]
[2]	[10]
[3]	[9]
[4]	[8]
[5]	[7]
[6]	[6]

The following table gives the elements and their orders.

Element	Order of the element
[0]	1
[1]	12
[2]	6
[3]	4
[4]	3
[5]	12
[6]	2
[7]	12
[8]	3
[9]	4
[10]	6
[11]	12

5. Let $(A, *)$ be a monoid such that for every x in A, $x * x = e$, where e is the identity element. Show that $(A, *)$ is an abelian group.

Solution : Since $x * x = e$, for all $x \in A$, every element is its own in inverse in A. Hence $(A, *)$ is a group. Let $a, b \in A$.

Consider $(a * b) * (b * a) = a * (b * b) * a = a * e * a = a * a = e$.

Similarly $(b * a) * (a * b) = e$.

Hence $b * a$ is the inverse of $a * b$. Since a group has unique inverse, it follows that

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

6. Let $(A, *)$ be a group. Show that $(A, *)$ is an abelian group if and only if $a^2 * b^2 = (a * b)^2$.

Solution : Let $(A, *)$ be an abelian group. Then $a * b = b * a$, for all $a, b \in A$.

Hence
$$\begin{aligned} a^2 * b^2 &= (a * a) * (b * b) \\ &= a * (a * b) * b && (* \text{ is associative}) \\ &= a * (b * a) * b && (* \text{ is commutative}) \\ &= (a * b) * (a * b) \\ &= (a * b)^2 \end{aligned}$$

Conversely, let $a^2 * b^2 = (a * b)^2$.

To show A is abelian we have

$$\begin{aligned} a * (a * b) * b &= (a * b) * (a * b) \\ &= a * (b * a) * b \end{aligned} \qquad \ldots (1)$$

premultiply (1) by a^{-1} and postmultiply by b^{-1}. Then

$$(a^{-1} * a) * (a * b) * (b * b^{-1})$$

$$= (a^{-1} * a) * (b * a) * (b * b^{-1})$$

$$\Rightarrow \quad e * (a * b) * e = e * (b * a) * e$$

$$\Rightarrow \quad a * b = b * a, \quad \text{for all } a, b \in A.$$

Hence $(A, *)$ is an abelian group.

7. Let G be a finite group with identity e, and let a be an arbitrary element of G. Prove that there exists a non-negative integer n such that $a^n = e$.

Solution : Let $|G| = m$, and $a \in G$. Consider $a, a^2, a^3, \ldots, a^m, a^{m+1}$. There are $m + 1$ elements. But since $|G| = m$, this means that $a^{m+1} = a^k$ $(1 \le k \le m)$.

Hence it follows that $a^{m+1-k} = e$. Putting $n = m + 1 - k$, we obtain $a^n = e$.

8. Let $(Z^+, \bullet)$ denote the group of positive integers under multiplication $\bullet$, and let $H = \{ 3^k \mid k \in Z \}$. Is H a subgroup of $(Z^+, \bullet)$?

Solution : First we have to show H is closed under $\bullet$. Let $3^{k_1}, 3^{k_2} \in H$.

Then $3^{k_1} \cdot 3^{k_2} = 3^{k_1 + k_2} \in H$. Hence H is closed under $\bullet$.

Next let $3^{k_1} \in H$. Then by definition 3^{-k_1} is also in H. Hence H is a subgroup of $(Z^+, \cdot)$.

9. Let G be an abelian group with identity e and let $H = \{ x \mid x^2 = e \}$. Show that H is a subgroup of G.

Solution : Let $x, y \in H$, then $x^2 = e$, $y^2 = e$. Consider $(xy)^2 = (xy)(yx) = x^2 y^2 = e$ using the fact that G is abelian. Hence H is closed under the group operation. By definition of H, every element x of H is its own inverse. Hence H is a subgroup.

10. Let G be a group with identity e. Show that the function $f : G \to G$ defined by $f(a) = e$, for all $a \in G$, is a homomorphism.

Solution : We have to show that for all $a, b \in G$, $f(a * b) = f(a) * f(b)$.

Now $\quad f(a * b) = e.$

Also $\quad f(a) * f(b) = e * e = e.$

Hence f is a homomorphism.

11. Let G be a group. Show that the function $f : G \to G$, defined by $f(a) = a^2$ is a homomorphism iff G is abelian.

Solution : Let G be abelian, and let $a, b \in G$.

Then $\quad f(ab) = (ab)^2 = abab$

$= aabb = a^2 b^2 = f(a) \cdot f(b).$

Hence if G is abelian, f is a homomorphism.

Conversely, let f be a homomorphism. We have to show G is abelian.

Let $a, b \in G$.

$f(ab) = f(a)\ f(b)$

$(ab)^2 = a^2 b^2$

$\Rightarrow \quad abab = aabb.$ Premultiply this equation by a^{-1} and b^{-1}.

Then $\quad a^{-1} ababb^{-1} = a^{-1} aabbb^{-1}$

$\Rightarrow \quad ebae = eabe$

$\Rightarrow \quad ba = ab,$ i.e. G is abelian.

12. Let $G = \{e, a, a^2, a^3, a^4, a^5\}$ be a group under the operation of $a^i a^j = a^r$, where $i + j = r \pmod 6$. Prove that G and Z_6 are isomorphic.

Solution : $Z_6 = \{[0], [1], [2], [3], [4], [5]\}$,

Define $f : G \to Z_6$ as follows

$e \to [0]$

$[1] \to [a]$

$[2] \to [a^2]$

$[3] \to [a^3]$

$[4] \to [a^4]$

$[5] \to [a^5]$.

$\therefore$ $f([i] + [j]) = a^r$, where $i + j = r \pmod 6$

f is clearly an isomorphism.

13. Find the subgroup of $(Z_4, +)$ generated by [2]. Subgroup generated by [3] ?

Solution : Subgroup $H_1 = \{[2], [0]\}$.

$H_2 = \{[3], [2], [1], [0]\} = Z_4$

14. Find the right cosets of $\{[0], [3], [6], [9]\}$ of $(Z_{12}, +)$.

Solution : $H = \{[0], [3], [6], [9]\}$

We obtain the following 3 distinct right cosets

$H_0 = \{[0], [3], [6], [9]\}$

$H_1 = \{[1], [4], [7], [10]\}$

$H_2 = \{[5], [8], [11], [2]\}$

14. The set $H = \{f_0, f_1, f_2\}$ is a subgroup of $(S_3, 0)$. Find the left coset of H. (Refer to article 7.6.2, Ex. vii).

Solution :

$$f_0 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \quad f_1 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix},$$

$$f_2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}, \quad g_1 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}, \quad g_2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$$

$$g_3 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$$

$$g_1 H = \{g_1, g_2, g_3\}$$

$$g_2 H = \{g_2, g_3, g_1\}$$

$$g_3 H = \{g_3, g_1, g_2\}$$

Ex. 16 : Find the subgroups of

(i) Z_8

(ii) $Z_2 \times Z_2$

Solution : (i) The group table for Z_8 under addition is given below :

+	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$	$\bar{6}$	$\bar{7}$
$\bar{0}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$	$\bar{6}$	$\bar{7}$
$\bar{1}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$	$\bar{6}$	$\bar{7}$	$\bar{0}$
$\bar{2}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$	$\bar{6}$	$\bar{7}$	$\bar{0}$	$\bar{1}$
$\bar{3}$	$\bar{3}$	$\bar{4}$	$\bar{5}$	$\bar{6}$	$\bar{7}$	$\bar{0}$	$\bar{1}$	$\bar{2}$
$\bar{4}$	$\bar{4}$	$\bar{5}$	$\bar{6}$	$\bar{7}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$
$\bar{5}$	$\bar{5}$	$\bar{6}$	$\bar{7}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$
$\bar{6}$	$\bar{6}$	$\bar{7}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$
$\bar{7}$	$\bar{7}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$	$\bar{6}$

The following are the subgroups of $(Z_8, +)$

$$H_1 = \{\bar{0}, \bar{2}, \bar{4}, \bar{6}\} \text{ and}$$

$$H_2 = \{\bar{0}, \bar{4}\}$$

H_1 and H_2 are closed under group operation. (cf. Theorem 7.7.3).

(ii) The group table for $(Z_2 \times Z_2, +)$ is given below :

+	$(\bar{0}, \bar{0})$	$(\bar{1}, \bar{0})$	$(\bar{0}, \bar{1})$	$(\bar{1}, \bar{1})$
$(\bar{0}, \bar{0})$	$(\bar{0}, \bar{0})$	$(\bar{1}, \bar{0})$	$(\bar{0}, \bar{1})$	$(\bar{1}, \bar{1})$
$(\bar{1}, \bar{0})$	$(\bar{1}, \bar{0})$	$(\bar{0}, \bar{0})$	$(\bar{1}, \bar{1})$	$(\bar{0}, \bar{1})$
$(\bar{0}, \bar{1})$	$(\bar{0}, \bar{1})$	$(\bar{1}, \bar{1})$	$(\bar{0}, \bar{0})$	$(\bar{1}, \bar{0})$
$(\bar{1}, \bar{1})$	$(\bar{1}, \bar{1})$	$(\bar{0}, \bar{1})$	$(\bar{1}, \bar{0})$	$(\bar{0}, \bar{0})$

The following are subgroups of $Z_2 \times Z_2$

$$H_1 = \{(\bar{0}, \bar{0}), (\bar{0}, \bar{1})\}$$

$$H_2 = \{(\bar{0}, \bar{0}), (\bar{1}, \bar{0})\}$$

$$H_3 = \{(\bar{0}, \bar{0}), (\bar{1}, \bar{1})\}$$

One can verify that H_1, H_2, H_3 are all closed under group operation. (cf. Theorem 7.7.3).

7.12 RINGS, INTEGRAL DOMAINS AND FIELDS

7.12.1 Rings

So for we have discussed groups which is an algebraic structure with a single binary operation. We now turn our attention to algebraic structures, with two binary operations, called **rings.** We shall denote these binary operations by + and • respectively. In analogy with numbers, + is called addition and • multiplication.

7.12.2 Definition

An algebraic structure (R, +, •) is called a ring if

(i) (R, +) is an abelian group.

(ii) Associativity of multiplication holds : $a \cdot (b \cdot c) = (a \cdot b) * c$.

(iii) The left distributive law

$a \cdot (b + c) = a \cdot b + a \cdot c$, and the right distributive law

$(b + c) \cdot a = b \cdot a + c \cdot a$ are satisfied by + and •.

7.12.3 Definition

A ring R is said to be commutative ring if $a \cdot b = b \cdot a$, for all $a, b \in R$.

7.12.4 Definition

A ring R is said to be a ring with **unit** element if there exists an element, denoted by the symbol 1 such that $a \cdot 1 = 1 \cdot a = a$, for all $a \in R$.

Examples

(i) (Z, +, •) is a ring, where Z is the set of integers, + and • are the usual addition and multiplication respectively. It is a commutative ring with unit element, the integer 1.

(ii) Z_m, the set of integers modulo m is a commutative ring with unit element (1) under addition and multiplication (modulo m).

(iii) The set of even integers including 0, under addition and multiplication is a commutative ring with no unit element.

(iv) The set of $m \times m$ matrices over the real numbers, is a non-commutative ring but with unit element (the identity matrix), under matrix addition and multiplication.