4 Monoids and Groups

Algebraic Structure : A non-empty set 'G' equipped with one or more binary operations is called an algebraic structure. Suppose * is a binary operation on G. Then (G, *) is an algebraic structure. (N, +), (I, +), (I, –) are all algebraic structures.

Binary Operation on a Set : Let us consider a non-empty set A and a function $f: A \times A \to A$ is called binary operation A. If * is a binary equation on A, it may be written as $a * b$.

It is denoted by +, –, *, ⊕, Δ, □, ∨, ∧ etc.

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

(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.

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. 1. 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. The operation * on A is associative, if for every $a\ b, c, \in A$, we have $(a*b)*c = a*(b*c)$.

Example 2. 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

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

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 3. Consider the binary operation * and Q, the set of rational numbers defined by :

$$a*b = \frac{ab}{2} \; \forall \; b \in Q$$

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

Sol. 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 def^n.

We have

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

$$= \frac{\frac{ab}{2}.c}{2} = \frac{abc}{4}$$

$$\therefore \quad a * (b * c) = a * (b * c)$$

Hence, * is associative.

(iii) Identity : Consider a non-empty. Set A and a binery operation * on A. The operation * has an identity property if there exists an element, e, in 1 A such that

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

Example 4. 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

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

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

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

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

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 E 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

$$a * a = a\ \forall\ a \in A.$$

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 c cella tion property, if for every $a, b, c \in A$. we have

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

and $$b * a = c * a \Rightarrow b = c \qquad \text{[Right cancellation)}$$

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 oper. ion * is a closed operation on set A.
2. The operation * is an associative operation.

Example 5. 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, *) 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 6. Consider the algebraic system [(0, i], *), 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 7. Let S be a semi-group with an identity element e and if 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 8. Consider a non-empty set S with the operation $a * b = a$

(a) Is the operation associative ?

(b) Is the opera n 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

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

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

$\therefore$ * is not commutative.

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

Consider

$$a * c = b * c \qquad \text{[Using given } a * b = a\text{]}$$
$$\Rightarrow a = b$$

$\therefore$ Right cancellation laws hold.

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

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

Hence, the result.

Example 9. Ley (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

$$= (a * b) * c = a * (b * c) \qquad [\because * \text{ is associative}]$$
$$= a * (c * b) \qquad [\because b * c = c * b]$$
$$= (a * c) * b \qquad [\because * \text{ is associative}]$$
$$= (c * a) * b \qquad [\because a * c = c * a]$$
$$= c * (a * b) \qquad [\because * \text{ is associative}]$$

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

Sub Semi-Group

Consider the semi-group (A, *) and let $B \subseteq A$. Then the system (B, *) is called a sub-semi group, if the set B is closed under the operation *.

For Example, Consider a semi-group (N, +), where N is the set of all natural numbers and + is an addition operation. The algebraic system (E, +) is a subsemi-group of (N, +), where E is a set of all +ve even integers.

Congruence Relation

(P. T. U. E. Tech. May 2005)

An equivalence relation R on the semi-group (S, *) is called a congruence relation if

aRa' and $bRb' \Rightarrow (a * b)\ R\ (a' * b')$

Example 10. Let (I, +) be a semi-group and R is an equivalence relation on I defined by aRb iff $a \equiv b$ (MOD 3).

Sol. If a and b yield the same remainder when divided by 3, then we have 3 divides $a - b$ *i.e.*, $3/a - b$.

Now, if $a \equiv b$ (MOD 3) and $c \equiv d$ (MOD 3) then 3 divides $a - b$ and 3 divides $c - d$. Thus, we can write

$$a - b = 3m \qquad \ldots(1)$$

and

$$c - d = 3n \qquad \ldots(2)$$

$[a/b \Rightarrow b = at \text{ for some } t]$

Here m and n are some integers of I.

Adding (1) and (2), we have

$$(a - b) + (c - d) = 3m + 3n \text{ or } (a + c) - (b + d) = 3(m + n)$$
$$\Rightarrow \quad 3 \text{ divides } (a + c) - (b + d)$$

Example 11. Consider the semi group (1, +), where + is an addition operation. Let $f(x) = x^2 - 2x - 3$ and also let R is a relation on I defined by aRb iff $f(a) = f(b)$. Show whether R is a congruence relation.

Sol. We first show that the relation R is an equivalence relation on the set I.

(i) $f(a) = f(a) \Rightarrow aRa$ *i.e.*, R *is* symmetric

(ii) $aRb \Rightarrow f(a) = f(b) \Rightarrow f(b) = f(a)$ *i.e.*, bRa. Hence R is symmetric

(iii) If aRb, bRc, then $f(b) = f(b)$ and $f(b) = f(c) \Rightarrow (fa) = f(c) \Rightarrow aRc$ *i.e.*, R is transitive

To check whether R is congruence relation or not, we will try to find two pair of num-bers aRb and cRd but $(a + b)\ R\ (c + d)$, if possible. Then we will say R is not a congruence relation.

Thus, we have

$$2R0 \qquad i.e., \qquad f(2) = f(0) = -3$$

and

$$-2R4 \qquad i.e., \qquad f(-2) = f(4) = 5$$

But $(2 + (-2))\ R\ (0 + 4)$ *i.e.*, $0\ R\ 4$

As $f(0) = -3$ and $f(4) = 5$

Hence, R is not congruence relation.

Example 12. Let (S, *) be a commutative semi-group. Show that if $x * x = x$ and $y * y = y$, then $(x * y) * (x * y) = x * y$.

Sol. Take L.H.S. $(x * y) * (x * y)$

$$= (x * y) * (y * x) \qquad [\because (S, *) \text{ is a commutative semi-group}]$$
$$= x * y * y * x = x * y * x \qquad [\because y * y = y]$$
$$= x * x * y \qquad [\because \text{Commutative semi-group}]$$
$$= x * y \qquad [\because x * x = x]$$

Hence, $= (x * y) * (x * y) = x * y$.

Example 13. Let (A, *) be a semi-group. Further more, for every a and b in A, if $a \neq b$ then $a * b \neq b * a$.

(a) Show that for every a in A, $a * a = a$

(b) Show that for every a, b in A, $a * b * a = a$

(c) Show that for every a, b, c in A, $a * b * c = a * c$.

Sol. (a) We know that A is a semi-group.

$\therefore \qquad (a * b) * c = a * (b * c)$

Now putting $b = a$ and $c = a$, we have

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

Since A is not commutative semi-group. i.e., $a * b \neq b * a$,

Hence $\qquad a * a = a$

(b) Let us assume that $b \in A$, then we have

$b * b = b$

Multiplying both sides by a, we get

$a * b * b = a * b$ or $(a * b) * b = a * b$ [$\because$ * is associative]

...(2)

Hence, $a * b = a$ [$\because$ * is associative]

So, $a * b * a = (a * b) * a$ [$\because a * b = a$ from (2)]

$= a * a$ [$\because a * a = a$ from (1)]

$= a * a$ [$\because$ * is associative]

(c) We know that $a * b * c = (a * b) * c$ [$\because a * b = a$ from (2)]

$= a * c$

Monoid

A non-emtpy set together with binary operation * on it is called a monoid if

(i) $a * b \in M \; \forall \; a, b \in M$ [Closure Property]

(ii) $(a * b) * c = a * (b * c)$ [Associative Property]

$\forall \; a, b, c \in M$

(iii) $\exists$ an element $e \in M$ such that. [Existence of Identity]

$e * a = a = a * e \; \forall \; a \in M$, e is called the identity element of M

Every group is a monoid but converse may not be true.

Example 14. Let $Z_+ = \{0, 1, 2, 3, ...\}$ and binary operations * be addition. Determine whether the algebraic system $(Z_+, *)$ is a monoid.

Sol. Closure Property : The operation addition is closed.

[$\because$ if $a \; b \in Z_+ \Rightarrow a + b \in Z_+$]

Associative Property : Let $a, b, c \in Z_+$, then

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

Identity : Clearly '0' is the identity element w.r.t to operation *, as $a + 0 = 0 + a = a$, for all $a \in Z$.

$\therefore$ algebraic system, $(Z_+, +)$ is a monoid.

Sub-monoid

Let $(A, *, e)$ be a monoid and let B be a subset of A. Then set B is a sub-monoid of A, if B is closed under and the identity element of A is an element of B.

Theorem 2. Let $\{M, *)$ be a monoid and S be a non-empty subset of M. Then S is a sub-monoid of M if

(*i*) $x, y \in S \Rightarrow x * y \in S$, *i.e.* S is closed under *.

(*ii*) For each $x \in S$, there exists $e \in S$, such that $x * e = e * x = x$.

Sol. Let S be a sub-monoid of M. Then by def^n, S must be closed under Also for each $x \in S$, there exists $e \in S$, such that $x * e = e * x$.

$\therefore$ (*i*) and (*ii*) hold.

Conversely : Let (*i*) and (*ii*) hold.

From (1), $x, y \in S \Rightarrow x * y \in S$, *i.e.* S is closed under *

Also if $x, y, z \in S$ and $S \subseteq M$, $\therefore x, y, z \in M$

But M is a monoid.

$\therefore \quad x * (y * z) = (x * y) * z, \; \forall \; x, y, z \in S$

i.e. associative property holds in S.

From (ii), S has an identity element.

S is a monoid, But $S \subseteq M$.

S is a sub-monoid of M under operation*

Example 15. Let an algebraic system such that for all a, b in A.

$(a * b) * a = a$

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

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

(*ii*) $a * b = b * a$, if and only if $a = b$. (*P. T U., B. Tech., 2004*)

Sol. (*i*) $a * (a * b) = [(a * b) * a] * (a * b)$ [$\because a = (a * b) * a$] ...(1)

$a * b$, by (1)

(*ii*) Let $a * b = b * a$ ...(2)

As $a = (a * b) * a$ (Given)

$= (b * a) * a$ ...[by (2)]

$= (a * b) * b$ [$\because (a * b) * b = (b * a) * a$]

$= (b * a) b$ ...[by (2)]

$= b$ etc.

Example 16. Prove that for any commutative monoid M, * the set of idempotent element of M forms a submonoid. (*PTU., B. Tech., Dec., 2004*)

Sol. Let S be the set of idempotent elements

i.e. $S = \{x \in M : x * x = x\}$.

To prove S is a sub-monoid.

If $x \in S \Rightarrow x * x = x \in S \Rightarrow x * x \in S$

i.e. S is closed under operation *

Also $e * e = e \Rightarrow e \in S$ *i.e.* S has an identity element, S is a sub-monoid.

Example. 17. Let S be semigroup with identity e and let b and b' be inverses of a. Show that $b = b'$ *i.e.* inverses are uniques, if are they exist. (*PTU., B. Tech., Dec. 2003*)

Sol. As S is a semi group with identity e and b and b' are inverses of a.

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

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

As S is a semi group under * $\therefore$ associativity property holds in S under operation *.

i.e. $b * (a * b') = (b * a) * b'$ [using (1) and (2)]

$\Rightarrow \quad b * e = e * b'$

$\Rightarrow \quad b = b'$.

Example 18. Let (A, *) be a semigroup. Let a be an element in A. Consider a binary operation $\square$ on A, such for every x and y in A.

$x \square y = x * a * y$.

Show that $\square$ is an associative operation. (*P. T U., B. Tech., 2002*)

Sol. $(x \square y) \square z = (x * a * y) \square z = (x * a * y) * a * z$

$= x * a * (y * a * z)$ ...(1) [$\because x, y, z, a \in A$, A is semi group $\therefore$ associative low holds in A.]

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

$= x * a * (y * a * z)$ ...(2)

$\therefore$ From (1) & (2), $\square$ is an associative operation.

Example 19. Let (A, *) be a commutative semi-group. Show that if $a * a = a$ and $b * b = b$, then $(a * a) * (a * b) = a * b$. (*P.T.U., B. Tech., 2002*)

Sol. $(a * a) * (a * b) = a * (a * b)$ [$\because a * a = a$]

$= (a * a) * b$ [$\because$ associative law hold in a semi-group]

$= a * b$ [$\because a * a = a$]

Example 20. Is the set of prime number closed under multiplication or under addition?

Sol. The prime numbers are not closed under either multiplication or addition because product and sum of two primes is not prime as $2.3 = 6$, $3 + 5 = 8$ etc.

Example 21. Show that the set of integers of the form 3K + 1 is closed under multiplication. Is this set a submonoid of (Z, ·, 1).

Sol. Let $a = 3x + 1$, $b = 3y + 1$

then $ab = (3x + 1)(3y + 1)$

$= 3(3xy + x + y) + 1 = 3K + 1$

Thus it is closed.

As $1 = 3.0 + 1$, the identity is included and the set is submonoid.

Group : Let G be a non-empty set together with a binary operation * then the algebraic structure (G, *) is called a group if it satisfies the following :

A non-empty set G together with our operation * on is called a group if

(*i*) $a * b \in G \; \forall \; a, b \in G$ (Closure property)

(*ii*) $(a * b) * c = a * (b * c) \; \forall \; a, b, c \in G$ (Associative Property).

(*iii*) $\exists$ an element $e \in G$ such that $e * a = a = a * e \; \forall \; a \in G$, e is then called the identity element of G w.r.t. *. (Existence of identity)

(iv) If $a \in G$, then $\exists \; b \in G$ such that $a * b = c = b * a$, b is then called the inverse of a and is denoted by a^{-1}. (Existence of Inverse)

Abelian Group : If in addition of above postulates G also satisfies the commutative law.

$a * b = b * a$ for all $a, b \in G$, then G is called an Abelian group.

Example 22. Determine whether the algebraic system (Q, +) is a group where Q is the set of all ratio 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.

Associate 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.

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

Example 23. The set 'I' of all integers with operation defined by $a * b = a + b + 1 \; \forall \; a, b \in I$. Determine whether (I, *) is a group.

Sol. (i) Closure Property. We have $a \in I$, $b \in I$,

$\Rightarrow$ $a + b + 1 \in I$ *i.e.* $a * b \in I$.

$\therefore$ I is closed w.r.t. the operation *.

Associativity. If $a, b, c \in I$, then

$(a * b) * c = (a + b + 1) * c = a + b + c + 1 + 1$

$= a + b + c + 2$

Also $a * (b * c) = a * (b + c + 1) = a + b + c + 1 + 1 = a + b + c + 2$

$\therefore$ $a * (b * c) = (a * b) * c \; \forall \; a, b, c \in I$.

Existence of Left Identity : $e \in I$ will be the identity if $e * a = a \; \forall \; a \in I$

Now $e * a = e + a + 1$

$e + a + 1 = a \Rightarrow e = -1$

Since $-1 \in I$ and we have for any $a \in I$,

$(-1) * a = -1 + a + 1 = a$

$\therefore$ -1 is the left identity element.

Existence of Left Universe : If $a \in I$, then $b \in I$ will be the left inverse of a if $b * a = -1$ (the l, ft idetity)

Now $b * a = -1 \Rightarrow b + a + 1 = -1$

$\Rightarrow$ $b = -2 - a$

Now $a \in I \Rightarrow -2 - a \in I$

Also, $(-2, -a) * a = -2 - a + a + 1 = -1$

$\therefore$ $-2 - a$ is the left universe of a.

Also, $a * b = a + b + 1 = b + a + 1 = b * a$.

$\therefore$ the composition is also commutative. Hence I is an infinite abelian group for the given composition.

Example 24. (i) Show that set I of all integers is a group w.r.t. operation of addition of integers.

(ii) Show that all natural numbers is not a group w.r.t. addition.

(iii) Show that the set Q_0 of all non-zero rational numbers forms a group under the operation multiplication of rational numbers.

Sol. (i) Closure property : We know that the sum of two integers is also an integer *i.e.*, $a + b \in I \; \forall \; a, b \in I$

Thus I is closed w.r.t. addition.

Associativity : We know that addition of integers is an associative composition.

Therefore.

$a + (b + c) = (a + b) + c \; \forall \; a, b, c \in I$

Existence of identity :
The number $0 \in I$. Also we have $0 + a = a = a + 0 \forall a \in I$.
Therefore, the integer 0 is the identity.
Existence of inverse : If $a \in I$, then $-a \in I$.
Also we have,
$$(-a) + a = 0 = a + (-a)$$
Thus every integer possesses additive inverse.
Therefore I is a group w.r.t. addition. Since addition of integers is a commutative composition therefore (I, +) is an abelian group. Also I contains an infinite number of elements. Therefore (I, +) is an abelian group of infinite order.

(ii) Addition is obviously a binary composition in N *i.e.* N *is* closed w.r.t. addition. Also addition of natural numbers is an associative composition. But there exists no natural number $e \in N$ such that
$$e + a = a = a + e \; \forall \; a \in N.$$
For the addition of numbers, the number 0 is the identity and $0 \notin N$.
Therefore, (N, +) is not a group.

(iii) Closure property : We know that the product of two non-zero rational numbers is also non-zero rational number. Therefore, Q_0 is closed w.r.t. multiplication.
Associativity : We know that multiplication of rational numbers is an associative composition.
Existence of identity : The rational number $1 \in Q_0$. Also we have
$$1a = a = a1 \; \forall \; a \in Q_0.$$
$\therefore$ The rational number 1 is the multiplicative identity.
Existence of inverse : If $a \in Q_0$, then obviously $1/a \in Q_0$. Also $(1/a)\, a = 1 = a\,(1/a)$.
Therefore $(1/a)$ is the multiplicative invsrse of a.
Hence Q_0 is a group w.r.t. multiplication
Since $ab = ba \; \forall \; a, b \in Q_0$
$\therefore$ Group is abelian.

Example 25. Let (G, *) be an algebraic system, where G is the set of all non-zero real number and binary operation * be defined by $a * b = \frac{ab}{4}$. Prove that (G, *) is an abelian group.

Sol. Closure. As $a * b = \frac{ab}{4}$, for all $a, b \in G$, is real *i.e.* $a * b \in G$

Associative. Let $a, b, c \in G$, then

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

Also $a * (b * c) = a * \left(\frac{bc}{4}\right) = \frac{a(bc/4)}{4} = \frac{abc}{16}$

$\therefore (a * b) * c = a * (b * c)$, $\therefore$ binary operation * is associative in G.
Identity. Clearly 4 is an identity element of G

As $4 * a = \frac{4a}{4} = a$, $a * 4 = \frac{a4}{4} = a$.

$\therefore$ $a * 4 = 4 * a = a$

Inverse. We note that $16/a$ is inverse of a, where $a \in G$, as $a * (16/a) = \frac{a(16/a)}{4} = 4$, identity elements.

Also $\left(\frac{16}{a}\right) * a = \frac{(16/a)a}{4} = 4$, an identity of G.

$\therefore$ inverse of each $a \in G$, is $16/a$.
Abelian. As for all $a, b \in G$

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

binary operation * is abelian or commutative.
$\therefore$ algebraic system (G, *) is an abelian group.

Example 26. Let G = {0, 1, 2, 3, 4}. Define a composition $\oplus_5$ on G by $a \oplus_5 b = 5$ where c is the least –ve integers obtained as remainder when $a + b$ is divided by 5. Show that (G, $\oplus_5$) is a group.

Sol. For all $a, b \in G$, $a \oplus_5 b \in G$ thus $\oplus_5$ is a binary composition on G (called additive modulo 5)
Associativity : $\forall \; a, b, c \in G$, $(a \oplus_5 b) \oplus_5 c = a \oplus_5 (b \oplus_5 c)$.
Identity : 0 is identity element as $a \oplus_5 0 = 0 \oplus_5 a = a \; \forall \; a \in G$.
Inverse : $\forall \; a \in G$, of $a^{-1} \in G$ s.t. $a \oplus_5 a^{-1} = 0$, identity [$\because 1^{-1} = 4, 2^{-1} = 3, 3^{-1} = 2, 4^{-1} = 1$ etc.]

Example 27. Show that the 4^{th} roots of unity namely 1, –1, i, $-i$ form a group w.r.t. multiplication. that the set $G = (1, \omega, \omega^2)$ is a group w.r.t. multiplication where ω is cube root of unity.

Sol. (i) Let $G = \{1, -1, i, -i\}$.
To show : Multiplication is a composition in G.
We form the composition table
Now we make the following conclusions :

Multiplication	1	–1	i	$-i$
1	1	–1	i	$-i$
–1	–1	1	$-i$	i
i	i	$-i$	–1	1
$-i$	$-i$	i	1	–1

1. Closure property : Since all the entries in the composition table are elements of the set **G, G** is closed w. r. t. multiplication.
Therefore, multiplication is a binary operation on G.

2. Associativity : The elements of G are all complex numbers and the multiplication of complex numbers is associative.

3. Existence of left identity : From the composition table, we see that the row headed by the element 1 just coincides with the top row of the composition table. Thus we have,

$$1(1) = 1$$
$$!(-1) = -1$$
$$1(i) = i$$
$$1\ (-i) = -i$$

In other words we have $1 \in G$ and

$$1a = a\ \forall\ a \in G$$

$\therefore$ 1 is the left identity.

4. Existence of left inverse : We know that the identity element is its own inverse. Therefore, the left inverse of 1 is 1.

From the composition table, we see that in the column headed by -1, the left identity 1 occurs in the row headed by -1 i. e., $(-1)(-1) = 1$.

Therefore, -1 is the left inverse of -1. Similarly they we see that each element of G possesses left inverse.

Hence G is a group w.r.t. multiplication. The number of elements in the set G is 4. Also the multiplication of complex numbers is commutative.

Therefore, G is an abelian group of order 4 w.r.t. multiplication.

(ii) We from the composition table .

Note that $\omega\omega^2 = \omega^3 = 1$

and $\omega^2\ \omega^2 = \omega^3\ \omega = 1.\omega = \omega$

1. Since all the entries in the composition table are elements of the set G, therefore G is closed w.r.t. multiplication.
2. The elements of G are all complex numbers and we know that multiplication of complex numbers is associative.
3. From the composition table, we see that

$$1(1) = 1$$
$$1(\omega) = \omega = \omega(1)$$
$$1(\omega^2) = \omega^2 = \omega^2\ (1)$$

X	1	ω	ω^2
1	1	ω	ω^2
ω	ω	ω^2	1
ω^2	ω^2	1	ω

Therefore, 1 is the identity element.

4. The inverses of 1, ω ω^2 are 1, ω^2, ω to respectively.
5. The multiplication of complex numbers is commutative. The number of elements in the set G is 3.

Hance G is a finite abelian group of order 3.

Example 28. Prove that set G = {0, 1, 2, 3, 4, 5} is a finite abelian group of order 6 w.r.t. multiplication modulo 6.

Sol. *(i)* Let us form the composition table :

We see that all the entries in the composition table are elements of the set G. Therefore. G is closed w.r.t. addition modulo 6 *i.e.* $+_6$.

The composition "$+_6$" is associative.

If $a, b, c \in G$, then

$a +_6 (b +_6 c) = a +_6 (b + c)$ $[\because b +_6 c = b + c \pmod 6]$

= least non-negative , remainder when $a + (b + c)$ is divided by 6

= least non-negative remainder when

$(a + b) + c$ is divided by 6.

$= (a + b) +_6 c = (a +_6 b) +_6 c$ $[\because a + b = a +_6 b \pmod 6]$

$+_6$	0	1	2	3	4	5
0	0	1	2	3	4	5
1	1	2	3	4	5	0
2	2	3	4	5	0	1
3	3	4	5	0	1	2
4	4	5	0	1	2	3
5	5	0	1	2	3	4

Existence of identity :

We have $0 \in G$. If a is any element of G, then from the composition table, we see that

$$0 +_6 a = a = a +_6 0$$

Therefore, 0 is the identity element.

Existence of inverse :

From the composition table, we see that the inverses of 0, 1, 2, 3, 4, 5 are 0, 5, 4, 3, 2, 1 respectively.

For example

$4 +_6 2 = 0 = 2 +_6 4$ implies 4 is the inverse of 2.

The compostion is commutative as the corresponding rows and columns in the composition table are identical.

The number of elements in the set G is 6.

$\therefore$ $(G +_6)$ finite-abelian group of order 6.

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

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

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 $e'e = ee' = e'$

$$e = e'$$

Hence, identity in a group is unique.

Theorem. 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,

$a_1^{-1}\ a = aa_1^{-1} = e$ and $a_2^{-1}a = aa_2^{-1} = e$

Now, $a_1^{-1} = a_1^{-1}\ e = a_1^{-1}\ (aa_2^{-1}) = (a_1^{-1}\ a)a^{2-1} = ea_2^{-1} = a_2^{-1}$

Thus, the inverse of an element is unique.

Theorem. 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

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

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

Theorem. 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 $(ab)(b^{-1} a^{-1}) = [(ab) b^{-1}]a^{-1} = [a(bb^{-1})] a^{-1}$

$= (ae) a^{-1} = aa^{-1} = e$ ...(1)

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

From (1) and (2), we have

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

Theorem : Prove left cancellation law in agroup G holds i.e., $ab = ac \Rightarrow b = c \; \forall \; a, b, e \in G$.

Proof. Consider $ab = ac$.

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

$= (a^{-1} a)c = ec = c$ (Associative Property)

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

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

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

Theroem : Let G be a group and $a\ b \in G$. Then the equation $a * x = b$ has a solution given by $x = a^{-1} * b$.

Proof. Given $a, b \in G$ and G is a group under *, therefore, a^{-1} exists in G

Hence $a^{-1} * b \in G$. G is closed

Consider $a * x = b = e * b$

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

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

$x = a^{-1} * b$ Left cancellation law

Uniqueness. Let the equation $a * x = b$ has two solutions, say, x_1 and x_2 then we have

$a * x_1 = b$

$a * x_2 = b$

(1) and (2) gives $a * x_1 = a * x_2$

$\Rightarrow \quad x_1 = x_2$ Left cancellation law

Z_m THE INTEGERS MODULO m

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

$Z_m = (0, 1, 2, \ldots m-1; +_m, x_m)$ where the operations $+_m$ (we read it as add it and x_m (read as multiplication modulo m) are defined as

$a +_m b$ = remainder after $a + b$ is divided by m

$a \times_m b$ = remainder after $a \times b$ is divided by m.

Finite Indefinite 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.

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 identity element i.e., ({e}).

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

Example 29. Let ({e, x, y} *) be a group of order 3. The table of operation is shown in figure given below :

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

Example 30. Consider an algebraic system ({0, 1} +) where the operation + is defined as shown in figure.

+	0	1
0	0	1
1	1	0

The system ({0, 1}. +) is a group of order 2. In this 0 is identity element and every element is its own inverse.

Theorem. 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 $m \le n$.

Proof : Consider the elements of the group G as $a, a^2, a^3, \ldots\ldots a^{n+1}$.

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 $m = Q - P$

$\therefore \quad a^m = a^{Q-P} = a^Q a^{-P}$

$= a^Q (a^P)^{-1} = a^Q (a^Q)^{-1}$ [$\because a^P = a^Q$]

$= e$

Further, since P, Q are among $n + 1$,

$1 \le P < Q \le n + 1 \Rightarrow Q - P = m \le n$.

Example 31. In the infinite multiplicative group of non-zero rational numbers, the order of every element except the elements 1 and –1 is infinite.

Sol. We have $(-1)^1 = -1, (-1)^2 = (-1)(-1) = 1$ (Identity element)

$0(-1) = 2$

Now $2^1 = 2, 2^2 = 4, 2^3 = 8$ and so on.

Thus there exists no positive integer n such that $2^n = 1$ (Identity element)

Therefore 0 (2) is infinite.

Example 32. In the additive group of integers the order of every element except 0 is infinite

Sol. We have $(-1)^1 = -1, (-1)^2 = (-1)(-1) = 1$ (Identity element)

$0(-1) = 2$

Now $2^1 = 2, 2^2 = 4, 2^3 = 8$ and so on. (Identity Element)

Then ∃ no positive integer n such that $2^n = 1$

Therefore 0(2) is infinite.

Example 33. In the additive group of integers the order of every element except 0 is infinite.

Sol. 0 is the identity element. Therefore $0(0) = 1$ i.e. order of zero is one.

Now $1 \in I$, we have $1(1) = 1, 2(1) = 1 + 1 = 2, 3(1) = 1 + 1 + 1 = 3$ and so on. Thus there exists no positive integer n such that $n(1) = 0$

∴ 0 (1) is infinite.

Example 34. If a, b are elements of a monoid M and $a * b = b * a$. Show that $(a * b) * (a * b) = (a * a) * (b * b)$

Sol. L.H.S. $(a * b) * (a * b) = a * (b * (a * b))$ [By associativity]

$a * ((b * a) * b)$ [By associativity]

$a * [(a * b) * b]$ [Commutativity]

$a * (a * (b * b))$ [Associativity]

$(a * a) * (b * b)$ [By Associativity]

Example 35. Let * be the operation on the set R of real numbers defined by $a * b = a + b + 2ab$.

(i) Find and $2 * 3, 3 * (-5)$ and $3 * \frac{1}{2}$

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

(iii) Find the identity element ?

(iv) Find the inverse ?

Sol. Given that

$a * b = a + b + 2ab$

$2 * 3 = 2 + 3 + 2.2.3 = 5 + 12 = 17$

$3 * (-5) = 3 + (-5) + 2.3.(-5) = -2 - 30 - 32$

$3 * \frac{1}{2} = 3 + \frac{1}{2} + 2.3.\frac{1}{2} = \frac{5}{2} + 3 = 11/2$

(ii) (R, *) is semi-group iff.

$a * (b * c) = (a * b) * c \; \forall \; a, b, c \in R$.

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

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

$= a + b + c + 2bc + 2ab + 2ac + 2abc$

Also $(a * b) * c = (a + b + 2ab) * c$ ...(i)

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

$= a + b + c + 2bc + 2ab + 2ac + 2abc$

From (i) and (ii) we have ...(ii)

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

∴ (R, *) is a semi-group.

Further (R, *) is commutative iff $a * b = b * a \; \forall \; a, b \in R$

Now $a * b = a + b + 2ab = b + a + 2ba = b * a$.

(ii) Let e be identity element of R, then for each $a \in R$, we have

$a * e = a$

$\Rightarrow \quad a + e + 2ae = a$

$\Rightarrow \quad e(1 + 2a) = 0$

$\Rightarrow \quad e = 0$

(iii) Let $b \in R$ is the inverse of a. Then we must have

$a * b = 0$

$\Rightarrow \quad a + b + 2ab = 0$

$\Rightarrow \quad a + b(1 + 2a) = 0$

$\Rightarrow \quad b(1 + 2a) = 0$

$\Rightarrow \quad b(1 + 2a) = -a$

$\Rightarrow \quad b = -\frac{a}{1+2a}; 1 + 2a \neq 0$

Example 36. If G is a group and for $a, b \in G$ then

(i) $(ab)^2 = a^2b^2$ iff G is abelian

(ii) a and $b^{-1}ab$ have equal order.

Sol. (i) Let G be abelian

Then $(ab)^2 = (ab)(ab)$

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

$= a(ab)b$

$= (aa)(bb)$

$= a^2b^2$

Conversely : Let a, b be any two elements of G

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

$\Rightarrow \quad (ab)(ab) = (aa)(bb)$

$\Rightarrow$ $a\,(ba)\,b = a\,(ab)b$

By left cancellation law

$(ba)\,b = (ab)b$

By right cancellation law

$ba = ab\ \forall\ a, b \in G$

Therefore G is abelian.

(ii) Let n and m are orders of a and $b^{-1}\,ab$ respectively.

Now $(b^{-1}\,ab)^2 = (b^{-1}\,ab)\,(b^{-1}\,ab)$

$= b^{-1}\,a\,(bb^{-1})ab$

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

$= b^{-1}\,aab$

$= b^{-1}\,a^2b$

Therefore in general, we get

$(b^{-1}\,ab)^n = b^{-1}\,a^n.\ b = b^{-1}\,eb = e$

$\Rightarrow$ $0\,(b^{-1}\,ab) \le n \Rightarrow m \le n$

$\Rightarrow$ $0\,(b^{-1}\,ab) = m$

Again $O\,(b^{-1}\,ab) \le n$

$(b^{-1}\,ab)^m = e$

$b^{-1}\,a^m b = e$

$b^{-1}\,a^m b = b^{-1}\,b$ [By left cancellation law]

$a^m b = b$ [By right cancellation law]

$a^m = be$

$a^m = e$

$O\,(a) \le m$ ...(ii)

$n \le m$

From (i) and (ii), we have

$n = m$

Example 37. (i) If G is a group such that $a^2 = e$ for all $a \in G$, prove that G is abelian.

(ii) Show that if every element of a group G is its own inverse, then G is abelian.

(iii) If $a, b, c \in G$ and $a * b = c * a$ then $b = c$? Explain your answer.

[P.T.U.B. Tech. Dec. 2006, May 2005]

Sol. (i) Let $a, b \in G$ then $a\,b \in G$ [By closure property]

$(ab)^2 = e$ [By the definition of inverse]

$(ab)\,(ab) = e \Rightarrow (ab)^{-1} = ab$ ...(i)

$b^{-1}\,a^{-1} = ab$

$a^2 = e \Rightarrow aa = e \Rightarrow a^{-1} = a$

Similarly $b^2 = e \Rightarrow b^{-1} = b$

Putting the values of a^{-1} and b^{-1} in (i), we have

$ba = ab\ \forall\ a, b \in G$

Therefore G is abelian.

(ii) Let $a, b \in G \therefore ab \in G$

Since every element is its own inverse [By closure property]

$(ab)^{-1} = ab$

$\therefore$ $b^{-1}\,a^{-1} = ab$

$\Rightarrow$ Also $a^{-1} = a$ and $b^{-1} = b$

Therefore putting the values of a^{-1} and b^{-1} in (i), we get

$ba = ab\ \forall\ a, b \in G \Rightarrow G$ is abelian.

(iii) Given $a, b \in G$

$a * b = c * a$

$b = c$

Given that $a * b = c * a \ne a * c$ unless G is abelian.

Hence the given statement is a false statement. However, the given statement is a true statement if G is an abelian groop. In this case

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

By left cancellation law

$b = c$

Example 38. (i) If $a^2 = a$, $a \in G$, show that $a = e$

(ii) If $a, b \in G$, prove that ab and ba have equal orders.

Sol. (i) Since $a^2 = a$

$\Rightarrow$ $aa = a$

$\Rightarrow$ $aa = ae$

$\Rightarrow$ $a = e$

Thus $a = e$ [By left cancellation]

(ii) We have

$a^{-1}\,(ab)a = (a^{-1}\,a)\,(ba) = e(ba) = ba$

$ba = a^{-1}\,(ab)\,a$

Thus $O\,(ba)$ = order of $a^{-1}\,(ab)a$

$\Rightarrow$ $O\,(ba) = 0\,(ab)$ ...[$O\,(a^{-1}\,ba) = 0\,(b)$]

Sub Group : Let us consider a group $(G, *)$. Also, let $S \subseteq G$; then $(S, *)$ is called a subgroup iff it satisfy the properties of the group.

Example 39. Which of the following subsets of the real numbers is a sub-group of $(R, \cdot, +)$?

(a) the rational numbers

(b) the positive real numbers

(c) $\{k/2, k$ is an integer$\}$

Sol. (a) Closure : If $a, b \in Q$, then $a + b \in Q$.

Associative : If $a, b, c \in Q$, then $(a + b) + c = a + (b + c)$

Identity : $0 \in Q$ is the identity, as for each $a \in Q$, $a + 0 = 0 + a = a$

Inverse : Also from each $a \in Q$, there exists $-a \in Q$ such that $a + (-a) = 0$, identity.

$\therefore$ Q is a subgroup of R.

(b) Let R^+ = set of positive real numbers.

Let $a, b \in R^+$, then $a + b \in R^+$, as sum of two +ve real numbers is a +ve real number.

But inverse of each element $a \in R^+$ under addition does not exist, $\therefore R^+$ is not a subgroup.

Closure : If a and b are nos. of type $k/2$, k *is* an integer, then $a + b$ is also of type $k/2$.

Associative : Also if a, b, c be nos. of type $k/2$, then $a + (b + c) = (a + b) + c$ holds.

Identity. 0 is the identity, as 0 is of type 0/2 and for each a of type $k/2$, $a + 0 = 0 + a = a$.

Inverse : Also for each $a = k/2$, there exists $a^{-1} = -k/2$, such that $a + a^{-1} = 0$, an identity under addition. $\therefore$ Set ($k/2$, k *is* an integer). is a sub graph of R under addition.

Example 40. (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 $(I, +)$.

Theorem. 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 inuerses 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 $a, b, c \in H$ and since $H \subseteq G \therefore a, b, c \in G$

Since elemen s of H are also elements of G

$\therefore$ associativity holds for H. Hence the Theorem.

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

Example 41. Let H_1 and H_2 be subgroup of group G, neither of which contains the other. Show that there exist an element of G belonging neither to H nor H_2.

(P.T.U. B.Tech. May 2003, Dec. 2002)

Sol. Given H_1 and H_2 are subgroups of G. Also $H_1 \not\subseteq H_2$ and $H_2 \not\subseteq H_1$. We show that these exists an element belonging neither to H_1 nor H_2. Let, if possible, the is an element belonging to H_1 and H_2 i.e., $a \in H_1 \cap H_2$.

Now $a \in H_1$ and since H_1 is a subgroup of G $\quad \therefore a^{-1} \in H_1$

But $a \in H_2$ and since H_2 is a subgroup of G $\therefore a^{-1} \in H_2$ ...(1)

(1) and (2) gives $H_1 \subseteq H_2$, a contradiction. ...(2)

Hence the theorem.

Theorem. If H and K are two subgroup of group G, then H∩K is also subgroup of G.

Proof. Let H and K are two subgroups of G. Then $H \cap K \neq \phi$. As at least the identity element e is common to both H and K. In order to Prove that H∩K is a subgroup, it is sufficient to prove that

Now, $\quad a \in H \cap K, b \in H \cap K \Rightarrow ab^{-1} \in H \cap K$.

$a \in H \cap K \Rightarrow a \in H$ and $a \in K$

But H and K are subgroups, therefore

$a \in H, b \in H \Rightarrow ab^{-1} \in H$

and $\quad a \in K, b \in K \Rightarrow ab^{-1} \in H$

Now, $\quad ab^{-1} \in H, ab^{-1} \in K$

$\Rightarrow \quad ab^{-1} \in H \cap K$

Hence, $H \cap K$ is a subgroup of G.

Theorem. Let H be a subgroup of G. Then (a) $H = Ha \Leftrightarrow a \in H$

(b) $Ha = Hb \Leftrightarrow ab^{-1} \in H$ (c) $aH = bH \Leftrightarrow a^{-1}b \in H$ (d) $HH = H$

Sol. $Ha = H$ If $e \in H \Rightarrow ea \in Ha \Rightarrow a \in H$.

Conversely, H Let a $\in$ H. As H sub. group and $h \in H$, $a \in H$ $ha \in H$ [H is closed under multiplication]

$Ha \subseteq H$

Again if $h \in H$, $a \in H$ and since H is a subgroup of G. As $ha^{-1} \in H$

$\Rightarrow \quad (ha)^{-1} a \in Ha$

$h(a^{-1}a) \in ha \Rightarrow he \in Ha$

$h \in Ha$

$H \subseteq Ha$

From (i) and (ii) $Ha = H$

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

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

$a \in Ha = Hb$

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

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

$\Rightarrow \quad (ab^{-1}) \in H$

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

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

$\Rightarrow$ $ab^{-1} b = hb \Rightarrow ae = hb$

$\Rightarrow$ $a = hb$

$\Rightarrow$ $Ha = Hhb = Hb$

(c) Let $aH = bH$ and we show $a^{-1} b \in H$.

Now $a = ae \in aH$

$\Rightarrow$ $a \in aH = bH$

$\Rightarrow$ $a \in bH \Rightarrow b = ah, h \in H$

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

$\Rightarrow$ $a^{-1} b \in H$

Conversely. Let $a^{-1} b \in H \Rightarrow a^{-1} b = h$, where $h \in H$

$\Rightarrow$ $b = aH$

$\Rightarrow$ $ahh = Hb$

$\Rightarrow$ $aH = Hb$

(d) Let $h \in H$. Then by the part a $H = Hh \; \forall \; h \in H$

$\Rightarrow$ $H \subseteq HH \subseteq H$

$\Rightarrow$ $HH = H$

Theorem. (i) If H is any subgroup of a group G, then [P.T.U. B. Tech. Dec. 2002]

HH = H

(ii) A non-empty subset H of a group G is a subgroup of G iff

(a) $a \in H, b \in H \Rightarrow ab \in H$

(b) $a \in H \Rightarrow a^{-1} \in H$, where a^{-1} is the inverse of a in G.

Proof. (i) Let $h_1, h_2 \in HH$ where $h_1 \in H, h_2 \in H$

Since H is a subgroup of G, ...(i)

$\therefore$ $h_1, h_2 \in H \Rightarrow h_1 h_2 \in H$

$\therefore$ $HH \subseteq H$

Again Let h be any element of H

Then $h = he \in HH$ Since $h \in H, e \in H$. ...(ii)

Thus $H \subseteq HH$

From (*i*) and (ii), we have

$HH = H$.

(ii) Necessary condition : Let H be a subgroup of group G. Then H must be closed w.r.t. multiplication i.e. the composition in G.

$a \in H, b \in H = ab \in H$

Let $a \in G$ and Let a^{-1} be the inverse of a in G.

Then the inverse of a in H is also a^{-1}

Since H itself is a group,

$\therefore$ each element of H must possess inverse.

Hence $a \in H \Rightarrow a^{-1} \in H$.

Sufficient part : Let the given conditions hold in H. We show that H forms a group.

Closure property : Since $a \in H, b \in H$

$\Rightarrow ab \in H$

Therefore H is closed with respect to multiplication.

Associativity : The elements of H are the elements of G. Since the composition in G is associative. Therefore the same composition must also be associative in H.

Existence of identity : The identity of the subgroup is the same as the identity of the group.

Now $a \in H \Rightarrow a^{-1} \in H$(by the given condition)

Then $a \in H, a^{-1} \in H \Rightarrow aa^{-1} \in H$

$\Rightarrow e \in H$

Thus e is the identity of H.

Existence of inverse : Since $a \in H \Rightarrow a^{-1} \in H$, therefore each element of H possesses inverse.

Hence H satisfies all conditions in the definition of a group and then H forms a group.

Therefore H is a subgroup of G.

Example 42. G = {0, 1, 2} and define * on G by $a * b = |a - b|$ Is system (G, *) is a group.

Sol. The composition table is

*	0	1	2
0	0	1	2
1	1	0	1
2	2	1	0

Closure. From composition, closure is established.

Identity. As $a * 0 = |a - 0| = a = 0 * a$, 0 is identity.

Inverse. $a * a = |a - a| = 0$ shows each element has its own inverse.

Associativity. But the system (G, *) does not satisfy the associative law.

$1 * (1 * 2) = 1 * 1 = 0$

$(1 * 1) * 2 = 0 * 2 = 2$

$\therefore$ The system (G, *) is not a group.

Example 43. The set Z of integers forms an abelian group w.r.t the usual addition of integer i.e. (Z, +, 0) is an abelian group.

Sol. (i) Closure Property. As sum of integers is a unique integer (thus closure property holds).

(ii) Associativity of Addition. Since $\forall (a, b, c) \in Z, (a + b) + c = a + (b + c)$

(iii) Identity. $\forall \; a \in Z$,

$a + 0 = a = 0 + a$, so 0 (zero) will be the identity.

(iv) Inverse. $\forall \; a \in Z$, these exists $-a \in Z$, s.t

$a + (-a) = 0 = (-a) + a$

$\therefore -a$ is the additive inverse of $a \in Z$.

(v) Commutative. $\forall\ a, b \in Z$,

$$a + b = b + a$$

$\therefore$ the set Z of integers forms an abelian group. It is of infinite order.

Example 44. Let A be the set $\{a, b, c, d\}$ and let * be the operation on 'A' defined by the table given in the table below :

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

Show that (A, *) is an Abelian group of order 4.

Sol. From the table, we observe that for all $x, y \in A$, $x * y \in A$

Associative. Clearly, the operation is both associative and commutative.

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

Identity. When we see the rows and columns labelled with 'a' we see that $x * a = a * x = x\ \forall$ x in A. Thus, 'a' is the identity element in A under *.

Inverse. The identity element 'e' appears exactly once in each row and each column of the Thus shows that each 'x' in A, there is a solution to the equation $b * x = a$ and also solves $x *$ a. Thus every element in A has an inverse.

The opeation * is commutative and so we concluded that (A, *, e) is an abelian group of order 4.

Theorem. If A, B are two subgroups of a group 'G' then AB is a subgroup of G iff AB = BA ?

Proof. Let A and B are subgroups of G. Let AB = BA

To Proove. AB is a subgroup of G. It is sufficient to prove that $(AB)(AB)^{-1} = AB$.

We have $(AB)(AB)^{-1} = (AB)(B^{-1}A^{-1})$

$= A(BB^{-1})A^{-1}$

$= (AB)A^{-1}$ [B is subgroup $\Rightarrow BE^{-1} = B$]

$= (BA)A^{-1}$ [AB = BA]

$= B(AA^{-1})$

$= BA$ [A is subgroup $\Rightarrow AA^{-1} = A$]

$\therefore \quad AB = BA$

$\therefore$ AB is subgroup of G.

Conversely. Suppose that AB is a subgroup.

Then $(AB)^{-1} = AB$

$\Rightarrow \quad B^{-1}A^{-1} = AB$

$\Rightarrow \quad BA = AB$ [B is subgroup $\Rightarrow B^{-1} = B$, Similarly for A, $A^{-1} = A$]

Hence the result.

Example 45. 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, $a, b = \frac{ab}{2}$ 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.

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

Similarly, $a * e = a$

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

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

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

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

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

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 46. 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 $n * m = \max.(n, m) \in Z \; \forall \; n, m \in Z$

Hence * is closed.

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

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)

Hance * 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 47. 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.

Write three distinct groups (G, ⊗) where G ⊂ S and G has 2 elements.

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

⊗	0	1
0	0	0
1	0	1

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

$$(a \otimes b) \otimes c = a \otimes (b \otimes c) \text{ e.g., } (0 \otimes 1) \otimes 1 = (0) \otimes = 0$$

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}, ⊗) is not a group.

(ii) The three distinct groups (G, ⊗), where G ⊂ S and G has 2 elements is as follows

(a) ({1, 3}, ⊗) (b) ({1, 5}, ⊗) (c) ({1, 7}, ⊗).

Example. 48. Determine whether a semi-group with more than one idempotent element can be a group.

Sol. Let (A, *) be a semi-group with two idempotent elements a and b $(a \neq b)$. Then we have

$$a * a = a \quad ...(1)$$

$$b * b = b. \quad ...(2)$$

Now assume that A is a group with identity element e.

Then, $a * e = a$ and $b * e = b$

From (1) and (2),

$a * e = a = a \neq a \Rightarrow e = a$ [Left Cancellation Law]

Also $b * e = b = b \neq b \Rightarrow e = b$ [Left Cancellation Law]

$a = e = b$

which is a contradiction to $a \neq b$.

Hence (A, *) can not be group.

Example 49. Let (G, o) be a group. Show that if (G, o) is an Abelain group then, $(o\ b)^2 = a^2\ o\ b^2$ for all a and b in G.

Sol. Let us assume G is an Abelian group, then

$$(a\ o\ b)^2 = (a\ o\ b)\ o\ (a\ o\ b) = a\ o\ (b\ o\ a)\ o\ b \quad [o \text{ is associative}]$$

$$a\ o\ (a\ o\ b)\ o\ b = (a\ o\ a)\ o\ (b\ o\ b) = a^2\ o\ b^2 \quad [\text{G is abelian}]$$

Hence, $(a\ o\ b)^2 = a^2\ o\ b^2 \; \forall \; a, b \in G.$

Example 50. 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 group of G.

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

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

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 $AB = \begin{pmatrix} a_1 & 0 \\ c_1 & d_1 \end{pmatrix}\begin{pmatrix} a_2 & 0 \\ c_2 & d_2 \end{pmatrix} = \begin{pmatrix} a_1a_2 & 0 \\ c_1a_1 + d_1c_2 & d_1d_2 \end{pmatrix} \in H$

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

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

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

Hence H is a subgroup of G.

Example 51. 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 statement of H has its inverse. Therefore H is a subgroup of G under multiplication.

Example 52. Consider the group under +. Let E The set of event integer. Then show that E is a subgroup integer +.

Sol. Given $E = [2m : m \in Z\}$ i.e., the set of even integers. Clearly

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

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

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

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

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

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 54. 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.

Cosets. Consider an algebraic system (G, *) where * a binary operation. Now, if (G, *) is a group and let a be an element of G and H be a subgroup of 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 $e * H = H * e = H$

Example 55. Let $H = \{7k, k \in Z\}$ be a subgroup of group G = (Z, +), where Z is set of integers. Determine cosets of H in G.

Sol. The set Z has 7 different cosets (left or right) of H, which are given below :

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

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

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

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

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

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

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

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

All other cosets coincides with any one of fhe cosets given above.

Example 56. Let G (Z, +) be a group where Z is the set of all integers and binary operation is additional.

Let H = E = {....., –4, –2, 0, 2, 4, 6, ...} be a subgroup of G, where E is set of left cosets of H in G.

Sol. We know that Z = {....., –2, –1, 0, 1, 2, ...}

H = {.... –4, –2, 0, 2, 4, 6....}

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

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

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

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

There is no other distinct left cosets, as any other cosets coincides with above cosets.

$\therefore$ There are two distinct left cosets of H in G. H & 1 + H.

Theorem : (i) Let G be a group and H be a subgroup of G, then $b \in aH$ iff $aH = bH$
(ii) If G be a group and H be a subgroup of G, then $a \in Hb$ iff $Ha = Hb$.

Proof : (*i*) Since $b \in aH$, then $b = a\,h_1$ for $h_1 \in H$.

$\Rightarrow \quad a = bh_1^{-1}$

The for any $h \in H$

$bh = (ah_1)\,h = a(h_1\,h) \in a\,H$

Therefore $b\,H \subseteq aH$ ...(i)

Again, for any $h \in H$,

$ah = (bh_1^{-1})h$

$= b\,(h_1^{-1}\,h) \in b\,H$

$\Rightarrow \quad aH \subseteq bH$ ...(ii)

From (*i*) and (ii), we have

$aH = bH$

Conversely Let $aH = bH$

Since $b \in b\,H$

$b \in aH.$

(*ii*) Since $a \in Hb$

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

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

$\Rightarrow \quad H\ ab^{-1} = H$ ...[HH = H]

$\Rightarrow \quad H\ ab^{-1}\ b = Hb$

$\Rightarrow \quad Ha\ (b^{-1}\ b) = Hb$

$\Rightarrow \quad Ha = Hb$

Conversely Let $Ha = Hb$

Since $a \in H\,a$

$\therefore \quad a \in H\,b$ ...[Ha = Hb]

Theorem : Two left (right) cosets of a subgroup H of a group G are either disjoint or identical.

Proof : Let H be a subgroup of G and let aH, bH be two left cosets of H in G. If $aH \cap bH = \phi$ we are done.

Let us suppose that $aH \cap bH \neq \phi$

Let $C \in aH$ and $C \in bH$

Then $C \in aH$ and $C \in bH$

Let $C = ah_1$ and $C = bh_2$ where $h_1, h_2, \in H$

$\therefore \quad ah_1 = bh_2$

$\Rightarrow \quad ah_1\ h_1^{-1} = bh_2\ h_1^{-1}$

$\Rightarrow \quad a\ e = bh_2\ h_1^{-1}$

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

Since H is a subgroup

$\therefore \quad h_2\ h_1^{-1} \in H$

Let $h_2\ h_1^{-1} = h'$

Then $a = bh'$

Now $aH = bh'\ H = b(h'\ H) = bH$

Then $aH = bH$ $[h' \in H \Rightarrow h'\ H \in H]$

Hence two left cosets are identical if they are not disjoint. Thus either $aH \cap bH = \phi$ or $aH = bH$.

Lagrange's Theorem

If G is a finite group and H is a subgroup of G, then O(H) | O(G).

[P.T.U.B. Tech. Dec. 2007, Dec. 2006, May 2006, Dec. 2003]

Proof : Let G be a finite group and H be a subgroup of G.

Let $O(H) = t$

Let $h_1, h_2, \ldots h_t$ be the t members of H.

Let $a \in G$.

Then Ha is a right coset of H in G.

$\therefore \quad Ha = \{h_1a, h_2\ a, \ldots, h_ta)$

Ha has t distinct members,.

$h_ta = h_ja \Rightarrow h_i = h_j$

Therefore each right coset of H in G has distinct members. Also we know that any two distinct nght cosets of H in G are disjoint.

Since G be a finite group, the number of distinct right cosets of H in G will be finite.

Let the number of distinct right cosets of H in G = K

Then $G = Ha_1 \cup Ha_l \cup \ldots \cup H\ a_k$

$\Rightarrow \quad O(G) = O(Ha_1) + O\ (Ha_2) + \ldots + O\ (H\ a_k)$

$\Rightarrow \quad O(a) = O\ (H) + O\ (H) + O\ (H) + \ldots + O\ (H)$ [K times]

[$\because$ There is always a one-one onto mapping between any two right cosets of H in G which implies that 0 (H) = O (Ha)]

$\Rightarrow \quad O\ (G) = Kt$

$\Rightarrow \quad O(G) = K.O(H)$

Hence O (H) divides O (G) i.e. O (H) |0 (G).

Index of Subgroup

Let G be a group and H, a subgroup of G. The index of H in G is the number of distinct right (left) cosets of H in G. It is denoted by $i_G(H)$ or [G : H].

Theorem : (i) If G is a finite group and H is a subgroup of G. Then

$$[G : H] = \frac{O(G)}{O(H)}$$

***(ii)* If G is a finite group of order *n* show that $a^n = e$ for any element $a \in G$.**

Proof. By Lagrange's theorem, we have

$$O(G) = K.O(H)$$

where K is the number of distinct right cosets of H in G.

$$\Rightarrow \quad K = \frac{O(G)}{O(H)}$$

$$\Rightarrow \quad [G : H] = \frac{O(G)}{O(H)}$$

(ii) Since G is a finite group and n = order of finite group G. Let $a \in G$ has order m then $a^m = h$. the order of each element in a finite group is finite.

Also we know that the order of every element of a finite group is a divisor of the order group. By Lagrange's theorem

$\therefore \quad O(a) \mid O(G)$

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

$\Rightarrow \quad a^n = a^{mr}$

$= (a^m)^r$

$= (e)^r = e.$

$\therefore \quad a^n = e.$

Hence the theorem.

Cyclic Group

[P.T.U.B. Tech. Dec. 2009, Dec. 2002]

A group G is called cyclic if, for some $a \in G$, every element $x \in G$ is of the form a^m, where m is some integer. The element a *is* then called a generator of G. There may be more than one generators of a cyclic group. If G is cyclic group generated by a, then we shall write $G = \{a\}$ or $G = (a)$.

Theorem : (i) Every cyclic group is abelian. ***[P.T.U.B. Tech. May 2006, May 2005]***

(ii) If a is generator of a cyclic group G, then a^{-1} is also generator of G. ***[Imp.]***

(iii) Every group of prime order is cyclic.

(iv) If a finite group of order n contains an element of order n, the group must be cyclic.

Proof : (i) Let $G = \{a\}$ be a cyclic group generated by a.

Let x, y be any two elements of G.

Then there exist integers r and s such that $x = a^r, y = a^s$.

Now $\quad xy = a^r a^s = a^{r+s}$

$= a^{s+r}$

$= a^s . a^r = yx$

Thus we have

$xy = yx \; \forall \; x, y \in G$

Therefore, G is abelian.

(ii) Let $G = \{a\}$ be a cyclic group generated by a.

Normal Subgroup. A subgroup H of group G is called normal subgroup of G if every $g \in G, h \in H$

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

Example 57 : Let G be a group of two invertible matrices $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$; $ad - bc \neq 0$ under matrix multiplication. Let $H = \left[\begin{pmatrix} a & b \\ c & d \end{pmatrix} : ab \neq 0\right]$. 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

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

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

$\Rightarrow$ 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 multiplication 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

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

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

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

Example 58. 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 $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ where $ad \neq 0$. Show that H is a subgroup of G, but not a normal subgroup.

Sol. Let A, B $\in$ H such that

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

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

$$= \begin{pmatrix} a_1 a_2 & 0 \\ c_1 a_2 + d_1 c_2 & d_1 d_2 \end{pmatrix} \in H$$

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

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

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

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

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

Theorem. Every subgroup of an abelian group is normal.

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

$ghg^{-1} = gg^{-1}h$ $\quad h \in H \subseteq G \Rightarrow h \in G$

$= eh$ Also, $h g^{-1} \in G$ and

$= h \in H$ since G is abelian

$\Rightarrow$ $ghg^{-1} \in H \ \therefore \ hg^{-1} = g^{-1} h$

Hence, H is a normal subgroup of G.

Theorem. Let H be a subgroup and K be a normal subgroup of a group G. Show that is a subgroup of G.

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

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

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 $k_1 \in K$,

$\therefore$ $h_2^{-1} k_1 h_2 \in K$

$\Rightarrow$ $(h_2^{-1} k_1 h_2) k_2 \in K$

$\Rightarrow$ $h_1 h_2 (h_2^{-1} k_1 h_2) k_2 \in HK$

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 $k_1 \in K$

$\Rightarrow$ $k_1^{-1} \in K$

Since K is a normal subgroup of G

$\therefore$ $h_1 k_1^{-1} h_1^{-1} \in K$

$\Rightarrow$ $h_1^{-1} (h_1 k_1^{-1}) h_1^{-1} \in HK$

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

Finally, $e \in H, e \in K \Rightarrow e \, . \, e \in HK \Rightarrow e \in HK$

Thus HK is a subgroup of G.

Theorem. 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

$aHa^{-1} = H$

$\Leftrightarrow$ $(aH a^{-1})a = Ha$

$\Leftrightarrow$ $aH (a^{-1}a) = Ha$

$\Leftrightarrow$ $aHe = Ha$

$\Leftrightarrow$ $aH = Ha$

Theorem. Let G is a group and H is a normal subgroup of G. Let G/H denotes the collection of right (left) cosets of H in G. Show that G/H is a group under the coset multiplication defined by

$$aHbH = abH \ \forall\ a, b \in G$$

Proof. (i) Closure Property. By definition, $G/H = \{aH : a \in G\}$

Let $aH, bH \in G/H$ and consider

$(aH)(bH) = a(Hb)H = a(bH)\,H \mid Ha = aH \Leftrightarrow H$ is normal in G

$= (ab)\,HH$

$= abH \quad |HH = H|$

Hence coset multiplication is well-defined *i.e.*, G/H is closed under coset multiplication.

(ii) Associativity. Let $aH, bH, cH \in G/H$ for all $a, b, c \in G$ |Using (i)|

Consider $aH\,(bH\,cH) = aH\,(bcH) = abcH$

Also $(aHbH)\,cH = (abH)\,cH = abcH$

$\Rightarrow$ $aH\,(bHcH) = (aHbH)cH$

Thus associativity holds in G/H. $|HH = H|$

(iii) Identity. Let $aH \in G/H$ for $a \in G$.

Consider $(aH)H = a(HH) = aH$

$\Rightarrow$ H is the identity element of G/H.

(iv) Inverse. Let $aH \in G/H$ and consider

$(a^{-1}H)(aH) = (a^{-1}a)\,H = eH = H$

i.e., $a^{-1}H$ is the inverse of aH

Thus G/H is a group under coset multiplication.

Theorem. The intersection of two normal subgroups of a group is a normal subgroup. **[P.T.U. *B. Tech. May 2007, May 2006, May 2010*]**

Proof. Let H and K be two normal subgroups of group G.

Since H and, K are subgroups of G.

$\therefore$ H$\cap$K is also subgroup of G. g be the el of G

Now we shall prove that H$\cap$K is a normal subgroup of G.

Let g be any element of G and h be any element of HnK.

We have $h \in H \cap K$

$\Rightarrow$ $h \in H$ and $h \cap K$.

Since H is a normal subgroup of G, ...(1)

$\therefore$ $g \in G, h \in H \Rightarrow ghg^{-1} \in H$

similarly K is a normal subgroup of G,

$\therefore$ $g \in G, h \in K$ ...(2)

$\Rightarrow$ $ghg^{-1} \in K$

From (1) and (2), we get

$ghg^{-1} \in H \cap K$

Thus we have

$g \in G, h \in H \cap K$

$\therefore$ $ghg^{-1} \in H \cap K$

Hence H$\cap$K is a normal subgroup of G.

Quotient Group. Let 'G' be a group and H is a normal subgroup of 'G'. Let G/H denotes the set of right (Left) cosets of H in G. Then G/H is called the quotient group or factor group under the coset multiplication defined by $(aH)(bH) = abH$.

Example 59. Let G be the group of all 2×2 matrices over reals of type $\begin{bmatrix} a & b \\ c & d \end{bmatrix}$, where $ad \neq 0$ under multiplication and let N be a subgroup of G containing members of type $\begin{bmatrix} 1 & b \\ 0 & 1 \end{bmatrix}$. Show that quotient group G/N is abelian.

Sol. Here $G = \left[\begin{bmatrix} a & b \\ 0 & d \end{bmatrix}, ad \neq 0\right]$

We can easily shot that G will form a group under matrix multiplication $\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$ will be identity element and $\begin{bmatrix} 1/a & -b/ad \\ 0 & 1/d \end{bmatrix}$ will be the inverse of any element $\begin{bmatrix} a & b \\ 0 & d \end{bmatrix}$. Also G is not abelian.

Also we can prove that if $x, y \in N$, and each element has its inverse and $\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$ is its identity.

$\Rightarrow$ N is a subgroup of G.

Let N be the subset which contains members of the type $\begin{bmatrix} 1 & b \\ 0 & 1 \end{bmatrix}$. Then N is a sub-group of G.

Also it is normal as the product of type

$$\begin{bmatrix} a & b \\ 0 & d \end{bmatrix}\begin{bmatrix} 1 & k \\ 0 & 1 \end{bmatrix}\begin{bmatrix} 1/a & -b/ad \\ d & 1/d \end{bmatrix} = \begin{bmatrix} 1 & ak/d + b/d - b/d \\ 0 & 1 \end{bmatrix} \in N$$

[$\because$ H is normal in G if $g^{-1}hg \in H$, for all $h \in H, g \in G$]

Thus we obtain the quotient group G/N. We will show G/N is abelian.

Let Nx, Ny$\in$G/N. be any elements, then $x, y \in G$.

Let $x = \begin{bmatrix} a & b \\ 0 & d \end{bmatrix}$, $y = \begin{bmatrix} c & e \\ 0 & f \end{bmatrix}$

$\frac{G}{N}$ will be abelian if $Nx\,Ny = Ny\,Nx$ (right coset = left coset)

$\Rightarrow$ $Nxy = Nyx$

$\Rightarrow$ $xy\,(yx)^{-1} ; \in N \begin{bmatrix} Nx\,Ny = x\,N\,N\,y \\ = x\,N\,y = N\,xy \end{bmatrix}$ ($\because$ NN = N)

$\Rightarrow$ $xy\,x^{-1}\,y^{-1} \in N$

Also we need to see ($\because$ H is normal of G if $Ha = aH$ for all $a \in G$)

$\begin{bmatrix} a & b \\ 0 & d \end{bmatrix}\begin{bmatrix} c & e \\ 0 & f \end{bmatrix}\begin{bmatrix} 1/a & -b/ad \\ 0 & 1/d \end{bmatrix}\begin{bmatrix} 1/c & -e/ad \\ 0 & 1/f \end{bmatrix}$ is a matrix of type $\begin{bmatrix} 1 & t \\ 0 & 1 \end{bmatrix}$

Cyclic Group. A group G is called a cyclic group if there exists an element $a \in G$ such that every element of 'G' can be expressed as a power of 'a'. The element 'a' is called the generator of G. [Dec. 04]

If G is cyclic, we write $G = \langle a \rangle$.

Example 60. If G = {1, –1, i, –i} then G is a cyclic group generated lay *i*.

Sol. Since $i = i$, $i^2 = -1$, $i^3 = -i$, $i^4 = 1$

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.

Example 61. The group of integers Z is cyclic under addition.

Sol. $Z = \{0, \pm1, \pm2, \pm3, ...\}$

As 1 = 1

1 + 1 = 2

1 + 1 + 1 = 3

1 + 1 + 1 + 1 = 4

⋮

1 + 1 + ...n times = n etc.

$\therefore$ we see that every element of Z is of the form $n(1)$. Thus Z is cyclic group. Hence $Z = \langle 1 \rangle$. Also $Z = \langle -1 \rangle$.

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

Proof. Let G is a cyclic group and 'a' be its generator i.e. $G = \langle a \rangle$.

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 $s \in Z$

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

Hence a^{-1} is a generator. [May, 06, 05]

Theorem. Every cyclic group is abelian

Proof. Let 'G' be a cyclic group and 'a' be its generator *i.e.* $G = \langle a \rangle$

Let $g_1 \in G$ then $g_1 = a^r$ for some $r \in Z$.

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

Now $g_1 g_2 = a^r a^s = a^{r+s}$

$= a^{s+r}$

$= a^s, a^r$ [$\because r + s = s + r$]

$= g_2 g_1$

$\therefore$ G is abelian i.e. every cyclic group.

Theorem. Prove that every order a prime is a cyclic.

Sol. Let G be a group of order p, where p is a prime.

Therefore $0(G) \geq 2$ (since 2 is the least prime)

$\therefore$ $\exists\, a \in G$ such that $a \neq e$ (identity element of G)

$\therefore$ $0(a) \geq 2$. Let $o(a) = m$

Suppose $H = \langle a \rangle$, be a cyclic group generated by a.

Thus H will be a cyclic subgroup of G of order m.

$\therefore$ By Lagrange's Theorem.

$o(H)/o(G)$ *i.e.* m/p but p is a prime and $m \geq 2$

$\Rightarrow$ $m = p$

i.e., $o(H) = o(G) \Rightarrow H = G$.

But H is cyclic group. $\Rightarrow$ G is also cyclic group.

Theorem. 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, $o(H) | o(G) \Rightarrow m/p$

$\Rightarrow$ $P = 1$ or $P = m$

But $P \neq 1$ $\therefore$ $P = m$

i.e. $o(H) = m = p \Rightarrow$ H is a subgroup of prime order and hence cyclic.

Also, $o(G) = m$.

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

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

$\langle a \rangle$ contains the identity element e closed under group operation, contains inverse.

$\therefore$ $\langle a \rangle$ is a subgroup of G and is called the cyclic group generated by a.

Example 62. 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).

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

$\therefore$ $3^{-1} = 5$

$6^{-1} = 6$

(c) We have $2 = 2$

$2 \times_7 2 = 4$

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

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

Hence $\langle 2 \rangle$ = 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 $\langle 3 \rangle = \{1, 2, 3, 4, 5, 6\} = G$

(d) Since $o(3) = 6 = o(G)$ $\Rightarrow$ G is cyclic. Recall that a group G is cyclic if element $a \in G$ such that $o(a) = o(G)$.

Example 63. 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

i.e., $5 \times_{12} 7 = 35 = 11$ 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 $o(a) = o(G)$.

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.

Theorem. The order of a cyclic group is same as the order of its generator.

Sol. If n be the order of generator a, then $a^n = e$

where n is the least +ve integer.

Now we shall show that the group G consists of exactly n elements namely.

$a, a^2, a^3 \ldots\ldots, a^n = e$ ...(1)

Let k be any integer greater than n and G contains the element a^k.

By division algorithm $k = nq + r$, where $0 \le r < n$.

$\therefore$ $a^k = a^{nq+r} = a^{nq}.\ a^r = (a^n)^q.a^r = a^r.$ [$\because a^n = e$]

But r is less than n and a^r is contained in (1) and hence the set shall not contain more than n elements. Now we shall establish that it contains n elements by showing that no two elements of (1) are same. For if possible let $a^r = a^q$, where $0 < r < n$

$a^r . a^{-r} = a^q.a^{-r} \Rightarrow a^0 = a^{q-r}$

$\therefore$ $a^{q-r} = e$, where $q - r$ is + ve integer less than n.

But this is not possible because n is the order of a and as such there can not be any other integers, $q - r$ less than n such that $a^{q-r} = e$. Hence $a^{q-r} \neq e$ and consequently $a^r \neq a^q$ showing thereby that all the elements listed in (1) are distinct.

$\therefore$ the group G consists of exactly n elements.

Example 64. How may generator are there of the cyclic group of order 8.

Sol. Let 'a' be generator of order 8. $\therefore$ $o(a) = 8$

We write $G = \{a, a^2, a^3, a^4, a^5, a^6, a^7, a^8\}$

As 7 is prime to 8

$\therefore$ a^7 is also a generator of G, As 5 is prime to 8

$\therefore$ a^5 is also generator of 'G'.

As 3 is prime to 8. $\therefore$ a^3 is also generator of 'G'.

As 3 is prime to 8. $\therefore$ a^3 is also a generator of G.

($\because$ If a cyclic group is generated by an element 'a' of order 'n' then a^m is a generator iff $(m, n) = 1$

Thus, there are only four generators of

i.e. a, a^3, a^5, a^7.

Example 65. Let G be a reduced residue system modulo 15, *i.e.* G = {1, 2, 4, 7, 8, 11, 13, 14}.
(i) Find the multiplication table of G.
(ii) Find 2^{-1}, 4^{-1}, 7^{-1}, 8^{-1}
(iii) Prove that G is a group under multiplication modulo 15.
(iv) Find the orders and subgroups generated by 2, 7 and 11.
(v) Is G cyclic ?

Sol. (*i*) $a \times_{15} b$ = remainder where *ab is* divided by 15.

The multiplication table of G is

$\times_{15}$	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	13	4	2
14	14	13	11	1	8	4	2	1

(ii) The identity element of G is 1

$\therefore 2^{-1} = 8, 4^{-1} = 4, 7^{-1} = 13, 8^{-1} = 2$

[Also $11^{-1} = 11, 13^{-1} = 7, 14^{-1} = 14$]

(iii) (a) Closure. From above table, G is closed under multiplication modulo 15.

(b) Associative. If $a, b, c \in G$, then $(ab)\ c = a(bc)$

[$\because (2.4).7 = 8.7 = 11, 2.(4.7) = 2(28) = 2(13) = 26 = 11$ etc.]

(c) '1' is the identity of G.

(d) Also inverse of each element of G exists. [by part (1)]

$\therefore$ G is a group under multiplication modulo 15.

(iv) We know that a group G is cyclic, if there exists an element $a \in G$ such that $O(a) = O(G)$

As $O(1) = 1, O(2) = 4, O(4) = 2, O(7) = 4, O(8) = 4$

$O(11) = 2, O(13) = 4, O(14) = 2$

$\therefore$ There is no element of G whose order = 8

$\therefore$ G is not cyclic.

Theorem. Every proper sub-group of an infinite cyclic group is infinite.

Proof. Let $G = \{a\}$ be an infiite cyclic group. Let H be a proper sub-group of G. Then H is cyclic and if m is the least positive integer such that $a^m \in H$, then $H = \{a^m\}$.

Suppose H is a finite group of order *p*. Since a^m is a generator of H, therefore $(a^m)^p = e$.

i.e. $a^{mp} = e$, when $mp > 0$.

$\therefore$ Order of *a is* finite and consequently G is finite, contrary to the hypothesis. Hence H must be an infinite cyclic sub-group of G.

Note 1. If $G = < a >$ we say that G is generated by *a*, *a* generates G and G is cyclic.

Note 2. If the operation on G is additive, then $< a > = (na.\ n \in Z)$

The following proposition helps us to find the generators of the group $(Z_m, +, [o])$

Example 66. Show that the group {{1, 2, 3, 4, 5, 6}, $\times_7$} is cyclic. How many generators are there ?

Sol. There exists an element $a \in G$, such that $O(a) = 6$ *i.e.* $O(a) = O(G)$, then G will be a cyclic group will be a generator of G.

Clearly $O(3) = 6$. [$\because 3^1 = 3, 3^2 = 2, 3^3 = 3^2 \times_7 3 = 2 \times_7 3 = 6, 3^4 = 3^3 \times 7^3 = 6 \times_3 3 = 4, 3^5 = 4 \times_7 3 = 5, 3^6 = 5 \times_7 3 = 1$, *i.e.* the identity element.]

$\therefore$ G is cyclic and 3 is a generator of G, we can write $G = \{3, 3^2, 3^3, 3^4, 3^5, 3^6\}$

As (5, 6) = 1. $\therefore$ 3^5 i.e. 5 is also a generator of G.

Example 67. Find the number of generators of a cyclic group of order 10.

Sol. Let $G = \{a\}$ be a cyclic group of order 10, generated by A, $O(a) = O(G) = 10$

$\therefore$ $G = \{a, a^2, a^3 \ldots, a^{10} = e\}$

Now a^k is a generator of G *i.e.* $k < 10$ and H.C.F. of *k* and 10 is 1.

$\therefore$ numbers Less than 10 and relatively prime to 10 are, 1, 3, 7, 9.

$\therefore$ a, a^3, a^7, a^9 are the generators of G.

$\therefore$ G has four generators.

Group Homomorphism. A mapping ϕ from a group G into a group G' is said to be a homomorphism if

$\phi(ab) = \phi(a)\ \phi(b)\ a, \forall\ b \in G$.

G' is said to be a homomorphic image of G.

Kernal *f*. If *f* is a homomorphism of G to G', then Kernal *f* is the set defined by

$\text{kerf} = \{x \in G : f(x) = e', e' \in G$

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

$I_m(f) = \{b \in G' : f(a) = b$ for $a \in G\}$

where *f* is a homomorphism of G to G'. It is also known as 'image *f*.

Theorem. Let $f : G \to G'$ is a group homomorphism. Then

(a) $f(e) = e', e \in G, e' \in G'$

(b) $f(a^{-1}) = (f(a))^{-1}\ \forall\ a \in G$

Proof. (a) Given $f : G \to G'$ is a homomorphism from G to G'. For $x \in G$, consider

$f(x)e^1 = f(x)\ |e^1$ is identity of G|

$= f(ex) = f(x)\ (fe)$ (*f* is homomorphism)

$e^1 = f(e)$ (Left cancellation Law)

$\Rightarrow$ $f(e) = e'$

(b) From the part (*a*),

$e' = f(e) = f(aa^{-1})$

$= f(a)\ f(a^{-1})$ (*f* is homomorphism)

$f(a)\, f(a^{-1}) = e'$

$(f(a))^{-1} f(a)\, f(a^{-1}) = (f(a))^{-1} e'$

$f(a^{-1}) = (f(a))^{-1}$

Theorem. Let f be homomorphism of a group G to a group G′ Let Im(f) be the homomorphism image of G in G′. Then Im(f) is a subgroup of G′.

Proof. By definition. $Im(f) = (f(x) : x \in G)$

i.e. $Im(f) \neq \phi$, we first show that Im(f) is a subgroup of G′. Let $x', y' \in Im(f)$

$\therefore$ There exists $x, y \in G$ such that $f(x) = x', f(y) = y'$

Consider $x'y'^{-1} = f(x)\,(f(y))^{-1}$ (f is a homomorphism)

$= (f(xy^{-1}) \in Im(f)$ ($x, y \in G$ and G is a group $\therefore xy^{-1} \in G$)

$\Rightarrow \quad x'\, y'^{-1} \in Im(f)$

$\Rightarrow$ Im(f) is a subgroup of G′.

Example 67. Let G be agroup of real numbers under addition and let G′ be the group of positive real numb - under multiplication. Define $f : G \to G'$ 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 $f: G \to G'$ is homomorphism.

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

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

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 G′ is isomorphism and the groups G and G′ are isomorphic i.e.

Example. 68. Let $f : G \to G'$ be defined by $f(Z) = |Z|$ where G = group of non-zero complex numbers under multiplication and G′ = group of non-zero real numbers and multiplication. Show that f is a group homomorphism. Also describe geometrically the Kernal k of the homomorphism f.

Sol. Let $Z_1, Z_2, \in G$ be any two non-zero complex numbers. Consider

$$f(Z_1\, Z_2) = |Z_1\, Z_2| = |Z_1|\,|Z_2| = f(Z_1)\, f(Z_2)$$

f is a group homomorphism.

Also by definition,

Kernel $f = \{Z \in G : f(Z) = 1,\ 1$ is the identity of G′$\}$

$= \{Z \in G : |Z| = 1\}$

which is a circle with unit radius.

Example 69. Let (G, *) be a group and a $\in$ G. Define f : G $\to$ G by $f(x) = a * x$

(a) prove that 'f' is a bijection

(b) on the basis of part (1), describe a set of bijection on the set of integers. [May '05]

Sol. Given G is a group under * and $a \in G$. Also $f: G \to G'$ is defined by $f(x) = a * x\ \forall\ x \in G$.

(i) We have to prove that f is a bijection i.e. f is one-one and onto.

***f* is one-one :** Let $x, y \in G$ s.t. $f(x) = f(y)$

$$a * x = a * y$$

$$x = y$$

[By left cancellation law]

f is one-one.

***f* is onto :** Let $a, x \in G$ and since G is a group under *, G must be closed under i.e., $a * x \in G$.

Also given $f(x) = a * x$.

Therefore, for each $x \in G$, there exists an element $a * x \in G$. such that

$$f(x) = a*x$$

Hence *f is* onto

$\Rightarrow$ *f is* a bijection.

(ii) Let z denote the set of integers and $a \in z$.

Define $f: z \to z$ s.t. $f(x) = x + a\ \forall\ x \in z$ we show *f is* one-one and onto.

Let $f(x)\, f(y)\ \forall\ x, y \in z$

$\Rightarrow \quad x + a = y + a$

$\Rightarrow \quad x = y$ [$\because$ Right cancellation law]

Hence *f is* one-one

Let $y \in z$ *s.t* $f(x) = y$

$\Rightarrow \quad x + a = y$

$\Rightarrow \quad x = y - a \in z$

Also for each $y \in z$, we can find

$x \in z$ s.t. $f(x)\ y$

Hence *f is* onto.

Since *f is* one-one and onto.

f is bijection.

Example 70. Let $\angle 1$ be the additive group of integers. Prove that map $f : \angle 1 \to \angle 1$ defined by $f(x) = 2x$, $x \in \angle 1$ is a group isomorphism. [Dec. 2012]

Sol. We shall show that the maping one-one and ono

(i) One-One

Let $f(x) = f(y)$

$\Rightarrow \quad 2x = 2y$

$\Rightarrow \quad x = y$

$\therefore$ *f* is one-one.

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

Applications of groups coding Theory

Or

How group theory is applied is coding theory [Dec. 05]

By using group code, we can find solutions of many coding problems by using the concept of Group theory.

A coing problem is a problem which is used to represe t distinct messages by mean of a sequence of letters from a given alphabet.

A sequence of letter from an alphabet is called a word. A co e is a collection of word that is used to represent distinct messages. A word in a code in known as code word. A black code is a code consisting of words that are of the same length. The concept of Group theory can be applied in many situations which arise in coding problems which is clear from the following discussion :

(i) In error correction : Suppose a codeword is transmitted from its origin to its destination. During the course of transmission, some of the information might cause some of the one's in the code codeword to be recieved as zero's and some of the zero's to be as one's.

Let A denote the set of all binary sequences of Length n. Let (D be a binary operation on A such that for $x\, y \in A$, $x \oplus y$ denotes the sequence of length n that has one's when x and y differ and has zero's when x and y are same. We observe that $(A, \oplus)$ is a group with all zero word as its identity and every word is its own inverse.

Further for $x, y \in A$, we define the distance between x and y denoted by $d(x, y)$ to be the weight of $x \oplus y$ say. $w(x \oplus y)$. The weight of x means the number of one's in x.

e.g. the weight of 1110000 is 3.

By using the minimum-distance decoding criteria, it has been proved that a code of distance $2t+1$, can correct or lesser transmission error.

(ii) In Group Coding : A subset G of A is called a group code if $(G, \oplus)$ is a subgroup of $(A, \oplus)$ A is the set of binary sequences of length n. By using minimum distance decoding criterion we &-termine, the transmit word corresponding to a received word. Let $(G, \oplus)$ is a group code.

Let y be a received word and $d(x, y)$ = The distance between x_i and $y = w(x_i \oplus y_1)$.

Also, the weight of the word in the cosec $G \oplus y$ is the distance between the code words in G and y. Let e denotes one of the words of smallest weight. Then, according to the minimum distance criterion, $e \oplus y = x_j$ is the transmitted code word. Thus, by using the axioms of group theory, we can find the transmitted code words.

5 Ring Theory

RINGS

(P.T.U. B.Tech, May 2008, 2007, Dec. 2006, May 2005, 2004, Dec. 2003)

Let R be a non-empty set with two binary operations, addition (+) and multiplication(.). Then R is called a ring iff it satisfies the following :

1. R is an abelian group under + *i.e.*,
   - (*i*) For $x, y \in R \Rightarrow x + y \in R$ *i.e.*, R is closed under addition
   - (*ii*) For $x, y, z \in R$, $x + (y + z) = (x + y)$ *c* i.e., Associativity under addition is satisfied.
   - (*iii*) For each $x \in R$, $\exists\ 0 \in R$ such that $x + 0 = x = 0 + i.e.$, R has additive identity.
   - (*iv*) For each $x \in R$, $\exists - x \in R$ such that $x + (-x) = 0$ *i.e.*, R has an additive inverse.
   - (*v*) For each $x, y \in R$, $x + y = y + a$ *i.e.*, R is commutative
2. **II.** For each $x, y \in R$, $x, y \in R$ *i.e.*, R is closed under multiplication.
3. **III.** For $x, y, z \in R$, $x.\ (y\ .\ z) = (x\ .\ y).\ z$ *i.e.*, Associativity under multiplication holds in R.
4. **IV.** For $x, y, z \in R$,
   - (*i*) $x.\ (y + z) = x\ .\ y + x\ .\ z$ (Left distributive law)
   - (*ii*) $(x + y)\ .\ z = x\ .\ z + y\ .\ z$ (Right distributive law).

Note : The additive identity 0 of R is unique. We call it 'zero' of the ring. The additive inverse is also unique.

Commutative Ring

A ring R is called a commutative ring $x.y = y.\ x\ \forall\ x, y \in R$. *(P.T.U. B.Tech. Dec. 2005)*

Ring With Unity

A ring R is called ring with unity if for each $a \in R$, $\exists\ 1 \in R$ such that $1.\ a = a = a.\ 1$. The element '1' is called multiplicative identity of R.