8 GROUPS

8.1. INTRODUCTION

In the present chapter, we introduce the concept of algebraic system, binary operations and groups. The study of cyclic groups, normal groups, group homomorphism etc. help us in understanding various applications of computer science. Groups play an important role in coding theory.

8.2. ALGEBRAIC STRUCTURE

If there exists a system such that it consists of a non-empty set and one or more operations on that set, then that system is called an algebraic system. It is generally denoted by (A, op_1, op_2, ..., op_n), where A is a non-empty set and op_1, op_2, ..., op_n are operations on A.

An algebraic system is also called an **algebraic structure** because the operations on the set A define a structure on the elements of A.

8.3. BINARY OPERATION

Consider a non-empty set A and a function *f* such that $f : A \times A \to A$ is called a binary operation on A. If $*$ is a binary operation on A, then it may be written as $a * b$.

A binary operation can be denoted by any of the symbols $+, -, *, \oplus, \Delta, \square, \vee, \wedge$ etc.

The value of the binary operation is denoted by placing the operator between the two operands.

e.g., (*i*) The operation of addition is a binary operation on the set of natural numbers.

(*ii*) The operation of subtraction is a binary operation on set of integers. But, the operation of subtraction is not a binary operation on the set of natural numbers because the subtraction of two natural numbers may or may not be a natural number.

(*iii*) The operation of multiplication is a binary operation on the set of natural numbers, set of integers and set of complex numbers.

(*iv*) The operation of set union is a binary operation on the set of subsets of a universal set. Similarly, the operation of set intersection is a binary operation on the set of subsets of a universal set.

8.5. PROPERTIES OF BINARY OPERATIONS

There are many properties of the binary operations which are as follows :

1. Closure Property. Consider a non-empty set A and a binary operation $*$ on A. Then A is closed under the operation $*$, if $a * b \in A$, where a and b are elements of A.

For example, the operation of addition on the set of integers is a closed operation. *i.e.,* if $a, b \in Z$, then $a + b \in Z \;\forall\; a, b \in Z$.

Example 2. *Consider the set* $A = \{-1, 0, 1\}$. *Determine whether A is closed under* (*i*) *addition* (*ii*) *multiplication.*

Sol. (*i*) The sum of the elements is $(-1) + (-1) = -2$ and $1 + 1 = 2$ does not belong to A. Hence A is not closed under addition.

(*ii*) The multiplication of every two elements of the set are

$$\begin{array}{lll} -1 * 0 = 0 ; & -1 * 1 = -1 ; & -1 * -1 = 1 \\ 0 * -1 = 0 ; & 0 * 1 = 0 ; & 0 * 0 = 0 \\ 1 * -1 = -1 ; & 1 * 0 = 0 ; & 1 * 1 = 1 \end{array}$$

Since, each multiplication belongs to A hence A is closed under multiplication.

Example 3. *Consider the set A = {1, 3, 5, 7, 9, ...}, the set of odd +ve integers. Determine whether A is closed under (i) addition (ii) multiplication.*

Sol. (*i*) The set A is not closed under addition because the addition of two odd numbers produces an even number which does not belong to A.

(*ii*) The set A is closed under the operation multiplication because the multiplication of two odd numbers produces an odd number. So, for every $a, b \in A$, we have $a * b \in A$.

2. Associative Property. Consider a non-empty set A and a binary operation * on A. Then the operation * on A is associative, if for every $a\ b, c, \in A$, we have $(a * b) * c = a * (b * c)$.

Example 4. *Consider the binary operation * on Q, the set of rational numbers, defined by*

$$a * b = a + b - ab \ \forall\ a, b \in Q.$$

*Determine whether * is associative.*

Sol. Let us assume some elements $a, b, c \in Q$, then by definition

$$(a * b) * c = (a + b - ab) * c = (a + b - ab) + c - (a + b - ab)c$$
$$= a + b - ab + c - ca - bc + abc = a + b + c - ab - ac - bc + abc.$$

Similarly, we have

$$a * (b * c) = a + b + c - ab - ac - bc + abc$$

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

Hence * is associative.

3. Commutative Property. Consider a non-empty set A and a binary operation * on A. Then the operation * on A is commutative, if for every $a, b \in A$, we have $a * b = b * a$.

Example 5. *Consider the binary operation * on Q, the set of rational numbers, defined by*

$$a * b = a^2 + b^2 \ \forall\ a, b \in Q.$$

*Determine whether * is commutative.*

Sol. Let us assume some elements $a, b \in Q$, then by definition

$$a * b = a^2 + b^2 = b^2 + a^2 = b * a$$

Hence * is commutative.

Example 6. *Consider the binary operation * and Q, the set of rational numbers defined by*

$$a * b = \frac{ab}{2} \quad \forall\ a, b \in Q.$$

*Determine whether * is (i) associative (ii) commutative.*

Sol. (*i*) Let $a, b \in Q$, then we have

$$a * b = \frac{ab}{2} = \frac{ba}{2} = b * a$$

Hence * is commutative.

(*ii*) Let $a, b, c \in Q$, then by definition we have

$$(a * b) * c = \left(\frac{ab}{2}\right) * c = \frac{\frac{ab}{2}.c}{2} = \frac{abc}{4}$$

Similarly, $$a * (b * c) = a * \left(\frac{bc}{2}\right) = \frac{\frac{abc}{2}}{2} = \frac{abc}{4}$$

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

Hence, $*$ is associative.

4. Identity. Consider a non-empty set A and a binary operation $*$ on A. Then the operation $*$ has an identity property if there exists an element, e, in A such that

$$a * e \text{ (right identity)} = e * a \text{(left identity)} = a \ \forall \ a \in \text{A}.$$

Theorem I. *Prove that $e_1' = e_1''$ where e_1' is a right identity and e_1'' is a left identity of a binary operation.*

Proof. We know that e_1'' is a right identity.

Hence, $$e_1'' * e_1' = e_1'' \qquad ...(1)$$

Also, we know that e_1'' is a left identity.

Hence, $$e_1'' * e_1' = e_1' \qquad ...(2)$$

From (1) and (2), we have $e_1' = e_1''$.

Thus, we can say that if e is a right identity of a binary operation, then e is also a left identity.

Example 7. *Consider the binary operation $*$ on I_+, the set of positive integers defined by $a * b = \dfrac{ab}{2}$. Determine the identity for the binary operation $*$, if exists.*

Sol. Let us assume that e be a +ve integer number, then

$$e * a = a, a \in \text{I}_+$$

$$\Rightarrow \qquad \frac{ea}{2} = a \quad \Rightarrow \quad e = 2 \qquad ...(1)$$

Similarly, $$a * e = a, a \in \text{I}_+$$

$$\frac{ae}{2} = a \quad \text{or} \quad e = 2 \qquad ...(2)$$

Form (1) and (2) for $e = 2$, we have $e * a = a * e = a$

Therefore, 2 is the identity element for $*$.

5. Inverse. Consider a non-empty set A and a binary operation $*$ on A. Then operation $*$ has the inverse property if for each $a \in$ A, there exists an element b in A such that

$a * b$ (right inverse) $= b * a$ (left inverse) $= e$, where b is called an inverse of a.

8.6. SEMI-GROUP *(P.T.U. B.Tech. May 2008, May 2004)*

; Let us consider, an algebraic system (A, $*$), where $*$ is a binary operation on A. Then, the system (A, $*$) is said to be a semi-group if it satisfies the following properties :

1. The operation $*$ is a closed operation on set A.
2. The operation $*$ is an associative operation.

Example 8. *Consider an algebraic system (A, $*$), where A = {1, 3, 5, 7, 9, ...}, the set of all positive odd integers and $*$ is a binary operation means multiplication. Determine whether (A, $*$) is a semi-group.*

Sol. Closure property. The operation $*$ is a closed operation because multiplication of two +ve odd integers is a +ve odd number.

Associative property. The operation $*$ is an associative operation on set A. Since for every $a, b, c \in$ A, we have

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

Hence, the algebraic system (A, $*$) is a semi-group.

Example 9. *Consider the algebraic system ({0, 1}, $*$), where $*$ is a multiplication operation. Determine whether ({0, 1}, $*$) is a semi-group.*

Sol. Closure property. The operation $*$ is a closed operation on the given set since

$$0 * 0 = 0 \,;\, 0 * 1 = 0 \,;\, 1 * 0 = 0 \,;\, 1 * 1 = 1.$$

Associative property. The operation $*$ is associative since we have

$$(a * b) * c = a * (b * c) \ \forall\ a, b, c$$

Since, the algebraic system is closed and associative. Hence, it is a semi-group.

Example 10. *Let S be a semi-group with an identity element e and if b and b′ are inverses of an element $a \in$ S, then b = b′ i.e., inverse are unique, if they exist.*

Sol. Given b is an inverse of a, therefore, we have

$$a * b = e = b * a$$

Also, b' is an inverse of a, therefore, we have

$$a * b' = e = b' * a$$

Consider $\quad b * (a * b') = b * e = b \qquad \text{...(1)}$

and $\quad (b * a) * b' = e * b' = b' \qquad \text{...(2)}$

Now, S is a semi-group, associativity holds in S *i.e.*, $b * (a * b') = (b * a) * b'$

$\Rightarrow \quad b = b'. \qquad$ | using (1) and (2)

Example 11. *Let N be the set of positive integers and let $*$ be the binary operation of least common multiple (L.C.M) on N. Find*

(*a*) *4 $*$ 6, 3 $*$ 5, 9 $*$ 18, 1 $*$ 6*

(*b*) *Is (N, $*$) a semi-group*

(*c*) *Is N commutative*

(*d*) *Find the identity element of N*

(*e*) *Which elements of N have inverses ?*

Sol. (*a*) Let $x, y \in$ N and $x * y$ = L.C.M. of x and y

$$\therefore \quad \begin{aligned} 4 * 6 &= \text{L.C.M. of } 4 \text{ and } 6 = 12 \\ 3 * 5 &= \text{L.C.M. of } 3 \text{ and } 5 = 15 \\ 9 * 18 &= \text{L.C.M. of } 9 \text{ and } 18 = 18 \\ 1 * 6 &= \text{L.C.M. of } 1 \text{ and } 6 = 6 \end{aligned}$$

(*b*) We know that the operation of L.C.M. is associative, *i.e.*,

$$a * (b * c) = (a * b) * c \quad \forall\, a, b, c \in \text{N}$$

$\therefore$ N is a semi-group under $*$.

(*c*) Also for $a, b \in$ N,

$$a * b = \text{L.C.M. of } a \text{ and } b = \text{L.C.M. of } b \text{ and } a = b * a$$

$\therefore$ N is commutative also.

(*d*) For $a \in$ N, consider $a * 1$ = L.C.M. of a and $1 = a$

Also, $1 * a$ = L.C.M. of 1 and $a = a$

$\therefore$ $a * 1 = a = 1 * a$

i.e., 1 is the identity element of N.

(*e*) Consider $a * b = 1$ *i.e.*, L.C.M. of a and b is 1, which is possible iff $a = 1$ and $b = 1$. *i.e.*, the only element which has an inverse is 1 and it is its own inverse.

Example 12. *Consider the set Q of rational numbers and let $*$ be the operation on Q defined by $a * b = a + b - ab$*

(*a*) *Find $3 * 4$, $2 * (-5)$, $7 * \frac{1}{2}$*

(*b*) *Is (Q, $*$) a semi-group?*

(*c*) *Is Q commutative?*

(*d*) *Find the identity element of Q.*

(*e*) *Which elements of Q have inverses and what are they ?*

Sol. Given $a * b = a + b - ab$ for $a, b \in$ Q

(*a*)
$$\begin{aligned} 3 * 4 &= 3 + 4 - 12 = -5 \\ 2 * (-5) &= 2 + (-5) - (-10) = 2 - 5 + 10 = 7 \\ 7 * \frac{1}{2} &= 7 + \frac{1}{2} - \frac{7}{2} = 4. \end{aligned}$$

(*b*) Q will be a semi-group if it holds associativity under $*$ for $a, b, c \in$ Q.

Consider
$$\begin{aligned} a * (b * c) &= a * (b + c - bc) \\ &= a + (b + c - bc) - a(b + c - bc) \\ &= a + b + c - bc - ab - ac + abc \qquad \text{...(1)} \end{aligned}$$

Also,
$$\begin{aligned} (a * b) * c &= (a + b - ab) * c \\ &= a + b - ab + c - (a + b - ab)\, c \\ &= a + b + c - ab - ac - bc + abc \\ &= a + b + c - bc - ab - ac + abc \qquad \text{...(2)} \end{aligned}$$

From (1) and (2),

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

Hence, (Q, $*$) is a semi-group.

(*c*) For $a, b \in Q$

Consider

$$a * b = a + b - ab = b + a - ba = b * a$$

$\therefore$ Q is commutative.

(*d*) Let e is the identity element of Q, therefore, for $a \in$ Q, we have

$$a * e = a$$

$\Rightarrow$ $a + e - ae = a$

$\Rightarrow$ $e - ea = 0$

$\Rightarrow$ $e(1 - a) = 0$

$\Rightarrow$ $e = 0, 1$ if $a \neq 1$

$\therefore$ The identity of Q is 0.

(*e*) If x is the inverse of $a \in$ Q, then $a * x = 0$ (identity)

$\Rightarrow$ $a + x - ax = 0$

$\Rightarrow$ $a + x(1 - a) = 0$

$\Rightarrow$ $a = x(a - 1)$

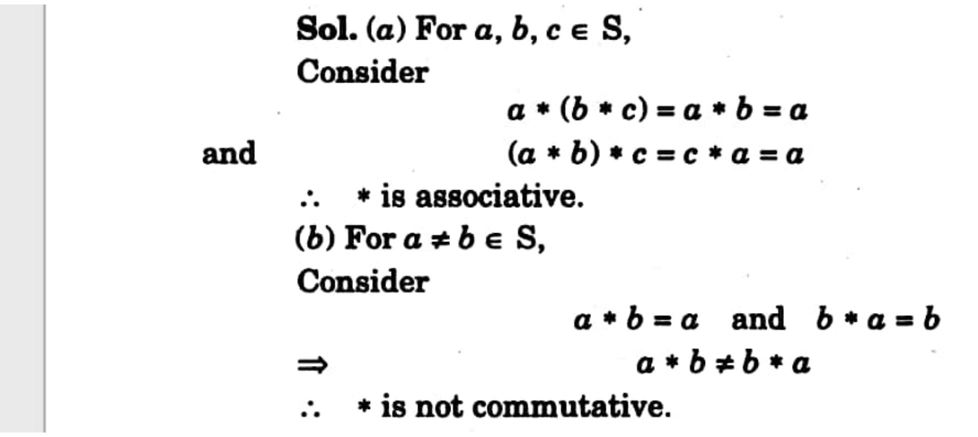
$\Rightarrow$ $x = \dfrac{a}{a-1}, a \neq 1$

Thus a has an inverse $\dfrac{a}{a-1}$.

Example 13. *Consider a non-empty set S with the operation* $a * b = a$

(*a*) *Is the operation associative ?*

(*b*) *Is the operation commutative ?*



Sol. (*a*) For $a, b, c \in S$,

Consider

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

and

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

$\therefore$ * is associative.

(*b*) For $a \neq b \in S$,

Consider

$$a * b = a \quad \text{and} \quad b * a = b$$

$$\Rightarrow \quad a * b \neq b * a$$

$\therefore$ * is not commutative.

8.10. MONOID

(P.T.U. B.Tech., May 2008 Dec. 2004)

Let us consider an algebraic system (A, *o*), where *o* is a binary operation on A. Then the system (A, *o*) is said to be a monoid if it satisfies the following properties.

(*i*) The operation *o* is a closed operation on set A.

(*ii*) The operation *o* is an associative operation.

(*iii*) There exists an identity element w.r.t. the operation *o*.

Example 21. *Consider an algebraic system (I, +), where the set I = {0, 1, 2, 3, 4, ...} the set of natural numbers and + is an addition operation. Determine whether (I, +) is a monoid.*

Sol. Closure property. The operation + is closed since sum of two natural numbers is a natural number.

Associative property. The operation + is an associative property since we have

$$(a + b) + c = a + (b + c) \ \forall \ a, b, c \in \text{I}.$$

Identity. There exists an identity element in set I w.r.t. the operation +. The element 0 is an identity element w.r.t. the operation +. Since, the operation + is a closed, associative and there exists an identity. Hence, the algebraic system (I, +) is a monoid.

TEST YOUR KNOWLEDGE 8.1

1. Let * be the operation on the set R of real numbers defined by $a * b = a + b + 2ab$

   (*a*) Find $2 * 3$, $3 * (-5)$, $7 * (1/2)$

   (*b*) Is (R, *) a semi-group ? Is it commutative ?

   (*c*) Find the identity element

   (*d*) Which elements have inverses and what are they ?

2. Let S be a semi-group with identity e and let b and b' be inverses of a. Show that $b = b'$ *i.e.*, inverses are uniques, if they exist. *(P.T.U.B.Tech. Dec. 2003)*

3. Prove that for any commutative monoid (M ; *), the set of idempotent elements of M form a submonoid. *(P.T.U. B.Tech. Dec. 2004)*

4. If a, b are elements of a monoid M and $a * b = b * a$. Show that

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

5. Let S = Q × Q, the set of ordered pairs of rational numbers, with the operation * defined by

$$(a, b) * (x, y) = (ax, ay + b)$$

   (*a*) Find $(3, 4) * (1, 2)$ and $(-1, 3) * (5, 2)$

   (*b*) Is S a semi-group ? Is it commutative ?

   (*c*) Find the identity element of S

   (*d*) Which elements, if any, have inverses and what are they ?

6. Let S = N × N, the set of ordered pairs of positive integers with the operation * defined by

   $(a, b) * (c, d) = (ad + bc, bd)$

   (*a*) Find $(3, 4) * (1, 5)$ and $(2, 1) * (4, 7)$

   (*b*) Is S a semi-group ? Is S commutative ?

7. Let A be a non-empty set with the operation * defined by $a * b = a$ and assume A has more than one element. Then

   (*a*) Is A a semi-groups ?

   (*b*) Is A commutative ?

   (*c*) Does A have an identity element ?

   (*d*) Which elements, if any have inverses and what are they ?

Answers

1. (*a*) $17, -32, \frac{29}{2}$ (*b*) Yes, Yes

   (*c*) zero (*d*) If $a \neq \frac{1}{2}$, then a has an inverse which is $\frac{-a}{(1+2a)}$.

5. (*a*) (3, 10), (– 5, 1) (*b*) Yes, No (*c*) (1, 0)

   (*d*) The element (a, b) has an inverse if $a \neq 0$ and its inverse is $\left(\frac{1}{a}, -\frac{b}{a}\right)$

6. (*a*) (19, 20), (18, 7) (*b*) Yes, Yes

7. (*a*) Yes (*b*) No (*c*) No (*d*) It is meaningless to talk about inverses when no identity element exists.

8.12. GROUP

(*P.T.U. B.Tech. May 2008, 2006 ; Dec. 2004 ; May 2004 ; Dec. 2001*)

Let us consider an algebraic system (G, $*$), where $*$ is a binary operation on G. Then the system (G, $*$) is said to be a group if it satisfies following properties.

(*i*) The operation $*$ is a closed operation.

(*ii*) The operation $*$ is an associative operation.

(*iii*) There exists an identity element w.r.t. the operation $*$.

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

For example, the algebraic system (I, +), where I is the set of all integers and + is an addition operation, is a group. The element 0 is the identity element w.r.t. the operation +. The inverse of every element $a \in$ I is $-a \in$ I.

Example 1. *Determine whether the algebraic system (Q, +) is a group where Q is the set of all rational numbers and + is an addition operation.*

Sol. Closure Property. The set Q is closed under operation +, since the addition of two rational numbers is a rational number.

Associative Property. The operation + is associative, since $(a + b) + c = a + (b + c) \; \forall \; a, b, c \in$ Q.

Identity. The element 0 is the identity element. Hence $a + 0 = 0 + a = a \; \forall \; a \in$ Q.

Inverse. The inverse of every element $a \in$ Q is $-a \in$ Q. Hence the inverse of every element exists.

Since, the algebraic system (Q, +) satisfies all the properties of a group, hence (Q, +) is a group.

Example 2. *Which of the following are groups under addition N, Z, Q, R, C ?*

Sol. The set of integers Z, the set of rationals Q, the set of reals R, the set of complex numbers C, are all groups under addition. (Prove yourself as in Example-1)

But N, the set of natural numbers donot form a group under addition. Since, N does not have additive identity. ($0 \notin$ N).

Example 3. *Let S be the set of $n \times n$ with rational entries under the operation of matrix multiplication. Is S a group ?*

Sol. We know that matrix multiplication is associative. But inverse does not always exist. As we know that if | A | $\neq 0$, then A^{-1} exists.

Example 4. *Prove that G = {1, 2, 3, 4, 5, 6} is a finite abelian group of order 6 under multiplication modulo 7.* (P.T.U. B.Tech. May 2009)

Sol. G = {1, 2, 3, 4, 5, 6, $\times_7$}

Consider the multiplication modulo 7 table as shown below. Recall that $a \times_7 b$ = The remainder when ab is divided by 7

$\times_7$	1	2	3	4	5	6
1	1	2	3	4	5	6
2	2	4	6	1	3	5
3	3	6	2	5	1	4
4	4	1	5	2.	6	3
5	5	3	1	6	4	2
6	6	5	4	3	2	1

From the table, we observe that each element inside the table is also an element of G. It means that G is closed under multiplication modulo 7.

Also for each $a, b, c \in$ G

$$a \times_7 (b \times_7 c) = (a \times_7 b) \times_7 c \quad \text{i.e., associative law hold.}$$

From the table, we observe that the first row inside the table is identical with the top-row of the table. Therefore, 1 is the identity (multiplicative) of G.

Also, $2 \times_7 4 = 1$; $3 \times_7 5 = 1$, $4 \times_7 2 = 1$, $5 \times_7 3 = 1, 6 \times_7 6 = 1$

Hence, each element G has an inverse, *i.e.*,

Inverse of 2 is 4 and of 4 is 2

Inverse of 3 is 5 and of 5 is 3

Inverse of 6 is 6

Hence, G is a group under the multiplication modulo 7.

Example 5. *Consider an algebraic system* (Q, *),*where Q is the set of rational numbers and * is a binary operation defined by*

$$a * b = a + b - ab \ \forall \ a, b \in Q.$$

Determine whether (Q, *) *is a group.*

Sol. Closure property. Since the element $a * b \in$ Q for every $a, b \in$ Q, hence, the set Q is closed under the operation *.

Associative property. Let us assume $a, b, c \in$ Q, then we have

$$\begin{aligned}(a * b) * c &= (a + b - ab) * c \\ &= (a + b - ab) + c - (a + b - ab)c \\ &= a + b - ab + c - ac - bc + abc \\ &= a + b + c - ab - ac - bc + abc\end{aligned}$$

Similarly, $a * (b * c) = a + b + c - ab - ac - bc + abc.$

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

∴ * is associative.

Identity. Let e is an identity element. Then we have $a * e = a \ \forall \ a \in$ Q

∴ $a + e - ae = a$ or $e - ae = 0$

or $e(1 - a) = 0$ or $e = 0$, if $1 - a \neq 0$

Similarly, for $e * a = a \ \forall \ a \in$ Q, we have $e = 0$

Therefore, for $e = 0$, we have $a * e = e * a = a$

Thus, 0 is the identity element.

Inverse. Let us assume an element $a \in$ Q. Let a^{-1} is an inverse of a. Then we have

$a * a^{-1} = 0$ **[Identity]**

∴ $a + a^{-1} - aa^{-1} = 0$

or $a^{-1}(1 - a) = -a$ or $a^{-1} = \frac{a}{a-1}, a \neq 1$

Now, $\frac{a}{a-1} \in$ Q, if $a \neq 1$

Therefore, every element has inverse such that $a \neq 1$.

Since, the algebraic system (Q, *) satisfy all the properties of a group. Hence, (Q, *) is a group.

8.13. Z_m THE INTEGERS MODULO *m*

The integers modulo m, denoted by Z_m, is the set given by

$Z_m = \{0, 1, 2, \ldots m - 1; +_m, \times_m\}$ where the operations $+_m$ (read as addition modulo m) and $\times_m$ (read as multiplication modulo m) are defined as

$$a +_m b = \text{remainder after } a + b \text{ is divided by } m$$
$$a \times_m b = \text{remainder after } a \times b \text{ is divided by } m.$$

Theroem X. *For each $n \geq 1$, $[Z_m; +_m]$ is a group.*

Proof. By definition, If $a, b \in Z_m$, then $a +_m b$ is remainder after $a + b$ is divided by m, which is again an element of Z_m. Hence Z_m is closed under $+_m$. Also the addition modulo m is always associative. 0 is the identity element for $+_m$ and every element of Z_m has an additive inverse. $\therefore$ Z_m is a group under addition modulo m.

8.14. FINITE AND INFINITE GROUP

A group (G, $*$) is called a finite group if G is a finite set.

A group (G, $*$) is called an infinite group if G is an infinite set.

For Example

1. The group (I, +) is an infinite group as the set I of integers is an infinite set.

2. The group G = {1, 2, 3, 4, 5, 6, 7} under multiplication modulo 8 is a finite group as the set G is a finite set.

8.15. ORDER OF GROUP

The order of the group G is the number of elements in the group G. It is denoted by $|G|$. A group of order 1 has only the identity element *i.e.*, ({e}).

A group of order 2 has two elements *i.e.*, one identity element and one some other element.

Example 6. *Let ({e, x}, $*$) be a group of order 2. The table of operation is shown in (Fig. 8.3).*

$*$	e	x
e	e	x
x	x	e

Fig. 8.3

The group of order 3 has three elements *i.e.*, one identity element and two other elements.

8.16. SUBGROUP

(*P.T.U. B.Tech. May 2007, May 2006*)

Let us consider a group (G, $*$). Also, let $S \subseteq G$; then (S, $*$) is called a subgroup iff it satisfies following conditions :

(*i*) The operation $*$ is closed operation on S.

(*ii*) The operation $*$ is an associative operation.

(*iii*) As e is an identity element belonged to G. It must belong to the set S *i.e.*, The identity element of (G, $*$) must belongs to (S, $*$).

(*iv*) For every element $a \in S$, a^{-1} also belongs to S.

For example, let (G, +) be a group, where G is a set of all integers and (+) is an addition operation. Then (H, +) is a subgroup of the group G, where $H = \{2m : m \in G\}$, the set of all even integer.

For example, let G be a group. Then the two subgroups of G are G and $G_1 = \{e\}$, e is the indentity element.

Example 9. *Let* (*I*, +) *be a group, where I is the set of all integers and* (+) *is an addition operation. Determine whether the following subsets of G are subgroups of G.*

(*a*) *The set* (G_1, +) *of all odd integers.* (*b*) *The set* (G_2, +) *of all positive integers.*

Sol. (*a*) The set G_1 of all odd integers is not a subgroup of G. It does not satisfy the closure property, since addition of two odd integers is always even.

(*b*) **Closure property.** The set G_2 is closed under the operation +, since addition of two even integers is always even.

Associative property. The operation + is associative since $(a + b) + c = a + (b + c)$ for every $a, b, c \in G_2$.

Identity. The element 0 is the identity element. Hence, $0 \in G_2$.

Inverse. The inverse of every element $a \in G_2$ is $-a \notin G_2$. Hence, the inverse of every element does not exists.

Since the system (G_2, +) does not satisfy all the conditions of a subgroup. Hence, (G_2, +) is not a subgroup of (I, +).

Example 10. *Consider the group Z of integers under addition. Let H be the subset of Z consisting of all multiples of a positive integer m i.e.*,

$$H = \{......, -3m, -2m, -m, 0, m, 2m, 3m, ...\}$$

Show that H is a subgroup of Z.

Sol. For $r, s \in Z$, $rm, sm \in$ H.

Consider $\quad rm + sm = (r + s)\,m \in$ H

i.e., H is closed under addition.

For $rm \in$ H, $-rm \in$ H and consider $rm + (-rm) = (r - r)\,m = 0 \in$ H

i.e., 0 is the identity of H and $-rm$ is the inverse of rm.

Hence, H is a subgroup of Z.

8.17. ABELIAN GROUP

(P.T.U. B.Tech. May 2002)

Let us consider, an algebraic system (G, $*$), where $*$ is a binary operation on G. Then the system (G, $*$)is said to be an abelian group if it satisfies all the properties of the group plus an additional following property :

(*i*) The operation $*$ is commutative *i.e.*,

$$a * b = b * a \ \forall \ a, b \in G$$

For example, consider an algebraic system (I, +), where I is the set of all integers and + is an addition operation. The system (I, +) is an abelian group because it satisfies all the properties of a group. Also the operation + is commutative for every a, $b \in$ I.

ILLUSTRATIVE EXAMPLES

Example 1. *Consider an algebraic system (G, $*$), where G is the set of all non-zero real numbers and $*$ is a binary operation defined by $a * b = \frac{ab}{4}$. Show that (G, $*$) is an abelian group.*

Sol. Closure property. The set G is closed under the operation $*$. Since, $a * b = \frac{ab}{2}$ is a real number. Hence, belongs to G.

Associative property. The operation $*$ is associative. Let a, b, $c \in$ G, then we have

$$(a * b) * c = \left(\frac{ab}{4}\right) * c = \frac{(ab)c}{16} = \frac{abc}{16}.$$

Similarly, $$a * (b * c) = a * \left(\frac{bc}{4}\right) = \frac{a(bc)}{16} = \frac{abc}{16}.$$

Identity. To find the identity element, let us assume that e is a positive real number. Then for $a \in G$,

$$e * a = a \quad \Rightarrow \quad \frac{ea}{4} = a \quad \text{or} \quad e = 4$$

Similarly, $$a * e = a$$

$$\Rightarrow \quad \frac{ae}{4} = a \quad \text{or} \quad e = 4.$$

Thus, the identity an element in G is 4.

Inverse. Let us assume that $a \in$ G. If $a^{-1} \in$ Q is an inverse of a, then $a * a^{-1} = 4$

$$\Rightarrow \quad \frac{aa^{-1}}{4} = 4 \quad \text{or} \quad a^{-1} = \frac{16}{a}$$

Similarly, $$a^{-1} * a = 4 \text{ gives}$$

$$\Rightarrow \quad \frac{a^{-1}a}{4} = 4 \quad \text{or} \quad a^{-1} = \frac{16}{a}.$$

Thus, the inverse of an element a in G is $\frac{16}{a}$.

Commutative. The operation $*$ on G is commutative.

Commutative. The operation $*$ on G is commutative.

Since, $$a * b = \frac{ab}{4} = \frac{ba}{4} = b * a.$$

Thus, the algebraic system (G, $*$) is closed, associative, has identity element, has inverse and commutative. Hence, the system (G, $*$) is an abelian group.

Example 2. *Let* (**Z**, $*$) *be an algebraic structure, where Z is the set of integers and the operation $*$ is defined by $n * m$ = maximum (n, m). Determine whether* (**Z**, $*$) *is a monoid or a group or an abelian group.*

Sol. Closure Property

We know that $n * m = \max. (n,m) \in \mathbf{Z} \quad \forall\, n, m \in \mathbf{Z}$

Hence $*$ is closed.

Associative property. Let us assume $a, b, c \in \mathbf{Z}$.

Then, we have $a * (b * c) = a * \max. (b, c) = \max. (a, \max. (b, c)) = \max. (a, b, c)$

Similarly, $(a * b) * c = \max. (a, b, c)$

Hence $*$ is associative.

Identity. Let e be the identity element. Then $\max. (a, e) = a$

Hence, the minimum element is the identity element.

Inverse. The inverse of any element does not exist. Since, the inverse does not exist, hence (**Z**, $*$) is not a group or abelian group but a monoid as it satisfies the properties of closure, associative and identity.

Example 3. *Let S = {0, 1, 2, 3, 4, 5, 6, 7} and multiplication modulo 8, that is*

$$x \otimes y = (xy) \text{ Mod } 8$$

(*i*) *Prove that* ({0, 1}, ⊗) *is not a group.*

(*ii*) *Write three distinct groups* (G, ⊗) *where* $G \subset S$ *and G has 2 elements.*

Sol. (*i*) (*a*) **Closure property.** The set {0, 1} is closed under the operation ⊗, as shown in table of operation (Fig. 8.6).

⊗	0	1
0	0	0
1	0	1

Fig. 8.6

(*b*) **Associative property.** The operation ⊗ is associative. Let $a, b, c \in$ G, then we have

$$(a \otimes b) \otimes c = a \otimes (b \otimes c) \quad e.g., \ (0 \otimes 1) \otimes 1 = (0) \otimes 1 = 0$$

Similarly, $0 \otimes (1 \otimes 1) = 0 \otimes (1) = 0.$

(*c*) **Identity.** The element 1 is the identity element as for every $a \in \{0, 1\}$: We have

$$1 \otimes a = a = a \otimes 1.$$

(*d*) **Inverse.** There must exist an inverse of every element $a \in \{0, 1\}$, such that

$$a \otimes a^{-1} = 1$$

Example 6. *Let G be a group of 2 × 2 matrices with rational entries and non-zero determinant. Let H be a subset of G consisting of matrices whose upper right entry is zero. Then show that H is a subgroup of G.*

Sol. Given
$$G = \left[\begin{pmatrix} a & b \\ c & d \end{pmatrix} : a, b, c, d \in Q \text{ and } ad - bc \neq 0\right]$$

$$H = \left[\begin{pmatrix} a & 0 \\ c & d \end{pmatrix} : a, c, d \in Q\right]$$

H is a subgroup of G iff

(*i*) H is closed under multiplication

(*ii*) For $A \in H$, $A^{-1} \in H$

Let $A, B \in H$ where $A = \begin{pmatrix} a_1 & 0 \\ c_1 & d_1 \end{pmatrix}$, $B = \begin{pmatrix} a_2 & 0 \\ c_2 & d_2 \end{pmatrix}$

Consider
$$AB = \begin{pmatrix} a_1 & 0 \\ c_1 & d_1 \end{pmatrix}\begin{pmatrix} a_2 & 0 \\ c_2 & d_2 \end{pmatrix} = \begin{pmatrix} a_1a_2 & 0 \\ c_1a_2 + d_1c_2 & d_1d_2 \end{pmatrix} \in H$$

i.e., H is closed under multiplication.

Further, For $A \in H$, we have

$$A = \begin{pmatrix} a & 0 \\ c & d \end{pmatrix}, \; |A| = \begin{vmatrix} a & 0 \\ c & d \end{vmatrix} = ad$$

Also
$$A_{11} = d, A_{12} = -c, A_{21} = 0, A_{22} = a$$

$\therefore$
$$\text{adj } A = \begin{pmatrix} A_{11} & A_{12} \\ A_{21} & A_{22} \end{pmatrix}^T = \begin{pmatrix} d & 0 \\ -c & a \end{pmatrix}$$

$\therefore$
$$A^{-1} = \frac{adjA}{|A|} = \begin{pmatrix} \frac{d}{ad} & 0 \\ -\frac{c}{ad} & \frac{1}{d} \end{pmatrix} \in H$$

Hence H is a subgroup of G.

Example 7. *Let G is a group of real numbers under multiplication. Let H = {– 1, 1}. Then show that H is a subgroup of G under multiplication.*

Sol. Consider the multiplication table of H under multiplication.

•	– 1	1
– 1	1	– 1
1	– 1	1

From the table, we observe that each element in the table belongs to H.

Hence H is closed under multiplication.

Also, the inverse of -1 is -1 and of 1 is 1. Thus each element of H has its inverse. Therefore H is a subgroup of G under multiplication.

Example 8. *Consider the group of integers Z under +. Let E = The set of even integers. Then show that E is a subgroup of Z under +.*

Sol. Given $E = \{2m : m \in Z\}$ *i.e.*, the set of even integers. Clearly E is a subset of Z.

Let $\quad a, b \in E \Rightarrow a = 2m, m \in Z$

$$b = 2n, n \in Z$$

$\therefore \quad a + b = 2m + 2n = 2(m + n) \in E \qquad | \; m, n \in Z \Rightarrow m + n \in Z$

i.e., E is closed under +. Also for each $a \in E$, we have $a = 2m, m \in Z$

$\Rightarrow \quad -a = -2m = 2(-m) = 2t, \; t = -m \in Z$

$\Rightarrow \quad -a \in E$

Thus each element belonging to E has additive inverse.

$\therefore$ E is a subgroup of Z under +.

Example 9. *Let Z be a group of integers under +. Let Z^+ is the set of non-negative integers. Is Z^+ a subgroup of Z ?*

Sol. $\quad Z^+ = \{0, 1, 2, 3, ...\}$

Clearly Z^+ is a subset of Z. But Z^+ is not a subgroup of Z. Since the elements of Z^+ do not have additive inverses. For *e.g.*, $2 \in Z^+$, but $-2 \notin Z^+$.

Example 10. *Consider $Z_{12} = [0, 1, 2, ... 11]$, the group under addition modulo 12. Let $H = [0, 3, 6, 9]$. Show that H is a subgroup of Z_{12} under $+_{12}$.*

Sol. Given H = [0, 3, 6, 9]. Clearly H is a subset of Z_{12}.

Let $a, b \in H \Rightarrow a +_{12} b$ is also in H. $\therefore$ H is closed under $+_{12}$. Also we have

$3 +_{12} 9 = 0$, 0 is the identity of Z_{12}

$6 +_{12} 6 = 0$

$9 +_{12} 3 = 0$

$\therefore$ each element of H has its inverse.

$\therefore$ H is a subgroup of Z_{12} under addition modulo 12.

Example 11. *Consider the group of integers Z under +. Let 2Z and 3Z are two subgroups of [Z; +]. Is $2Z \cap 3Z$ a subgroup of Z ?*

Sol. We know that if H and K are two subgroups of a group G. Then $H \cap K$ is also a subgroup of G. Using this result, we can say that $2Z \cap 3Z$ is a subgroup of Z. (Theorem XII)

Example 12. Consider Z_{15}, the group under addition modulo 15. Let H_1 = [0, 5, 10], H_2 = [0, 4, 8, 12]. Are H_1 and H_2 subgroups of Z_{15} under $+_{15}$?

Sol. To check whether H_1 is a subgroup of Z_{15}, compute the following table.

$+_{15}$	0	5	10
0	0	5	10
5	5	10	0
10	10	0	5

From the table, we observe that each element which is in the interior of the addition table is also in H_1. ∴ H_1 is closed under $+_{15}$. Also we have $5 +_{15} 10 = 0$, $10 +_{15} 5 = 0$, 0 is the identity ∴ each element of H, has its inverse. ∴ H_1 is a subgroup of Z_{15}.

To check, whether H_2 is a subgroup of Z_{15}, compute the following table.

$+_{15}$	0	4	8	12
0	0	4	8	12
4	4	8	12	1
8	8	12	1	5
12	12	1	5	9

From the table, we observe that there are some elcments in the interior of the addition table, which are not in H_2 (*e.g.*, $9 \notin H_2$). Hence H_2 is not closed under $+_{15}$. ∴ H_2 is not a subgroup of Z_{15}.

TEST YOUR KNOWLEDGE 8.2

1. If a, b, c are elements of a group G and $a * b = c * a$. Then $b = c$? Explain your answer.
(*P.T.U. B.Tech, Dec. 2006, May 2005*)

2. Discuss the relation between groups and monoids ? Is every monoid a group ? Is every group a monoid ?

3. Which of the following are groups ?

   (*i*) $M_{2\times3}(R)$ with matrix addition

   (*ii*) $M_{2\times2}(R)$ with matrix multiplication

   (*iii*) The positive real numbers with multiplication

   (*iv*) The non-zero real numbers with multiplication

   (*v*) The set [– 1, 1] with multiplication.

4. Give an example of (*i*) a finite abelian group (*ii*) an infinite non-abelian group.

5. Let V = {e, a, b, c}. Let * be defined by $x * x = e$ for all $x \in$ V. Write a complete table for * so that (V, *) is a group.

6. Which of the following subsets of the real numbers is a subgroup of [R, +] ?

   (*a*) The rational numbers
   (*b*) The positive real numbers

   (*c*) $H = \left\{\frac{K}{2} : \text{K is an integer}\right\}$
   (*d*) H = {2^K : K is an integer}

   (*e*) H = {$x : -100 \le x \le 100$}

Answers

2. No, Yes (Every group is a monoid)

3. (i), (iii), (iv), (v) are groups

4. (i) G = $\{e, a, b, c\}$ is a finite abolian group under * defined by the following Table:

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

(ii) $M_{2\times 2}(R)$, the set of all 2 × 2 matrices $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$; $ad - bc \neq 0$ is an infinite non-abelian group w.r.t. the matrix multiplication.

5. See Q. 4 (i)

6. (a) and (c)

11. $\{e\}$ and G itself.

8.18. (a) COSETS *(P.T.U. B.Tech. Dec. 2006 ; May 2004 ; Dec. 2003 ; May 2002)*

Consider an algebraic system (G, $*$), where $*$ is a binary operation. Now, if (G, $*$) is a group and let a be an element of G and H $\subseteq$ G, then

The **left coset** $a * H$ of H is the set of elements such that

$$a * H = \{a * h : h \in H\}.$$

The **right coset** $H * a$ of H is the set of elements such that

$$H * a = \{h * a : h \in H\}.$$

The subset H is itself a left and right coset since $e * H = H * e = H$.

8.18. (b) COSET REPRESENTATIVE SYSTEM FOR H IN G

A subset C of G is said to be a *coset representative system of H* if C contains exactly one element from each coset. Such an element is called a representative of the coset. The number of coset representatives is equal to [G : H], the index of H in G.

Example. *Let H be a subgroup of a finite group G. How many coset representative systems exist for the cosets of H ?*

Sol. There are $n(H)$ ways of choosing an element from any coset and there are [G : H] distinct cosets. Hence, the desired number is $H^{[G : H]}$.

ILLUSTRATIVE EXAMPLES

Example 1. *Let us consider a group (G, *), where G is a set having elements {0, 1} and * is a binary operation. Also, let H = {1} is a subgroup of G. Determine all the left cosets of H in G.*

Sol. There are only 2 left cosets *i.e.,*

$$1 * H = H = \{1\}$$

$$0 * H = \{0\}.$$

Example 2. *Let (I, +) is a group, where I is the set of all integers and + is an addition operation and let H = {..., – 4, – 2, 0, 2, 4, 6, 8, ...} be the subgroup consisting of multiples of 2. Determine all the left cosets of H in I.*

Sol. There are two distinct left cosets of H in I.

$$0 + H = \{ ..., -6, -4, -2, 0, 2, 4, 6, ...\} = H$$

$$1 + H = \{... -5, -3, -1, 1, 3, 5, 7, ...\}$$

$$2 + H = \{... -4, -2, 0, 2, 4, ...\} = H$$

$$3 + H = \{..., -5, -3, -1, 1, 3, 5, ...\} = 1 + H$$

so on.

There is no other distinct left coset because any other left coset coincides with the cosets given above.

Example 3. *Let G = (I, +) be a group, where I is the set of integers and + is an addition operation, also let G_1 = {......– 14, – 7, 0, 7, 14, 21, ...} be a subgroup consisting of the multiples of 7. Determine the cosets of G_1 in I.*

Sol. The set I has 7 different cosets (left or right) of G_1, which are as shown below.

$$0 + H = \{...... -14, -7, 0, 7, 14, 21, ...\}$$

$$1 + H = \{...... -13, -6, 1, 8, 15, 22, ...\}$$

$$2 + H = \{...... -12, -5, 2, 9, 16, 23, ...\}$$

$$3 + H = \{...... -11, -4, 3, 10, 17, 24, ...\}$$

$$4 + H = \{...... -10, -3, 4, 11, 18, 25, ...\}$$

$$5 + H = \{...... -9, -2, 5, 12, 19, 26, ...\}$$

Lagrange's Theorem *(P.T.U.B.Tech. Dec. 2007, 2006, May 2006, Dec. 2003)*

Theorem III. *If G is a finite group and H is a subgroup of G, then o(H)* $|$ *o*(G).

Proof. Since H is a subgroup of a finite group G, $\therefore$ H is also finite, say,

$$H = \{h_1, h_2, \dots h_n\}, \text{ where each } h_i \text{ is distinct.}$$

Consider Ha = $\{h_1a, h_2a, \dots h_na\}$. We claim all h_ia's are distinct. For if,

$$h_ia = h_ja$$

$\Rightarrow$ $h_i = h_j$ | Right cancellation law

a contradiction, since h_i's are distinct. Hence Ha has distinct elements.

Now G is finite $\therefore$ The number of distinct right cosets of H in G is also finite, say, k.

Let $G = Ha_1 \cup Ha_2 \cup \dots \cup Ha_k = \bigcup_{i=1}^{k} Ha_i$

$\Rightarrow$ $o(G)$ = Number of elements in Ha_1 + number of elements in Ha_2 + ... + number of elements in Ha_K

$= n + n + \dots k$ Times $= nk$

$\Rightarrow$ $n \mid o(G)$

$\Rightarrow$ $o(H) \mid o(G)$

Hence the Theorem.

8.19. INDEX OF A SUBGROUP

Let G be a group and H be a subgroup of G. Then the number of right (left) cosets of H in G is called the index of H in G. The index of H in G is denoted by [G : H].

Theorem IV. *If G is a finite group and H is a subgroup of G. Then* $[G: H] = \dfrac{o(G)}{o(H)}$.

Proof. Proceeding in the same way as in the proof of Lagrange's theorem, we have

$o(G) = nk$, where k is the number of distinct right cosets of H in G

$\Rightarrow$ $k = \dfrac{o(G)}{n} = \dfrac{o(G)}{o(H)}$

$\Rightarrow$ $[G: H] = \dfrac{o(G)}{o(H)}$.

8.20. NORMAL SUBGROUP *(P.T.U. B. Tech. Dec. 2007, 2002, May 2002, Dec. 2001)*

A subgroup H of a group G is called normal subgroup of G if for every $g \in$ G, $h \in$ H, $\Rightarrow$ $ghg^{-1} \in$ H.

or

A subgroup H of a group G is called a normal subgroup of G iff for $g \in$ G, we have

$$gHg^{-1} = H \ \forall \ g \in G$$

Example 4. *Let G be the group of two by two invertible matrices* $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$*; ad – bc ≠ 0. Let* $H = \left[\begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix} : a \neq 0\right]$. *Then H is a normal subgroup of G.*

Sol. We first show that H is a subgroup of G.

Let $h_1, h_2 \in$ H such that

$$h_1 = \begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix}, h_2 = \begin{pmatrix} a_1 & 0 \\ 0 & a_1 \end{pmatrix}; a \neq 0, a_1 \neq 0$$

Now $$h_1 h_2 = \begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix}\begin{pmatrix} a_1 & 0 \\ 0 & a_1 \end{pmatrix} = \begin{pmatrix} aa_1 & 0 \\ 0 & aa_1 \end{pmatrix} \in H \qquad | \ aa_1 \neq 0$$

i.e., H is closed under matrix multiplication. Further, For A $\in$ H,we have

$$A = \begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix}, \ | A | = \begin{vmatrix} a & 0 \\ 0 & a \end{vmatrix} = a^2$$

Also $$A_{11} = a, A_{12} = 0, A_{21} = 0, A_{22} = a$$

$\therefore$ $$\text{adj } A = \begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix}^T = \begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix}$$

Hence $$A^{-1} = \frac{\text{adj}A}{|A|} = \frac{1}{a^2}\begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix} = \begin{pmatrix} \frac{1}{a} & 0 \\ 0 & \frac{1}{a} \end{pmatrix} \in H, a \neq 0$$

Thus each element belonging to H has multiplicative inverse. Hence H is a subgroup of G.

Further, For $g = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in$ G, $h = \begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix} \in$ H, Consider

$$ghg^{-1} = \begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix}\begin{pmatrix} a & b \\ c & d \end{pmatrix}^{-1} = \begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix}\begin{pmatrix} \frac{d}{ad-bc} & \frac{-b}{ad-bc} \\ \frac{-c}{ad-bc} & \frac{a}{ad-bc} \end{pmatrix}$$

$$= \begin{pmatrix} a^2 & ba \\ ca & da \end{pmatrix}\begin{pmatrix} \frac{d}{ad-bc} & \frac{-b}{ab-bc} \\ \frac{-c}{ad-bc} & \frac{a}{ad-bc} \end{pmatrix} = \begin{pmatrix} \frac{a^2d-bac}{ad-bc} & \frac{-a^2b+ba^2}{ad-bc} \\ \frac{cad-dac}{ad-bc} & \frac{-cab+da^2}{ad-bc} \end{pmatrix}$$

$$= \begin{pmatrix} \frac{a\,(ad-bc)}{ad-bc} & 0 \\ 0 & \frac{a\,(ad-bc)}{ad-bc} \end{pmatrix} = \begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix} \in H$$

Hence H is a normal subgroup of G under matrix multiplication.

Example 5. *Let G be a group of two by two invertible matrices* $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$*; $ad - bc \neq 0$ under matrix multiplication. Let* $H = \left[\begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix} : ab \neq 0\right]$*. Is H a normal subgroup of G ?*

Sol. We first show that H is a subgroup of G. Let A, B ∈ H such that

$$A = \begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix},\ ab \neq 0, \quad B = \begin{pmatrix} a_1 & 0 \\ 0 & b_1 \end{pmatrix},\ a_1\, b_1 \neq 0$$

Consider
$$AB = \begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix}\begin{pmatrix} a_1 & 0 \\ 0 & b_1 \end{pmatrix} = \begin{pmatrix} aa_1 & 0 \\ 0 & bb_1 \end{pmatrix} \in H, \qquad | \because \quad aba_1b_1 \neq 0$$

⇒ H is closed under multiplication of matrices

Further, for $A \in H$, $A^{-1} = \begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix}^{-1} = \begin{pmatrix} \frac{b}{ab} & 0 \\ 0 & \frac{a}{ab} \end{pmatrix} = \begin{pmatrix} \frac{1}{a} & 0 \\ 0 & \frac{1}{b} \end{pmatrix} \in H,\ \frac{1}{ab} \neq 0$

Thus, every element of H has multiplicative inverse. Thus H is a subgroup of G under matrix multiplication.

Also, For $g = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in G$, $h = \begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix} \in H$, Consider

$$ghg^{-1} = \begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix}\begin{pmatrix} a & b \\ c & d \end{pmatrix}^{-1} = \begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix}\begin{pmatrix} \frac{d}{ad-bc} & \frac{-b}{ad-bc} \\ \frac{-c}{ad-bc} & \frac{a}{ad-bc} \end{pmatrix}$$

$$= \begin{pmatrix} a^2 & b^2 \\ ca & db \end{pmatrix}\begin{pmatrix} \frac{d}{ad-bc} & \frac{-b}{ad-bc} \\ \frac{-c}{ad-bc} & \frac{a}{ad-bc} \end{pmatrix} = \begin{pmatrix} \frac{a^2d - b^2c}{ad-bc} & \frac{-a^2b + b^2a}{ad-bc} \\ \frac{cad - dbc}{ad-bc} & \frac{-cab + dab}{ad-bc} \end{pmatrix} \notin H$$

Hence H is not a normal subgroup of G under matrix multiplication.

Example 6. *Let G be the group of non-singular 2 × 2 matrices under matrix multiplication. Let H be the subset of G consisting of the lower triangular matrices i.e.; matrices of the form* $\begin{pmatrix} a & 0 \\ c & d \end{pmatrix}$ *where $ad \neq 0$. Show that H is a subgroup of G, but not a normal subgroup.*

Sol. Let A, B ∈ H such that

$$A = \begin{pmatrix} a_1 & 0 \\ c_1 & d_1 \end{pmatrix}, \quad B = \begin{pmatrix} a_2 & 0 \\ c_2 & d_2 \end{pmatrix}$$

Consider
$$AB = \begin{pmatrix} a_1 & 0 \\ c_1 & d_1 \end{pmatrix}\begin{pmatrix} a_2 & 0 \\ c_2 & d_2 \end{pmatrix}$$

$$= \begin{pmatrix} a_1a_2 & 0 \\ c_1a_2 + d_1c_2 & d_1d_2 \end{pmatrix} \in H$$

$\therefore$ H is closed under matrix multiplication.

Also for any M $\in$ H, we have $M = \begin{pmatrix} a & 0 \\ c & d \end{pmatrix}$

$$\Rightarrow \qquad |M| = \begin{vmatrix} a & 0 \\ c & d \end{vmatrix} = ad \neq 0 \text{ (given)}$$

$\therefore$ M^{-1} exists. Further $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \in$ H is the identity of H. Hence, H is a subgroup of G. But H is not a normal subgroup of G.

Since, for example,

Take $$g = \begin{pmatrix} 1 & 2 \\ 1 & 3 \end{pmatrix} \in G; \quad h = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} \in H$$

Consider $$ghg^{-1} = \begin{pmatrix} 1 & 2 \\ 1 & 3 \end{pmatrix}\begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}\begin{pmatrix} 1 & 2 \\ 1 & 3 \end{pmatrix}^{-1}$$

$$= \begin{pmatrix} 1 & 2 \\ 1 & 3 \end{pmatrix}\begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}\begin{pmatrix} 3 & -2 \\ -1 & 1 \end{pmatrix}$$

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

$$= \begin{pmatrix} 7 & -4 \\ 9 & -5 \end{pmatrix} \notin H.$$

Example 7. *Let G be the group of non-singular 2 × 2 matrices under matrix multiplication. Let H be a subset of G consisting of matrices with determinant 1. Show that K is a normal subgroup of G.*

Sol. We know that if $I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$, then

$$\det(I) = 1 \quad \therefore \quad I \in H. \text{ i.e., H has an identity.}$$

Let A, B $\in$ H $\Rightarrow$ det (A) = 1, det (B) = 1

Now, det (AB) = (det A) (det B) = 1.1 = 1

$\Rightarrow$ AB $\in$ H *i.e.*, H is closed under matrix multiplication. Let A $\in$ H $\Rightarrow$ det(A) = 1

Further, $\det(A^{-1}) = 1/\det(A) = 1/1 = 1$

$\therefore$ $A^{-1} \in$ H. *i.e.,* H has an inverse.

$\therefore$ H is a subgroup of G.

Let X $\in$ G and A $\in$ H such that det A = 1

Consider $\det(XAX^{-1}) = \det(X)\det(A)\det(X^{-1})$

$$= \det(X) . 1 . \frac{1}{\det(X)} = 1$$

$\therefore$ $XAX^{-1} \in H$ for all $X \in G$

$\therefore$ H is a normal subgroup of G.

Example 8. *Every subgroup of an abelian group is normal.*

Sol. Let H be a subgroup of a normal group G. We show H is normal. Let $h \in H$ and $g \in G$. Consider

$$\begin{aligned} ghg^{-1} &= gg^{-1}h \\ &= eh \\ &= h \in H \end{aligned}$$

$\Rightarrow$ $ghg^{-1} \in H.$

$h \in H \subseteq G \;\Rightarrow\; h \in G$

Also $h, g^{-1} \in G$ and since G is abelian

$\therefore$ $hg^{-1} = g^{-1}h$

Hence, H is a normal subgroup of G.

8.21. QUOTIENT GROUP

Let G be a group and H be a normal subgroup of G. Let G/H denotes the set of right (left) cosets of H in G. Then G/N is a group (Proved in above theorem IX) called quotient group, or factor group under the coset multiplication defined by

$$(a\text{H})\,(b\text{H}) = ab\text{H}.$$

8.22. CYCLIC GROUP

(P.T.U. B.Tech. Dec. 2002)

A group G is called cyclic if for some $a \in$ G, every element $x \in$ G is of the form a^n for some $n \in$ Z. The element a is called the generator of G.

If G is cyclic, we write G = $< a >$

For *e.g.*, If G = $\{1, -1, i, -i\}$, then G is a cyclic group generated by i.

Since $$i^1 = i,\ i^2 = -1,\ i^3 = -i,\ i^4 = 1$$

i.e., every element of G is of the form i^n for some $n \in$ Z. Hence i is a generator for the cyclic group.

Remark. The order of a generator of the cyclic group is equal to the order of the group.

e.g., $Z_{12} = [Z_{12}\,;\, +_{12}]$ is a cyclic group.

Sol. $$Z_{12} = \{0, 1, 2, \ldots\ 11, +_{12}\}.$$

Consider
$$5 = 5$$
$$5 +_{12} 5 = 10$$
$$5 +_{12} 5 +_{12} 5 = 3$$
$$5 +_{12} 5 +_{12} 5 +_{12} 5 = 8$$
$$5 +_{12} 5 +_{12} 5 +_{12} 5 +_{12} 5 = 25 = 1 \text{ etc.}$$

Thus we see that every element of Z_{12} is of the form $5n$ for some $n \in$ Z. Thus 5 is a generator of Z_{12}.

Hence $[Z_{12}, +_{12}]$ is a cyclic group with 5 as generator. Since inverse of 5 is 7 ($5 +_{12} 7 = 0$), therefore, 7 is also a generator. (theorem X below)

Example 9. *The group of integers Z is cyclic under addition.*

Sol. Z = $\{0, \pm 1, \pm 2, \pm 3, \ldots\}$

Since
$$1 = 1$$
$$1 + 1 = 2$$
$$1 + 1 + 1 = 3$$
$$\underbrace{1 + 1 + 1 + \ldots 1}_{n \text{ times}} = n \text{ etc}$$

Thus we see that every element of Z is of the form $n(1)$. Thus Z is cyclic group. Hence Z = $< 1 >$. ALso Z = $< -1 >$.

Example 11. *Consider the group G = {1, 2, 3, 4, 5, 6} under multiplication modulo 7.*

(a) Find the multiplication table of G

(b) Find 2^{-1}, 3^{-1}, 6^{-1}

(c) Find the orders and subgroups generated by 2 and 3

(d) Is G cyclic ?

Sol. By definition, $a \times_7 b$ = The remainder when ab is divided by 7

For *e.g.*, $5 \times_7 6 = 30 = 2$ (when 30 is divided by 7, the remainder is 2)

The multiplication table is shown below

$\times_7$	1	2	3	4	5	6
1	1	2	3	4	5	6
2	2	4	6	1	3	5
3	3	6	2	5	1	4
4	4	1	5	2	6	3
5	5	3	1	6	4	2
6	6	5	4	3	2	1

(*b*) The identity element of G is 1. (As the first row inside the table is identical with the top most row).

$\therefore$ $2^{-1} = 4$ (In the table, the intersection of 2 and 4 is 1)

$3^{-1} = 5$

$6^{-1} = 6$

(*c*) We have $2 = 2$

$2 \times_7 2 = 4$

$2 \times_7 2 \times_7 2 = 8 = 1$

$\therefore$ $o(2) = 3$

Hence <2> = The subgroup generated by 2 = {1, 2, 4}

Also $3 = 3$

$3 \times_7 3 = 9 = 2,$

$3 \times_7 3 \times_7 3 = 27 = 6$

$3 \times_7 3 \times_7 3 \times_7 3 = 81 = 4$

$3 \times_7 3 \times_7 3 \times_7 3 \times_7 3 = 243 = 5$

$3 \times_7 3 \times_7 3 \times_7 3 \times_7 3 \times_7 3 = 729 = 1$

$\therefore$ $o(3) = 6$. $\therefore$ The group generated by 3 is given as

<3> = {1, 2, 3, 4, 5, 6} = G

(*d*) Since $o(3) = 6 = o(G)$ ⇒ G is cyclic. Recall that a group G is cyclic if there exists an element $a \in$ G such that $o(a) = o(G)$.

Example 12. *Let G = [1, 5, 7, 11] under multiplication modulo 12.*

(a) Find the multiplication table of G

(b) Find the order of each element

(c) If G cyclic ?

Sol. (*a*) We know $a \times_{12} b$ = The remainder when the product ab is divided by 12

Sol. (*a*) We know $a \times_{12} b$ = The remainder when the product ab is divided by 12

i.e., $$5 \times_{12} 7 = 35 = 11 \text{ etc.}$$

The multiplication table is shown below

$\times_{12}$	1	5	7	11
1	1	5	7	11
5	5	1	11	7
7	7	11	1	5
11	11	7	5	1

(*b*) Order (1) = 1 (since 1 is the identity element)

To find order of 5. $5 \times_{12} 5 = 25 = 1$

$\therefore$ $$o(5) = 2$$

To find order of 7. $7 \times_{12} 7 = 49 = 1$

$\therefore$ $$o(7) = 2$$

To find order of 11. $11 \times_{12} 11 = 121 = 1$

$\therefore$ $$o(11) = 2$$

(*c*) We know that a group G is cyclic if there exists an element $a \in$ G such that $o(a) = o(\text{G})$. Since $o(1) = 1$, $o(5) = 2$, $o(7) = 2$, $o(11) = 2$ *i.e.*,

There is no element of G whose order = 4

$\therefore$ G is not cyclic.

8.23. (a) GROUP HOMOMORPHISM

(*P.T.U. B. Tech. May 2007, May 2006, May 2002 ; Dec. 2001*)

A mapping from a group (G,.). into a group $(\overline{\text{G}}, *)$ is said to be a group homomorphism if

$$\phi(a \,.\, b) = \phi(a) * \phi(b) \quad \forall\ a, b \in \text{G}$$

8.23. (b) GROUP ISOMORPHISM

(*P.T.U. B. Tech. Dec. 2007*)

A homomorphism ϕ which is one-one and onto is called **isomorphism** and the groups G and G′ are called **isomorphic**, written as G ≅ G′.

A homomorphism which is onto is called **epimorphism**

A homomorphism which is one-one is called **monomorphism.**

8.24. KERNEL f

If f is a homomorphism of G to $\overline{\text{G}}$, then kernel f is the set defined by

$$\text{Ker } f = [x \in \text{G} : f(x) = \bar{e},\ \bar{e} \in \overline{\text{G}}]$$

8.25. IMAGE f

The image f is the set of the images of the elements under f *i.e.*,

$$\text{Im}(f) = \{b \in G' : f(a) = b \text{ for } a \in G\} \text{ where } f \text{ is a homomorphism of G to G}'$$

The term 'range f' is also used for 'image f'.

Example 13. *Let G be a group of real numbers under addition and let G′ be the group of positive real numbers under multiplication. Define $f : G \rightarrow G'$ by $f(a) = 2^a$.*

Show that f is a homomorphism. Also show that G and G′ are isomorphic.

Sol. Given f is a mapping from (G, +) to (G′, .) defined by $f(a) = 2^a$

Let $a, b \in$ G and consider

$$f(a + b) = 2^{a+b} = 2^a \cdot 2^b = f(a) \cdot f(b)$$

Hence $f : G \rightarrow G'$ is homomorphism.

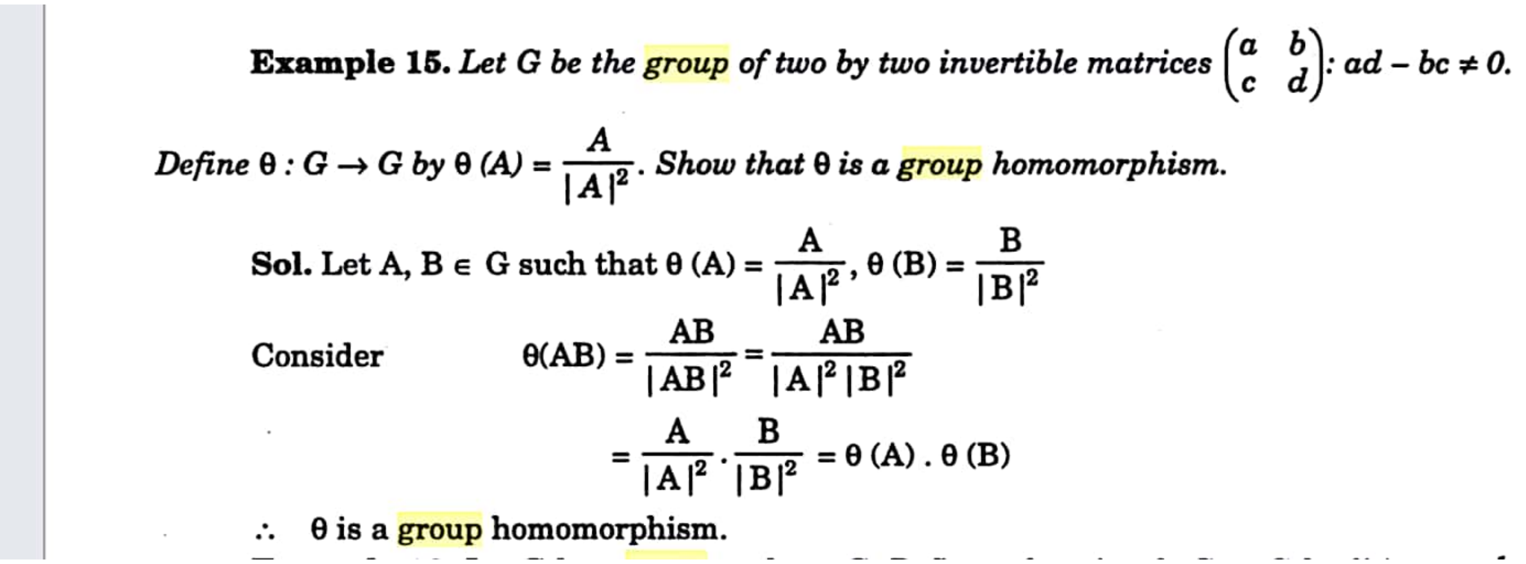
To check f is one-one. Let $f(a) = f(b)$

$\Rightarrow$ $$2^a = 2^b \Rightarrow a = b$$

$\therefore$ f is one-one.

To check f is onto : For each $a \in$ R, we have 2^a is a positive real number. Thus $f(a) = 2^a$ is onto.

Hence $f : G \rightarrow G'$ is an isomorphism and the groups G and G′ are isomorphic *i.e.*, $G \cong G'$.



Example 15. *Let G be the group of two by two invertible matrices* $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$*: ad – bc ≠ 0.*

Define $\theta : G \to G$ *by* $\theta(A) = \dfrac{A}{|A|^2}$*. Show that θ is a group homomorphism.*

Sol. Let A, B ∈ G such that $\theta(A) = \dfrac{A}{|A|^2}, \theta(B) = \dfrac{B}{|B|^2}$

Consider $$\theta(AB) = \frac{AB}{|AB|^2} = \frac{AB}{|A|^2 |B|^2}$$

$$= \frac{A}{|A|^2} \cdot \frac{B}{|B|^2} = \theta(A) . \theta(B)$$

∴ θ is a group homomorphism.