8 MONOIDS AND 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 $f : A \times A \to A$, then f is called a binary operation on A whose domain is the set of ordered pairs of elements of 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.

8.4. TABLES OF OPERATION

Consider a non-empty finite set $A = \{a_1, a_2, a_3, \ldots, a_n\}$. A binary operation $*$ on A can be described by means of table as shown below:

$*$	a_1	a_2	a_3		a_n
a_1	a_1*a_1	a_1*a_2			
a_2	a_2*a_1	a_2*a_2			
a_3			a_3*a_3		
a_n					a_n*a_n

The empty cell in the j^{th} row and k^{th} column represent the element a_j*a_k.

ILLUSTRATIVE EXAMPLES

Example 1. *Consider the set A = {1, 2, 3} and a binary operation $*$ on the set A defined by $a * b = 2a + 2b$. Represent operation $*$ as a table on A.*

Sol. The table of operation is shown below: (Table 8.1)

Table 8.1

*	1	2	3
1	4	6	8
2	6	8	10
3	8	10	12

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

$-1 * 0 = 0$; $-1 * 1 = -1$; $-1 * -1 = 1$

$0 * -1 = 0$; $0 * 1 = 0$; $0 * 0 = 0$

$1 * -1 = -1$; $1 * 0 = 0$; $1 * 1 = 1$

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

Example 3. *Consider the set $A = \{1, 3, 5, 7, 9, \ldots\}$, 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. (*a*) *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.

(*b*) *Consider the binary operation $*$ on the set N of positive integers defined by*

$$a * b = a^b$$

Determine whether $*$ is associative?

Sol. (*a*) 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.

(*b*) $*$ will be associative if

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

Take $a = 2, b = 2, c = 3$ and consider

$$a * (b * c) = 2 * (2 * 3) = 2 * 2^3 = 2 * 8 = 2^8 = 256$$

and $(a * b) * c = (2 * 2) * 3 = 2^2 * 3 = 4 * 3 = 4^3 = 64$

Hence $a * (b * c) \neq (a * b) * c$

$\therefore$ $*$ is non-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. (*a*) *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.

(*b*) *Consider $S = \{a, b, c, d\}$ and $*$ be a binary operation on S defined by as shown in the following table.*

Table 8.2

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

*Determine (i) whether * is associative ?*

*(ii) whether * is commutative?*

Sol. (a) 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.

(b) (i) Let $a, b, c \in S$ and consider

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

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

$\Rightarrow$ $$b * (c * c) \neq (b * c) * c$$

Thus, * is non-associative

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

$\Rightarrow b * c * c * b$

$\therefore$ * is non-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

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

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

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

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, $$e_1'' * e_1' = e_1'' \qquad \ldots(1)$$

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

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

Hence,

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 $a * b = \frac{ab}{2}$. Determine the identity for the binary operation $*$, if exists.*

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

$$e * a = a,\ a \in I_+$$

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

$\Rightarrow$

$$a * e = a,\ a \in I_+$$

Similarly,

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

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.

6. Idempotent. Consider a non-empty set A and a binary operation $*$ on A. Then the operation $*$ has the idempotent property, if for each $a \in$ A, we have

$$a * a = a \ \forall\ a \in \text{A}.$$

7. Distributivity. Consider a non-empty set A and two binary operations $*$ and $+$ on A. Then the operation $*$ distributes over $+$, if for every $a, b, c \in$ A, we have

$$a * (b + c) = (a * b) + (a * c) \qquad \text{[Left distributivity]}$$

and

$$(b + c) * a = (b * a) + (c * a) \qquad \text{[Right distributivity]}$$

8. Cancellation. Consider a non-empty set A and a binary operation $*$ on A. Then the operation $*$ has the cancellation property, if for every $a, b, c \in$ A, we have

$$a * b = a * c \quad \Rightarrow \quad b = c \qquad \text{[Left cancellation]}$$

and

$$b * a = c * a \quad \Rightarrow \quad b = c \qquad \text{[Right cancellation]}$$

8.6. SEMI-GROUP

(P.T.U. B.Tech. Dec. 2009, May 2008)

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 $b * (a * b') = b * e = b$ ...(1)

and $(b * a) * b' = e * b' = b'$ ...(2)

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

$\Rightarrow$ $b = b'$. | 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

$\therefore$ $4 * 6$ = L.C.M. of 4 and 6 = 12

$3 * 5$ = L.C.M. of 3 and 5 = 15

$9 * 18$ = L.C.M. of 9 and 18 = 18

$1 * 6$ = L.C.M. of 1 and 6 = 6

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

$$a * (b * c) = (a * b) * c \quad \forall \; a, b, c \in N$$

$\therefore$ 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 $1 = a$

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

Also, $a * 1 = a = 1 * a$

$\therefore$ 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) $3 * 4 = 3 + 4 - 12 = -5$

$2 * (-5) = 2 + (-5) - (-10) = 2 - 5 + 10 = 7$

$7 * \frac{1}{2} = 7 + \frac{1}{2} - \frac{7}{2} = 4.$

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

Consider $a * (b * c) = a * (b + c - bc)$

$= a + (b + c - bc) - a(b + c - bc)$

$= a + b + c - bc - ab - ac + abc$ ...(1)

Also, $(a * b) * c = (a + b - ab) * c$

$= a + b - ab + c - (a + b - ab)\, c$

$= a + b + c - ab - ac - bc + abc$

$= a + b + c - bc - ab - ac + abc$ ...(2)

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

$a * e = a$

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

$\Rightarrow \quad e - ea = 0$

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

$\Rightarrow \quad e = 0$ 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)

$$\Rightarrow \quad a + x - ax = 0$$
$$\Rightarrow \quad a + x(1 - a) = 0$$
$$\Rightarrow \quad a = x(a - 1)$$
$$\Rightarrow \quad x = \frac{a}{a-1}, \; a \neq 1$$

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

Example 13. *Consider a non-empty set S with the operation $a * b = a$*
(a) Is the operation associative ?
(b) Is the operation commutative ?
(c) Show that the right cancellation law holds.
(d) Does the left cancellation law hold ?

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.

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

$$a * c = b * c$$
$$\Rightarrow \quad a = b \qquad \text{| Using given } a * b = a$$

$\therefore$ Right cancellation laws hold.

(d) The left cancellation law does not hold. For example, suppose $b \neq c$, then

$$a * b = a * c$$
$$\Rightarrow \quad b = c, \quad \text{a contradiction}$$

Hence, the result.

Example 14. *Let $(A, *)$ be semi-group. Show that for a, b, c in A, if $a * c = c * a$ and $b * c = c * b$, then $(a * b) * c = c * (a * b)$.*

Sol. Take L.H.S., we have

$$\begin{aligned}
(a * b) * c &= a * (b * c) && [\because \; * \text{ is associative}] \\
&= a * (c * b) && [\because \; b * c = c * b] \\
&= (a * c) * b && [\because \; * \text{ is associative}] \\
&= (c * a) * b && [\because \; a * c = c * a] \\
&= c * (a * b) && [\because \; * \text{ is associative}]
\end{aligned}$$

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

8.12. MONOID

(P.T.U. B.Tech., Dec. 2013, May 2013, Dec. 2012, May 2008)

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.

Examples. (N, ×), (Z, +), (Q, +) are monoids

Example 29. *Consider an algebraic system (I, +), where the set I = {0, 1, 2, 3, 4, ...} the set of natural numbers including zero 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.

Example 30. *Let S be a finite set and F(s) be the collection of all functions $f : S \to S$ under the operation of composition of functions. Show that F(s) is a semi-group. Is F(s) a monoid?*

Sol. Let $f, g, h \in \text{F}(s)$, then we know that composition of functions is associative *i.e.*, $fo(goh) = (fog)oh \; \forall \; f, g, h \in \text{F}(s)$. Hence, F(s) is a semi-group. Also the identify function is an identify element of F(s).

$\therefore$ F(s) is a monoid.

(*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 $-a \in I$.

Examples (*i*) The sets (Q, +) (R, +) and (C, +) are groups under addition.

(*ii*) The sets R* (set of non-zero reals), Q* (set of non-zero rationals) and C* (set of non-zero complex numbers) are groups under multiplication.

ILLUSTRATIVE EXAMPLES

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 2010, 2009)

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

Consider the multiplication modulo 7 table as shown below (Table 8.5). 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

Table 8.5

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 $a, b, c \in G$

$a \times_7 (b \times_7 c) = (a \times_7 b) \times_7 c$ *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, $(a * b) * c = a * (b * c)$

$\therefore$ $*$ is associative.

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

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

[Identity]

$$a * a^{-1} = 0$$

$\therefore$ $a + a^{-1} - aa^{-1} = 0$

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

Now, $\dfrac{a}{a-1} \in Q$, 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.

Theorem III. *Show that the identity element in a group is unique.*

Proof. Let us assume that there exists two identity elements *i.e.*, e and e' of G.
Since, $e \in G$ and e' is an identity. We have $e'e = ee' = e$
Also, $e' \in G$ and e is an identity. We have $e'e = ee' = e'$
$\therefore \quad e = e'$
Hence, identity in a group is unique.

Theorem IV. *Show that inverse of an element a in a group G is unique.*

Proof. Let us assume that $a \in G$ be an element. Also, assume that a_1^{-1} and a_2^{-1} be two inverse elements of a. Then we have,

$$a_1^{-1} a = a a_1^{-1} = e \quad \text{and} \quad a_2^{-1} a = a a_2^{-1} = e$$

Now, $$a_1^{-1} = a_1^{-1} e = a_1^{-1}(a a_2^{-1}) = (a_1^{-1} a) a_2^{-1} = e a_2^{-1} = a_2^{-1}$$

Thus, the inverse of an element is unique.

Theorem V. *Show that $(a^{-1})^{-1} = a$ for all $a \in G$, where G is a group and a^{-1} is an inverse of a.*

Proof. Given that a^{-1} is an inverse of a. Then, we have

$$a a^{-1} = a^{-1} a = e$$

This implies that a is also an inverse of a^{-1}. Therefore $(a^{-1})^{-1} = a$.

Theorem VI. *Show that $(ab)^{-1} = b^{-1} a^{-1}$ for all $a, b \in G$.*

Proof. We have to prove that ab is inverse of $b^{-1} a^{-1}$. We prove

$$(ab)(b^{-1} a^{-1}) = (b^{-1} a^{-1})(ab) = e$$

Consider $$(ab)(b^{-1} a^{-1}) = [(ab)\, b^{-1}]a^{-1} = [a(bb^{-1})]\, a^{-1}$$
$$= (ae)\, a^{-1} = a a^{-1} = e \qquad \ldots(1)$$

Similarly, $(b^{-1} a^{-1})(ab) = e$ ...(2)

$\therefore$ From (1) and (2), we have

$$(ab)\ (b^{-1} a^{-1}) = e = (b^{-1} a^{-1})\ ab$$ Hence proved.

Theorem VII. *Prove the left cancellation law in a group G holds i.e., $ab = ac \Rightarrow b = c$ $\forall\ a, b, c \in G$.*

Proof. Consider $ab = ac$.

Then, we have $$b = eb = (a^{-1} a)b = a^{-1}(ab) = a^{-1}(ac)$$ [$\because ab = ac$]
$$= (a^{-1} a)c = ec = c$$ | Associativity

Hence, $ab = ac \Rightarrow b = c$.

Theorem VIII. *Prove the right cancellation law in a group G holds i.e., $ba = ca \Rightarrow b = c$ $\forall\ a, b, c \in G$.*

Proof. Consider $ba = ca$.

Then, we have $$b = be = b(aa^{-1}) = (ba)a^{-1} = (ca)a^{-1}$$ [$\because ba = ca$]
$$= c(aa^{-1}) = ce = c$$ | Associativity

Hence, $ba = ca \Rightarrow b = c$.

If G is a group under +, then a is said to be of order n if n is a least positve integer such that $na = e$. Here e is the identity element of G.

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.

Example 7. *Let ({e, x, y}, *) be a group of order 3. The table of operation is shown in (Fig. 8.4).*

*	e	x	y
e	e	x	y
x	x	y	e
y	y	e	x

Fig. 8.4

Example 8. *Consider an algebraic system ({0, 1}, +) where the operation + is defined as shown in (Fig. 8.5).*

+	0	1
0	0	1
1	1	0

Fig. 8.5

The system ({0, 1}, +) is a group. In this 0 is identity element and every element is its own inverse.

Theorem XI. *If G is a finite group of order n and $a \in G$, then there exists a positive integer m such that $a^m = e$ and $m \leq n$.*

Proof. Consider the elements of the group G as $a, a^2, a^3, \ldots a^{n+1}$. These are $n+1$ elements. Since $|\ G\ | = n$. Therefore two of its elements, say, a^p, a^q must be equal, *i.e.*, $a^p = a^q$, $p < q$. Take $m = q - p$

$$\therefore \quad a^m = a^{q-p} = a^p \cdot a^{-p}$$
$$= a^q \cdot (a^p)^{-1} = a^q \cdot (a^q)^{-1} \qquad | \ a^p = a^q$$
$$= e$$

Further, since p, q are among $n + 1$,

$$\therefore \quad 1 \leq p < q \leq n+1 \ \Rightarrow \ q - p = m \leq n.$$

8.18. SUBGROUP

(P.T.U. B.Tech. May 2013, 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.

Since $Z \subseteq Q$, Z is a subgroup of Q under addition.

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 identity 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.,*

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

Show that H is a subgroup of Z.

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

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

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.

Theorem XII. *A subset H of a group G is a subgroup of G iff*

(*i*) *The identity element $e \in H$*

(*ii*) *H is closed under the same operation as in G*

(*iii*) *H is closed under inverses i.e., if $a \in H$, then $a^{-1} \in H$.*

Proof. Given G is a group and H is a subset of G. Let H is a subgroup of G, then, by definition, (*i*), (*ii*), (*iii*) are true.

Converse. Let (*i*), (*ii*), (*iii*) hold. We show H is a subgroup of G. We show the associativity of elements of H.

Let $a, b, c \in G$ and since $H \subseteq G$ $\therefore$ $a, b\, c \in H$

Since elements of G are also elements of H

$\therefore$ Associativity holds for H. Hence the **Theorem.**

Another statement : A subset H of a group G is a subgroup of G iff $a * b^{-1} \in H$. $\forall\, a, b \in H$

Theorem XVI. Let H be a subgroup of G. Then

(*a*) $H = Ha \Leftrightarrow a \in H$

(*b*) $Ha = Hb \Leftrightarrow a\,b^{-1} \in H$

(*c*) $aH = bH \Leftrightarrow a^{-1} b \in H$

(*d*) $HH = H$.

Proof. (*a*) Let $Ha = H$. If $e \in H \Rightarrow e\,a \in Ha = H$

$a \in H$ | $ea = a$

$\Rightarrow$ Conversely, Let $a \in H$. As H is a subgroup and $h \in H$, $a \in H$

$h\,a \in H$ | H is closed under multiplication.

$\Rightarrow$ $H\,a \subseteq H$ ...(1)

$\Rightarrow$ Again, if $h \in H$, $a \in H$ and since H is a subgroup of G, $\therefore\ h\,a^{-1} \in H$ (Theorem X)

$(ha^{-1})\,a \in H\,a$

$\Rightarrow$ $h(a^{-1}a) \in Ha \Rightarrow h\,e \in Ha$

$\Rightarrow$ $h \in H\,a$

$\Rightarrow$ $H \subseteq H\,a$ ...(2)

$\Rightarrow$ From (1) and (2) $Ha = H$

(*b*) Let $Ha = Hb$ and we show $ab^{-1} \in H$

Now $a = e\,a \in Ha$

$\Rightarrow$ $a \in Ha = Hb$

$\Rightarrow$ $a \in Hb \Rightarrow a = hb,\ h \in H$

$\Rightarrow ab^{-1} = (hb)b^{-1} = h(bb^{-1}) = he = h \in H$

$\Rightarrow ab^{-1} \in H$

Conversely, Let $ab^{-1} \in H \Rightarrow ab^{-1} = h,\ h \in H$

$\Rightarrow$ $a = hb$

$\Rightarrow$ $Ha = Hhb = Hb$ | For $h \in H$, $Hh = H$

(*c*) Proceed yourself as in Part (*b*).

(*d*) Let $h \in H$. Then,

$H = Hh \quad \forall\ h \in H$ | Using part (*a*)

$\Leftrightarrow$ $H \subseteq HH \subseteq H$

$\therefore$ $HH = H$.

8.19. ABELIAN GROUP

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 $a, b \in I$.

Example 11. *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, $a * b = \frac{ab}{4}$ 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 $a \in G$,

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

Similarly, $a * e = a$

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

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 $a * a^{-1} = 4$

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

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

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

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

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

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 12. *Let $(\mathbf{Z}, *)$ be an algebraic structure, where Z is the set of integers and the operation $*$ is defined by $n * m$ = maximum (n, m). Determine whether $(\mathbf{Z}, *)$ 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 13. *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 $(\{0, 1\}, \otimes)$ is not a group.

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

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

$\otimes$	0	1
0	0	0
1	0	1

Fig. 8.6

(b) **Associative property.** The operation $\otimes$ 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

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

But the inverse of element 0 does not exist.

Therefore, since the inverse of every element $a \in \{0, 1\}$ does not exist. Hence $(\{0, 1\}, \otimes)$ is not a group.

(ii) The three distinct groups (G, $\otimes$), where G $\subset$ S and G has 2 elements is as follows

(a) $(\{1, 3\}, \otimes)$ (b) $(\{1, 5\}, \otimes)$ (c) $(\{1, 7\}, \otimes)$.

8.20. (a) COSETS

(P.T.U. B.Tech. Dec. 2006)

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 $e * H = H * e = H$.

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.

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

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

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

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

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

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

$$6 + H = \{..... -8, -1, 6, 13, 20, 27, ...\}$$

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

All other cosets coincides with any one of the cosets shown above, hence we will not count them.

Theorem I. *If $b \in a * H$ (left coset), then $a * H = b * H$. Also, if $b \in H * a$ (right coset), Then $H * a = H * b$*

Proof. Case I. Let $x \in a * H$, we show $x \in b * H$

Now $x \in a * H \Rightarrow$ there exists an element $h_1 \in H$ such that $x = a * h_1$

Also $b \in a * H \Rightarrow$ There exists an element $h_2 \in H$ such that $b = a * h_2$

$$b * h_2^{-1} = (a * h_2) * h_2^{-1} = a * (h_2 * h_2^{-1}) = a * e = a$$

$\Rightarrow$ $a = b * h_2^{-1}$

$\Rightarrow$ $x = a * h_1 = (b * h_2^{-1}) * h_1 = b * (h_2^{-1} * h_1)$

$\therefore$ Since $h_1, h_2 \in H$ and H is subgroup of G

$h_2^{-1} \in H$ and $h_2^{-1} * h_1 \in H$

$\therefore$ $x = b * (h_2^{-1} * h_1) \in b * H$

Hence $x \in b * H$

$\Rightarrow$ $a * H \subseteq b * H$

$\Rightarrow$ Similarly, if $x \in b * H$, we can easily show that $x \in a * H$. ...(1)

$\Rightarrow$ $b * H \subseteq a * H$

from (1) and (2), $a * H = b * H$ ...(2)

Case II. Let $x \in H * a$. We show $x \in H * b$. Now $x \in H * a \Rightarrow$ There exists an element $h_1 \in H$ such that $x = h_1 * a$

Also $b \in H * a \Rightarrow$ There exists an element $h_2 \in H$ such that $b = h_2 * a$

$\Rightarrow$ $h_2^{-1} * b = h_2^{-1} * (h_2 * a) = (h_2^{-1} * h_2) * a$

$= e * a = a$

$\Rightarrow$ $a = h_2^{-1} * b$

$\therefore$ $x = h_1 * a = h_1 * (h_2^{-1} * b) = (h_1 * h_2^{-1}) * b$

Since $h_1, h_2 \in H$ and H is a subgroup of G. $\therefore$ $h_1 * h_2^{-1} \in H$

Hence $x = (h_1 * h_2^{-1}) * b \in H * b$

$\Rightarrow$ $x \in H * b$

$\Rightarrow$ $H * a \subseteq H * b$

Similarly, if $x \in H * b$, we can easily show that $x \in H * a$

$\Rightarrow$ $H * b \subseteq H * a$

Hence $H * a = H * b$

Theorem II. *Let H be a subgroup of a group G. Then the right cosets Ha form a partition of G.*

Or

Any two right (left) cosets in a group G are either disjoint or equal.

Proof. Let Ha and Hb be two right cosets and suppose $Ha \cap Hb \neq \phi$. We show $Ha = Hb$

Let $x \in Ha \cap Hb \Rightarrow x \in Ha$ and $x \in Hb$

$\Rightarrow$ $x = h_1 a$ and $x = h_2 b$ for some $h_1, h_2 \in H$

$\Rightarrow$ $h_1 a = h_2 b \in Hb$

$\Rightarrow$ $h_1 a \in Hb$

$\Rightarrow$ $Ha \subseteq Hb$

Also $h_2 b = h_1 a \in Ha$

$\Rightarrow$ $h_2 b \in Ha$

$\Rightarrow$ $Hb \subseteq Ha$

Hence $Ha = Hb$

Lagrange's Theorem

(P.T.U. B.Tech. Dec. 2007, 2006, May 2006, May 2012, May 2013)

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,

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

We claim H and any coset Ha have the same number of elements.

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

$$h_ia = h_ja$$

$$h_i = h_j \quad \text{| Right cancellation law}$$

$\Rightarrow$ a contradiction, since h_i's are distinct. Thus, H and Ha have same number of elements.

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

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

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

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

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

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

Hence the Theorem.

Converse of Lagrange's theorem is however, not true *i.e., If* $o(H) \mid o(G)$. Then G may not have a subgroup of order $o(H)$.

Consider the alternating group A_4. Here $o(A_4) = \frac{4!}{2} = 12$ and $6 \mid 12$. But there is no subgroup of A_4 whose order is 6. (see the topic "Symmetric Group" in this chapter)

8.21. 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* $[G: H] = \frac{o(G)}{o(H)}$.

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

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

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

Theorem V. *Let G be a finite group of order n show that* $a^n = e$ *for any element* $a \in G$.

(P.T.U. B.Tech. Dec. 2010)

Proof. Let $a \in G$ has order m, then $a^m = e$

Let H be a subgroup of G, of order m. By Lagrange's theorem,

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

$\Rightarrow$ $m/n \Rightarrow n = mr$, for some r

$\therefore$ $a^n = a^{mr} = (a^m)^r = e^r = e$

Hence the Theorem.

8.22. NORMAL SUBGROUP

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

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

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 real matrices* $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$; $ad - bc \neq 0$. *Let* $H = \left[\begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix} : a \neq 0\right]$. *Then H is a normal subgroup of G.* (P.T.U. B.Tech. Dec. 2010)

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

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

$\Rightarrow$ 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 ≠ 0. Show that H is a subgroup of G, but not a normal subgroup.*

Sol. Let A, B $\in$ 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 $M = \begin{pmatrix} a & 0 \\ c & d \end{pmatrix}$

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

$\therefore$ 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

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

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

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

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

$\therefore$ $XAX^{-1} \in H$ 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

$$ghg^{-1} = gg^{-1}h$$
$$= eh$$
$$= h \in H$$
$$ghg^{-1} \in H.$$

$h \in H \subseteq G \Rightarrow h \in G$
Also $h, g^{-1} \in G$ and since G is abelian
$\therefore \quad hg^{-1} = g^{-1}h$

$\Rightarrow$ Hence, H is a normal subgroup of G.

Theorem VI. *Let H be a subgroup and K be a normal subgroup of a group G. Show that HK is a subgroup of G.* (P.T.U. B.Tech. Dec. 2013)

Proof. We show that (*i*) HK is closed under multiplication

(*ii*) For $x \in$ HK, we should have $x^{-1} \in$ HK

(*iii*) $e \in$ HK

Let $x, \quad y \in HK \Rightarrow \quad x = h_1 k_1, y = h_2 k_2$, where $h_1, h_2 \in H; k_1, k_2 \in K$

Consider $\quad xy = h_1 k_1 h_2 k_2 = h_1 h_2 (h_2^{-1} k_1 h_2) k_2 \in HK$

[Let $h_2 \in H \Rightarrow h_2^{-1} \in H \subseteq G \Rightarrow h_2^{-1} \in G$
Since K is a normal subgroup of G, and $k_1 \in K$,
$\therefore \quad h_2^{-1} k_1 h_2 \in K$
$\Rightarrow \quad (h_2^{-1} k_1 h_2) k_2 \in K$
$\Rightarrow \quad h_1 h_2 (h_2^{-1} k_1 h_2) k_2 \in HK$]

Thus HK is closed under multiplication.

Further, For $x \in$ HK, we have

$$x^{-1} = (h_1 k_1)^{-1} = k_1^{-1} h_1^{-1} = h_1^{-1}(h_1 k_1^{-1} h_1^{-1})$$

[Let $h_1 \in H \subseteq G \Rightarrow h_1 \in G$. Also $k_1 \in K$
$\Rightarrow \quad k_1^{-1} \in K$
Since K is a normal subgroup of G
$\therefore \quad h_1 k_1^{-1} h_1^{-1} \in K$
$\Rightarrow \quad h_1^{-1} (h_1 k_1^{-1}) h_1^{-1} \in HK$]

Thus $\quad x^{-1} \in HK.$

Finally, $\quad e \in H, e \in K \Rightarrow e \cdot e \in HK \Rightarrow e \in HK$

Thus HK is a subgroup of G.

Theorem VII. *Let H is a subgroup of a group G. Then H is a normal subgroup of G iff*

$$aH = Ha \ \forall \ a \in G.$$

Proof. Let H is a normal subgroup of G. Then for $a \in$ G, we have

$$aHa^{-1} = H$$
$\Leftrightarrow \quad (aH\,a^{-1})a = Ha$
$\Leftrightarrow \quad aH(a^{-1}\,a) = Ha$
$\Leftrightarrow \quad aH\,e = Ha$
$\Leftrightarrow \quad aH = Ha$

Theorem VIII. *The intersection of any number of normal subgroups of G is a normal subgroup of G.*

8.24. (b) CYCLIC GROUP

A group whose all elements are integral powers of one or more elements is called cyclic.

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

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

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 subgroup 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 $$1 = 1$$

$$1 + 1 = 2$$

$1 + 1 + 1 = 3$

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

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

Theorem X. *If a is a generator of a cyclic group G, show that inverse of a is also a generator.*

Proof. Let $G = <a>$ *i.e.*, G is a cyclic group and a is its generator. Let $g \in G$, then

$g = a^r$ for some $r \in Z$

Take $r = -s$, $s \in Z$, we have

$g = a^{-s} = (a^{-1})^s$ for some $s \in Z$

Thus every element $g \in G$ is of the form $(a^{-1})^s$. Hence a^{-1} is a generator.

Theorem XI. *Every cyclic group is abelian.* (P.T.U. B. Tech. May 2006, May 2005)

Proof. Let G be a cyclic group with a as its generator. *i.e.*, let $G = <a>$ and $g_1 \in G$.

Then $g_1 = a^r$ for some $r \in Z$

Let $g_2 \in G$, then $g_2 = a^s$ for some $s \in Z$

Consider $g_1 \cdot g_2 = a^r \cdot a^s = a^{r+s}$

$= a^{s+r}$ | $r + s = s + r$ as Z is abelian

$= a^s \cdot a^r = g_2 \cdot g_1$

$\Rightarrow$ G is abelian.

Theorem XII. *Every subgroup of a cyclic group is cyclic.*

(P.T.U. B.Tech. Dec. 2009)

Proof. Let $G = <a>$ *i.e.*, G is a cyclic group with a as its generator. Let H be a subgroup of G.

Case I. If $H = \{e\}$, then $H = <e>$ *i.e.*, H is a cyclic group with e as a generator.

Case II. If $H \neq [e]$, then $o(H) \geq 2$ *i.e.*, there exists $e \neq a \in H$.

Since H is a subgroup, it must be closed under inverses and so contains positive powers of a. Let m is the smallest power of a such that $a^m \in H$. We claim $b = a^m$ is a generator of H. Let $x \in H$. But $H \subseteq G \quad \therefore \quad x \in G$.

Since G is a cyclic group G with a as its generator. $\therefore \quad x = a^n$ for some $n \in Z$.

Dividing n by m, we get a quotient q and remainder r. *i.e.*,

$n = mq + r$, $0 \leq r < m$

Now $a^n = a^{mq+r} = a^{mq} \cdot a^r = b^q \cdot a^r$

$\Rightarrow$ $a^r = b^{-q} \cdot a^n$

Here a^n, $b \in H$ and since H is a subgroup $\therefore \quad b^{-q}\, a^n \in H$ which means $a^r \in H$.

But m was the least positive integer of a such that $a^m \cdot \in H$ and $r < m$.

$\therefore$ We must have $r = 0$

Hence $a^n = b^q$ for some $q \in Z$

$\Rightarrow$ $x = a^n = b^q$ *i.e.*, every element $x \in H$ is of the form b^q for some $q \in Z$

$\therefore$ H is cyclic.

Theorem XIII. *If G is a cyclic group of order n and a is a generator of G. Let $(n, k) = d$. Then the order of the cyclic group generated by ka is $\frac{n}{d}$ where d is the greatest common divisor of n and k.*

Proof. Proof of this theorem is beyond the scope.

Example 10. *Find the order of the cyclic subgroup generated by 18 in Z_{30}*

Sol. We know that 1 is a generator of Z_{30}. Also $18 = 18(1)$ *i.e.*, $k = 18$, $a = 1$, $n = 30$
The greatest common divisor of $(n, k) = (30, 18) = 6 = d$

$\therefore$ The order of cyclic subgroup generated by $18 = \frac{30}{6} = 5$. (Theorem XIII)

Theorem XIV. *Every group of prime order is cyclic.*

Proof. Let G be a group of order p, p is prime. It means G must contain at least two elements. Since 2 is the least positive integer which is prime *i.e.*, if $a \in G$, then $o(a) \geq 2$.
Let $o(a) = m$ and H be a cyclic subgroup of G generated by a, then

$o(H) = o(a) = m$ | The order of a cyclic group is equal to the order of its generator

Also By Lagrange's theorem,

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

$p = 1$ or $p = m$

$\Rightarrow$ $p \neq 1 \quad \therefore \quad p = m$

But $o(H) = o(G) \Rightarrow H = G.$

$\Rightarrow$ Hence G is cyclic since H is cyclic.

Theorem XV. *Let G is a cyclic group of order p (p is prime). Show that G has no proper subgroups except G and {e}.*

Proof. Let G is a cyclic group of order p.
Let H be any subgroup of G and $o(H) = m$.
By Lagrange theorem, $o(H) \mid o(G) \Rightarrow m \mid p$

$p = 1$ or $p = m$

$\Rightarrow$ $p \neq 1 \quad \therefore \quad p = m$

But *i.e.*, $o(H) = m = p \Rightarrow$ H is a group of prime order and hence cyclic. Also $o(G) = m$

$\therefore$ G = H *i.e.* G has no proper subgroups.

Remark. Cyclic subgroup generated by a. Let G be any group and $a \in G$. Define $a^0 = e$; the *cyclic subgroup generated by a*, denoted by $<a>$, where $< a >$ denotes the set of all powers of a, is defined by $<a> = \{....., a^{-2}, a^{-1}, e, a, a^2, a^3, ...\}$

$<a>$ contains the identity element e, closed under group operation, contains inverses.

$\therefore$ $<a>$ is a subgroup of G and is called the *cyclic subgroup generated* by a.

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 ? (P.T.U. B.Tech. Dec. 2013)

Sol. (a) 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 Table 8.10

Table 8.10

$\times_7$	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 $o(3) = 6 = o(G) \Rightarrow$ 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) Is G cyclic ?

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

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

The multiplication table is shown below (Table 8.11)

Table 8.11

$\times_{12}$	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 $o(a) = o(G)$. 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.

Example 13. *Consider the group G = {1, 2, 3, 4, 5, 6} under multiplication modulo 7.*

(a) Find the multiplication table of G

(b) Prove that G is a group

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

(d) *Find the orders and subgroups generated by 2 and 3*

(e) *Is G cyclic ? Justify your answer* (P.T.U. B.Tech. Dec. 2009)

Sol. (a) and (b). Proceed yourself as in above example 12.

(c) $2^{-1} = 4$, $3^{-1} = 5$, $6^{-1} = 6$

(d) $<2> = \{1, 2, 4\}$, $<3> = \{1, 2, 3, 4, 5, 6\}$

(e) Since $o(B) = 6 = o(G) \Rightarrow$ G is cyclic.

Example 14. *Let G be a reduced residue system modulo 15 say, G = {1, 2, 4, 7, 8, 11, 13, 14}. Then G is a group under multiplication modulo 15*

(a) *Find the multiplication table of G.*

(b) *Find* 2^{-1}, 7^{-1}, 11^{-1}.

(c) *Find the orders and subgroups generated by 2, 7 and 11.*

(d) *Is G cyclic ?*

Sol. (a) The multiplication of G is shown below (Table 8.12):

Table 8.12

×	1	2	4	7	8	11	13	14
1	1	2	4	7	8	11	13	14
2	2	4	8	14	1	7	11	13
4	4	8	1	13	2	14	7	11
7	7	14	13	4	11	2	1	8
8	8	1	2	11	4	13	14	7
11	11	7	14	2	13	1	8	4
13	13	11	7	1	14	8	4	2
14	14	13	11	8	7	4	2	1

(b) From the table, $2 \times_{15} 8 = 1$ *i.e.*, 8 is the inverse of 2. Hence $2^{-1} = 8$

Also, $7 \times_{15} 13 = 1 \Rightarrow 13$ is the inverse of 7. Hence $7^{-1} = 13$

Further $11 \times_{15} 11 = 1 \Rightarrow 11$ is the inverse of 11. Hence $11^{-1} = 11$.

(c) (*i*) We have $2 \times_{15} 2 = 4$

$2 \times_{15} 2 \times_{15} 2 = 8$

$2 \times_{15} 2 \times_{15} 2 \times_{15} 2 = 1$

$\therefore$ order of $2 = o(2) = 4$

The group generated by 2 is given by

$<2> = \{2^0, 2^1, 2^2, 2^3\} = \{1, 2, 4, 8\}$

(*ii*) We have $7 \times_{15} 7 = 4$

$7 \times_{15} 7 \times_{15} 7 = 4 \times_{15} 7 = 13$

$7 \times_{15} 7 \times_{15} 7 \times_{15} 7 = 13 \times_{15} 7 = 1$

$\therefore$ order of $7 = o(7) = 4$

The group generated by 7 is given by

$<7> = \{7^0, 7^1, 7^2, 7^3\} = \{1, 7, 4, 13\}$

(*iii*) $11 \times_{15} 11 = 1 \quad \therefore$ order of $11 = o(11) = 2$

The subgroup generated by 11 is

$<11> = \{11^0, 11^1\} = \{1, 11\}$

(d) The group G is cyclic if $\exists$ an element whose order equals to the order of G. Here $O(G) = 8$

But we have proved that

$$2 \times_{15} 2 \times_{15} 2 \times_{15} 2 = 1 \quad \therefore \quad o(2) = 4$$

$$4 \times_{15} 4 = 1 \quad \therefore \quad o(4) = 2$$

$$7 \times_{15} 7 \times_{15} 7 \times_{15} 7 = 1 \quad \therefore \quad o(7) = 4$$

$$8 \times_{15} 8 = 64 = 4$$

$$8 \times_{15} 8 \times_{15} 8 = 4 \times_{15} 8 = 2$$

$$8 \times_{15} 8 \times_{15} 8 \times_{15} 8 = 2 \times_{15} 8 = 1 \quad \therefore \quad o(8) = 4$$

$$11 \times_{15} 11 = 1 \quad \therefore \quad o(11) = 2$$

Also,

$$13 \times_{15} 13 = 4$$

$$13 \times_{15} 13 \times_{15} 13 = 4 \times_{15} 13 = 7$$

$$13 \times_{15} 13 \times_{15} 13 \times_{15} 13 = 7 \times_{15} 13 = 1 \quad \therefore \quad o(13) = 4$$

$$14 \times_{15} 14 = 1 \quad \therefore \quad o(14) = 2$$

Hence, there is no element $a \in G$ such that $o(a) = o(G) = 8$

$\therefore$ G is not cyclic.

8.25. MORPHISMS

The word '*morphism*' is a combination of various terms like, *homomorphism, isomorphism, actomorphism, endomorphism* etc.

8.25.1. Group Homomorphism

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

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

$$\phi(a \cdot b) = \phi(a) * \phi(b) \quad \forall\ a, b \in G$$

8.25.2. 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 $G \cong G'$.

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

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