5.1 Introduction

- In this chapter, we shall deal with sets with additional structures, induced by one or more binary operations on the elements of the set. We will study some algebraic structures, groups, rings integral domains and fields.

5.2 Algebraic Structures

5.2.1 Binary Operation

I) Let A be any non empty set. A function

$f : A \times A \to A$ is called the binary operation on the set A.

'$*$' is a binary operation on the set A iff $a * b \in A, \forall\ a, b \in A$ and $a * b$ is unique.

II) An n-ary operation on a set $A \neq \phi$ is a function

$f : A \times A \times \ldots \times A$ (n times) $\to A$ i.e. $f : A^n \to A$

The n-ary operation is defined for each n-tuple $(a_1, a_2, \ldots a_n) \in A$ for all $a_i \in A$

If n = 1 then f is called unary operation

If n = 2 then f is called binary operation

If n = 3 then f is called ternary operation

Examples

1) A function $f : \Re \to \Re$ such that $f(x) = x\ ;\ \forall x \in \Re$ then f is a unary operation.

2) A function $f : \Re \times \Re \to R$ such that $f(x, y) = x + y$ then f is a binary operation.

3) A function $f : \mathbf{Z} \times \mathbf{Z} \times \mathbf{Z} \to \mathbf{Z}$ such that $f(x, y, z) = x + y + z$. then f is a ternary operation.

4) If $A = \Re$ (or C)

where $\Re$ = Real number set

C = Complex number set

then '+' '–' and '$\times$' are binary operations as

$x \pm y$ and $x \cdot y \in \Re$(or C) ; $\forall\ x, y \in \Re$ (or C)

5) For any $x, y \in N = \{1, 2, 3, 4, \ldots\}$, $x + y, x \times y \in N$

$\therefore$ '+' and '$\times$' are binary operations on N

But '–' and + are not binary operations on N, as $2 - 5 = -3 \notin N$ and $\frac{2}{3} \notin N$

6) Union, intersection and difference are binary operations in P(A), for any non empty set A.

5.2.2 Properties of Binary Operations

I) Commutative Property

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

e.g. $x + y = y + x$ and $x \times y = y \times x$ for all $x, y \in \Re$

$\therefore$ '+' and '$\times$' are commutative binary operations on $\Re$

But '–' is not commutative on $\Re$ i.e. $a - b \neq b - a$

II) Associative Property :

A binary operation '$*$' on set A is said to be associative if $a * (b * c) = (a * b) * c\ ;\ \forall\ a, b, c \in A$

e.g. '+' and '$\times$' are associative on the set of real numbers. But '–' is not associative on $\Re$

III) Idempotent

A binary operation '$*$' on set A is said to be idempotent if $a * a = a$; for all $a \in A$

e.g.

1) 1 is idempotent element in $\Re$ w.r.t. binary operation '$\times$'.

2) 0 is idempotent element in $\Re$ w.r.t. '+'.

3) 1 is not idempotent element in $\Re$ w.r.t. '+'.

Examples

Ex.5.2.1 : For each of the following, determine whether $*$ is a binary operation.

i) R is the set of real numbers and $a * b = ab$

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

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

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

v) On R, where $a * b = a \times |b|$

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

Sol. :

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

ii) No, since $(a,b) \in z^+ \times z^+$ does not imply that $a * b = a/b \in z$
$(1, 2) \in z^+ \times z^+$, but $1/2 \notin z^+$

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

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

v) Yes, since * is a function with $a \times |b| \in R$

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

Ex.5.2.2 : Let $(A, *)$ be algebraic system where * is a binary operation such that for any $a, b \in A$, $a * b = a$.
i) Show that * is an associative operation.
ii) Can * ever be a commutative operation ?

Sol. :

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

$= a*c = a$

Hence * is associative

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

Ex.5.2.3 : Determine whether or not following operations on the set of integers Z are associative.
i) Division ii) Exponentiation

Sol. :

i) Division on the set of integers is not associative as

$(a/b)/c \neq a/(b/c)$ i.e. $(20/2)/5 = 10/5 = 2$ and

$20/(2/5) = \frac{20 \times 5}{2} = 50$

$\therefore \quad (20/2)/5 \neq 20/(2/5)$

ii) Exponentiation on the set of integers is not associative as

$(a^b)^c \neq a^{(b^c)}$ e.g. $(4^3)^2 \neq 4^{(3^2)}$

Ex. 5.2.4 : Consider the binary operation * defined on the set A = {a, b, c, d} by the following table.

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

Find i) $c*d$ and $d*c$ ii) $b*d$ and $d*b$
iii) $a*(b*c)$ and $(a*b)*c$
iv) Is * commutative, associative ?

Sol. :

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

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

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

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

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

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

5.3 Special Algebraic Structures

5.3.1 Groupoid

A non empty set k with binary operation '*' is called groupoid if the binary operation '*' satisfies $\forall a, b \in G$, $a*b \in G$

In other words, every algebraic structure is groupoid.

e.g. $(\Re, +)$, $(\Re, -)$, $(Z, +)$, $(Z, \times)$ are groupoids.

5.3.2 Semi Group

A non empty set G with binary operation '*' is called a semigroup if it satisfies the following properties.

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

i.e. '*' is associative in G

A semigroup is said to be commutative if * is commutative.

e.g. i) $(\Re, +)$, $(N, +)$, $(Z, +)$ are commutative semigroups.

ii) $(\Re, \times)$, $(Z, \times)$ are commutative semigroups.

iii) $(Z, -)$ is not a semigroup as '–' is not associative.

5.3.3 Monoid

- Let G be a non empty set and * be a binary operation on G. (G, *) is called monoid if it satisfied the following properties.

i) Associative property : $a*(b*c) = (a*b)*c$; $\forall a, b, c \in G$

ii) Existence of identity : $\exists$ an element $e \in G$ such that $e*a = a*e = a$; $\forall a \in G$

The element 'e' is called the identity element.

Example 1) $(\Re, +)$ is a monoid as $a+b \in \Re$ $\forall a, b \in \Re$ i.e. $(\Re, +)$ is closed

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

and $0 + a = a + 0 = a$, $\forall a \in \Re$

0 is the identity element in $\Re$ w.r.t. '+'.

Example 2

$(C, +)$, $(C, \times)$, $(Z, +)$, $(Z, \times)$, $(Q, +)$ are monoids.

Example 3

$(N, \times)$ is a monoid but $(N, +)$ is not monoid as $0 \notin N$

Ex.5.3.1 : Show that the algebraic system (A, +) is a monoid, where A is the set of integers and '+' is a binary operation giving addition of two integers.

Sol. : Let A be the set of all integers and '+' defined on A.

i) Closure property : $a+b \in A$; $\forall a, b, \in A$ as a + b is an integer.

ii) Associative property :

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

iii) Existence of identity element :

For any $a \in A$, $\exists\ 0 \in A$ such that

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

Therefore (A, +) is a monoid.

5.4 Group

AKTU : 2013-14

- Let G be a non empty set equipped with a binary operation '*'. (G, *) is called a group if it satisfies the following postulates or axioms.

i) **Associativity :** $a*(b*c) = (a*b)*c$; $\forall a, b, c \in G$

ii) **Existence of the identity :** For any $a \in G$, $\exists\ e \in G$ such that $a*e = e*a = a$;

An element e is called the identity element in (G, *)

iii) **Existence of the inverse :**

For all $a \in G$, $\exists\ b \in G$ such that

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

Then b is called the inverse of a in (G, *)

$$\therefore \quad b = a^{-1}$$

5.4.1 Abelian Group or Commutative Group

A group (G, *) is called an Abelian group if

$$a*b = b*a \quad ; \quad \forall a, b \in G.$$

i.e. * is commutative in (G, *)

A group which not abelian is called non abelian group.

5.4.2 Properties of Group

I) The identity element in a group is unique.

Proof : Suppose e_1 and e_2 are two identity elements in group G.

We have, $e_1 e_2 = e_1$; if e_2 is identity element in G.

and $e_1 e_2 = e_2$; If e_1 is identity element in G.

$\Rightarrow e_1 e_2 = e_1 = e_2$. Hence the identity element in group G is unique.

II) The inverse of each element in group G is unique.

AKTU : 2015-16

Proof : Let a be any element of a group G and let e be identity element in group G.

Suppose b and c are two inverses of a in G.

$$\therefore \quad ba = ab = e \text{ and } ac = ca = e$$

We have, $b = be = b(ac)$

$$b = (ba)c$$

$$b = ec$$

$$b = c$$

Hence, the inverse of each element is unique.

III) The inverse of an inverse of the element is the original element. i.e. If the inverse of a is a^{-1} then $(a^{-1})^{-1} = a$. AKTU : 2011-12, 2014-15

Proof : Let $e \in G$ be the identity element of the group G.

Let $a \in G$.

We have, $a^{-1}a = e$

$[(a^{-1})^{-1}(a^{-1})]a = (a^{-1})^{-1} e$ ... (Multiplying by $(a^{-1})^{-1}$)

$[(a^{-1})^{-1}(a^{-1}]\, a = (a^{-1})^{-1}$

... ($\because$ Associativity of e identity)

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

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

Hence, the proof

IV) Prove that the inverse of the product of two elements of a group G is the product of the inverses taken in reverse order. i.e. $(ab)^{-1} = b^{-1} a^{-1}$; $\forall$ a, b $\in$ G.

AKTU : 2011-12, 2014-15, 2015-16

Proof : Let a^{-1} and b^{-1} be the inverses of a and b in a group G respectively. Let e be the identity in G. Then $a^{-1} a = a\, a^{-1} = e$ and $b^{-1} b = b^{-1} b = e$

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

($\because$ Associativity)

$= a(e)\, a^{-1}$ ($\because bb^{-1} = e$)

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

$= aa^{-1} = e$ ... (5.4.1)

Similarly,

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

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

$= b^{-1} b = e$ ... (5.4.2)

From equation (5.4.1) and equation (5.4.2),

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

$b^{-1} a^{-1}$ is the inverse of ab

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

V) Prove that the cancellation laws hold in a group.i.e. If a, b, c $\in$ G then $ab = ac \Rightarrow b = c$ and $ba = ca \Rightarrow b = c$.

Proof : Let a be any element in G and e be the identity element of a group G.

Now we have, $ab = ac$

Permultiplying by a^{-1} we get,

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

$(a^{-1} a)\, b = (a^{-1} a)\, c$ ... ($\because$ Associativity)

$eb = ec$ ... ($\because aa^{-1} = e$)

$b = c$

Similarly, $ba = ca$

$\Rightarrow \quad (ba)\, a^{-1} = (ca)\, a^{-1} \Rightarrow be = ce$

$\Rightarrow \quad b = c$ Hence, the proof

VI) If a, b are any elements of a group G then equation ax = b and ya = b have unique solutions in G.

Proof : Let $a \in G$

$\therefore \exists\, a^{-1} \in G$ such that $aa^{-1} = a^{-1}a = e$

$a, a^{-1} \in G$ and $b \in G \Rightarrow a^{-1}b \in G$.

Now substituting $a^{-1}b$ for x in the L.H.S. given equation, we get,

$ax = a(a^{-1}b) = (aa^{-1})\, b = eb = b$

Thus, $x = a^{-1} b$ is the solution of $ax = b$

Let us suppose that x_1 and x_2 are two solutions of $ax = b$.

$\therefore \quad ax_1 = b$ and $ax_2 = b$

$\Rightarrow \quad b = ax_1 = ax_2 \Rightarrow x_1 = x_2$

Hence solution is unique.

Similarly prove for $ya = b$.

Examples

Ex.5.4.1 : Determine whether a semigroup with more than one idempotent element can be group :

Sol. : Let $\in(A,*)$ be a semigroup with two idempotent element a and b ($a \neq b$). We have $a * a = a$ and $b * b = b$

Assume that A is a group with identity element e.

$\therefore \quad a * e = a \quad \ldots (1)$

$b * e = b \quad \ldots (2)$

$\therefore \quad a * e = a = a * a \Rightarrow a = e$

$b * e = b = b * b \Rightarrow b = e$

Therefore $a = b = e$

Which is the contradiction to $a \neq b$

Hence (A, *) is not a group.

Ex.5.4.2 : Let {(a, b), *} be a semigroup where $a * a = b$ show that
i) $a * b = b * a$ ii) $b * b = b$

Sol. : Given that {(a, b), *} is a semigroup and

$a * a = b$

i) $a * b = a * (a * a) \quad (\because a * a = b)$

$= (a * a) * a \quad (\because * \text{ is associative})$

$= b * a \quad (\because b = a * a)$

$\therefore \quad a * b = b * a$. Hence the proof.

ii) Show that $b * b = b$

{a, b} is closed with respect to *

∴there are only two options $a * b = b$ or $a * b = a$

a) Let $a * b = a$

Now, $b * b = b * (a * a) \quad (\because b = a * a)$

$= (b * a) * a \quad (\because * \text{ is associative})$

$= (a * b) * a \quad (\text{by i})$

$= a * a \quad (\because a * b = a)$

$b * b = b$

b) Let $a * b = b$

Now $b * b = (a * a) * b \quad (\because b = a * a)$

$= a * (a * b) \quad (\because * \text{ is associative})$

$= a * b \quad (\because a * b = b)$

$b * b = b$

Ex.5.4.3 : Let (A, *) be a commutative semigroup. Show that if $x * x = x$ and $y * y = y$ then $(x * y) * (x * y) = x * y$.

Sol. : Consider L.H.S. $= (x * y) * (x * y)$

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

$(\because * \text{ is commutative})$

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

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

Hence the proof.

Ex. 5.4.4 : Let (A, *) be a semigroup. Furthermore for every a, 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 $a, b, c \in A$, $a * b * c = a * c$ AKTU : 2012-13

Sol. : a) We have (A, *) is a semigroup.

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

Now, putting $b = a$ and $c = a$. we get

But (A, *) is not commutative semigroup

Hence $a * a = a$

b) Let $b \in A \quad \therefore b * b = b$

∴Multiplyig both sides by a

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

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

$\Rightarrow \quad a * b = a \quad \ldots (1)$

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

$a * b * a = a$

c) We know that

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

$= a * c \quad (\text{by (1)})$

Ex.5.4.5 : Let (A, x) be a monoid such that for every $x \in A$, $x * x = e$ where e is the identity element. Show that (A, *) is an abelian group. AKTU : 2012-13

Sol. : Given that, (A, *) is a monoid. Therefore it satisfies closure property, associativity and the existence of identity.

We have $x * x = e \ , \ \forall x \in A$

$$x = x^{-1} \ , \ \forall x \in A$$

Thus inverse exists for all $x \in A$.

$\therefore$ (A, *) is a group.

Consider, for $a, b \in A$

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

... ($\because$ * is asssociative)

$$= a * e * a \quad \text{... } (\because b * b = e)$$

$$= a * a = e$$

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

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

Thus b * a is the inverse of a * b

But $x = x^{-1}$, $\forall x$ in A

$$b * a = a * b$$

Thus, (A, *) is an abelien group.

Ex.5.4.6 : Show that the set $G = \{a + b\sqrt{2} \ / \ a, b \in Q\}$ is a group with respect to addition.

Sol.: Given that, $G = \{a + b\sqrt{2} \ / \ a, b \in Q\}$

(i) Closure property : Let $x, y \in G$.

$$x = a + b\sqrt{2},$$

$$y = c + d\sqrt{2} \ a, b, c, d \in Q.$$

Consider, $x + y = (a + b\sqrt{2})(c + d\sqrt{2})$

$$= (a + c) + (b + d)\sqrt{2},$$

$a + c$ and $b + d \in Q$

$$\Rightarrow \quad x + y \in G$$

$\therefore$ G is closed w.r.t. +

(ii) Associativity : All elements of G are real numbers and associativity holds in R.

$\therefore$ Associativity holds in G.

(iii) Existence of the idenity : We have, $0 \in Q$

$$0 + 0\sqrt{2} = 0 \in G$$

Consider

$$(0 + 0\sqrt{2}) + (a + b\sqrt{2}) = (0 + a)(0 + b)\sqrt{2}$$

$$= a + b\sqrt{2}$$

and $(a + b\sqrt{2}) + (0 + 0\sqrt{2}) = a + b\sqrt{2}$

$\therefore$ 0 is the additive identity element in G.

(iv) Existence of the inverse : We have a, b and $-a, -b \in Q$.

$\therefore$ $a + b\sqrt{2}$ and $-a - b\sqrt{2}$ G.

Consider,

$$(a + b\sqrt{2}) + (-a - b\sqrt{2}) = (a - a) + (b - b)\sqrt{2}$$

$$= 0 + 0\sqrt{2} = 0$$

and

$$(-a - b\sqrt{2}) + (a + b\sqrt{2}) = (-a + a) + (-b + b)\sqrt{2}$$

$$= 0 + 0\sqrt{2} = 0$$

$\therefore$ $-a - b\sqrt{2}$ is the inverse of $a + b\sqrt{2}$. Hence G is a group with respect to addition.

Ex. 5.4.7 : If set Q_1 of all rational numbers other than 1 with $a * b = a + b - ab$. Show that (G, *) is a group.

Sol. : We have, $a * b = a + b - ab, \ \forall \ a, b \in G$.

(i) Closure property : Let $a, b \in Q_1$, $a \neq 1$, $b \neq 1$

$\therefore$ $ab \neq 1$.

$\therefore$ $a * b = a + b - ab \neq 1$ and $a * b \in Q_1$

Q_1 is closed w.r.t. *

(ii) Associativity : Let $a, b, c \in Q_1$.

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

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

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

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

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

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

$\therefore$ From equation (1) and equation (2)

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

$\therefore$ * is associative

(iii) Existence of the identity : Let e be the identity element in Q_1

$a * e = a$

$\Rightarrow a + e = ae = a$

$\Rightarrow e - ae = 0$

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

$\Rightarrow e = 0$

$\therefore$ 0 is the identity element.

(iv) Existence of the inverse : Let $a \in Q_1$, $a \neq 1$.

Suppose $b \in Q$, is the inverse of a.

$\therefore a * b = e$

$\Rightarrow a + b - ab = 0$

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

$b (1 - a) = - a$

$\Rightarrow b = \frac{-a}{1-a} = \frac{a}{a-1} \neq 1$ and $b \in Q_1$.

$\therefore$ The inverse exist for all a in Q_1.

Thus, $(Q_1, *)$ is a group.

Ex. 5.4.8 : If $S = \{(a, b) | a \neq 0, a, b, \in \Re\}$ and (a, b) * (c, d) = (ac, bc + d) then show that G is a group but not abelian group w.r.t.*

Sol. : (i) Closure property : Let (a, b) (c, d) $\in S$;

$a \neq 0$; $c \neq 0$

$\therefore ac \neq 0$.

$(a, b) * (c, d) = (ac, bc + d) \in S$

(ii) Associativity : Let (a, b), (c, d) and (e, f) $\in S$

Consider

$[(a, b) * (c, d)] * (e, f) = [ac, (bc + d)] * (e, f)$

$= ([ac] e, [bc + d] e + f)$

$= (ace, bce + de + f)$ ... (1)

and $(a, b) * [(c, d) * (e, f)] = (a, b) * [ce, de + f]$

$= [ace, b (ce) + de + f]$

$= (ace, bce + de + f)$ ... (2)

From equation (1) and equation (2) * is associative operation.

(iii) Existence of the identity : Let $(a, b) \in S$ and $(x, y) \in S$, $x \neq 0$

Consider, $(a, b) * (x, y) = (a, b)$

$(ax, bx + y) = (a, b)$

$\Rightarrow ax = a$ and $bx + y = b$

$\Rightarrow x = 1$ and $b + y = b$

$\Rightarrow y = 0$

Similarly, $(x, y) * (a, b) = (a, b)$

(1, 0) is the identity element in S.

(iv) Existence of the inverse : Let (a, b) and $(c, d) \in S$.

$(a, b) * (c, d) = (1, 0)$

$(ac, bc + d) = (1, 0)$

$\Rightarrow ac = 1$

and $bc + d = 0$

$\therefore c = \frac{1}{a}$

and $d = - bc = - \frac{b}{a}$ and $c \neq 0$

Thus $\left(\frac{1}{a}, -\frac{b}{a}\right)$ is the inverse of (a, b) in S.

Thus (S, *) is a group.

Consider, $(a, b) * (c, d) = (ac, bc + d)$

and $(c, d) * (a, b) = (ca, da + b)$

$\Rightarrow$ $(a, b) * (c, d) \neq (c, d) * (a, b)$

Thus, (S, *) is not an abelian group.

Ex.5.4.9 : If $G = \left\{ \begin{bmatrix} a & 0 \\ 0 & 0 \end{bmatrix} / a \text{ is non zero real number} \right\}$ **show that G is an abelian group w.r.t. matrix multiplication.**

Sol. : (i) Closure property : Let $A = \begin{bmatrix} a & 0 \\ 0 & 0 \end{bmatrix}$, $B = \begin{bmatrix} b & 0 \\ 0 & 0 \end{bmatrix}$ be any two elements of G where a, b are non-zero real numbers.

$$AB = \begin{bmatrix} ab & 0 \\ 0 & 0 \end{bmatrix}, \text{ ab is non zero real number.}$$

$\therefore AB \in G$

$\therefore$ G is closed w.r.t. multiplication.

(ii) Associativity : We know that matrix multiplication is associative.

(iii) Existence of the identity : Let $E = \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix} \in G$

Consider $AE = \begin{bmatrix} a & 0 \\ 0 & 0 \end{bmatrix}\begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix} = \begin{bmatrix} a & 0 \\ 0 & 0 \end{bmatrix} = A$

and $EA = \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}\begin{bmatrix} a & 0 \\ 0 & 0 \end{bmatrix} = \begin{bmatrix} a & 0 \\ 0 & 0 \end{bmatrix} = A$

$\therefore$ $E = \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}$ is the identity element w.r.t. matrix multiplication.

(iv) Existence of the inverse :

Let $A = \begin{bmatrix} a & 0 \\ 0 & 0 \end{bmatrix}$ and $B = \begin{bmatrix} b & 0 \\ 0 & 0 \end{bmatrix} \in G$

Consider $AB = \begin{bmatrix} a & 0 \\ 0 & 0 \end{bmatrix}\begin{bmatrix} b & 0 \\ 0 & 0 \end{bmatrix}$

$$= \begin{bmatrix} ab & 0 \\ 0 & 0 \end{bmatrix}, ab \neq 0$$

$$= \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}$$

$\Rightarrow$ $ab = 1 \Rightarrow b = \frac{1}{a}$

$$B = \begin{bmatrix} \frac{1}{a} & 0 \\ 0 & 0 \end{bmatrix} \in G$$

And $AB = BA = \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}$

$\therefore$ B is the inverse of A in G.

(v) Commutativity :

$$AB = \begin{bmatrix} a & 0 \\ 0 & 0 \end{bmatrix}\begin{bmatrix} b & 0 \\ 0 & 0 \end{bmatrix} = \begin{bmatrix} ab & 0 \\ 0 & 0 \end{bmatrix}$$

$$BA = \begin{bmatrix} b & 0 \\ 0 & 0 \end{bmatrix}\begin{bmatrix} a & 0 \\ 0 & 0 \end{bmatrix} = \begin{bmatrix} ba & 0 \\ 0 & 0 \end{bmatrix}$$

$\Rightarrow$ $AB = BA$

Hence G is an abelian group.

Ex. 5.4.10 : If $G = \left\{ \begin{bmatrix} x & x \\ x & x \end{bmatrix} / x \text{ is non zero real number} \right\}$. **Show that G is an abelian group w.r.t. matrix multiplication.**

Sol. : (i) Closure property :

Let $A = \begin{bmatrix} x & x \\ x & x \end{bmatrix}$ and $B = \begin{bmatrix} y & y \\ y & y \end{bmatrix} \in G$

then $AB = \begin{bmatrix} x & x \\ x & x \end{bmatrix}\begin{bmatrix} y & y \\ y & y \end{bmatrix} = \begin{bmatrix} 2xy & 2xy \\ 2xy & 2xy \end{bmatrix} \in G$

(ii) Associativity : We know that any matrix multiplication is associative.

(iii) Existence of the identity : Let $E = \begin{bmatrix} e & e \\ e & e \end{bmatrix}$ such that $AE = A \Rightarrow$

$$\begin{bmatrix} x & x \\ x & x \end{bmatrix}\begin{bmatrix} e & e \\ e & e \end{bmatrix} = \begin{bmatrix} e & e \\ e & e \end{bmatrix}$$

$\Rightarrow$ $\begin{bmatrix} 2xe & 2xe \\ 2xe & 2xe \end{bmatrix} = \begin{bmatrix} e & e \\ e & e \end{bmatrix}$

$\Rightarrow$ $2xe = e$

$\Rightarrow$ $2x = 1$

$$\Rightarrow \quad x = \frac{1}{2}$$

$$\therefore \quad E = \begin{bmatrix} \frac{1}{2} & \frac{1}{2} \\ \frac{1}{2} & \frac{1}{2} \end{bmatrix}$$

is the identity element of G.

(iv) Existence of the inverse : Let $A = \begin{bmatrix} x & x \\ x & x \end{bmatrix} \in G$

and

$B = \begin{bmatrix} y & y \\ y & y \end{bmatrix} \in G$ such that $AB = E$

$$\Rightarrow \begin{bmatrix} 2xy & 2xy \\ 2xy & 2xy \end{bmatrix} = \begin{bmatrix} \frac{1}{2} & \frac{1}{2} \\ \frac{1}{2} & \frac{1}{2} \end{bmatrix}$$

$$\Rightarrow \quad 2xy = \frac{1}{2}$$

$$\Rightarrow \quad xy = \frac{1}{4}$$

$$\Rightarrow \quad y = \frac{1}{4x}$$

$$A^{-1} = \begin{bmatrix} \frac{1}{4x} & \frac{1}{4x} \\ \frac{1}{4x} & \frac{1}{4x} \end{bmatrix}$$

(v) Commutative property :

We have, $AB = BA = \begin{bmatrix} 2xy & 2xy \\ 2xy & 2xy \end{bmatrix} \in G$

Thus G is an abelian group w.r.t. matrix multiplication.

Ex. 5.4.11 : If

$$G = \left\{ \begin{bmatrix} \cos\alpha & -\sin\alpha \\ \sin\alpha & \cos\alpha \end{bmatrix} / a \text{ is non zero real number} \right\}$$

, then G is a group w.r.t. matrix multiplication.

Sol. : (i) Closure property :

Let A and B $\in$ G

$$A = \begin{bmatrix} \cos\alpha & -\sin\alpha \\ \sin\alpha & \cos\alpha \end{bmatrix}$$

and

$$B = \begin{bmatrix} \cos\beta & -\sin\beta \\ \sin\beta & \cos\beta \end{bmatrix}$$

$$AB = \begin{bmatrix} \cos(\alpha+\beta) & -\sin(\alpha+\beta) \\ \sin(\alpha+\beta) & \cos(\alpha+\beta) \end{bmatrix} \in G$$

(ii) Matrix multiplication is associative i.e.
(AB)C = A(BC)

(iii) Existence of the identity : As $0 \in R$

$$E = \begin{bmatrix} \cos 0 & -\sin 0 \\ \sin 0 & \cos 0 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$$

$$AE = EA = E$$

$$E = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \text{ is the idenity element in G.}$$

(iv) Existence of the inverse :

Let $A \in G$ and $A = \begin{bmatrix} \cos\alpha & -\sin\alpha \\ \sin\alpha & \cos\alpha \end{bmatrix}$

$$B = \begin{bmatrix} \cos\alpha & \sin\alpha \\ -\sin\alpha & \cos\alpha \end{bmatrix} \in G$$

Consider $AB = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} = BA$

$\Rightarrow$ B is the inverse of A in G.

Thus G is a group w.r.t. matrix multiplication.

Ex.5.4.12 : Let G be the set of all non-zero real numbers and let $a * b = \frac{ab}{2}$. Show that (G, *) is an abelian group.

AKTU : 2015-16

Sol. : (i) Closure property : Let a, b $\in$ G.

$$a * b = \frac{ab}{2} \in G \text{ as } ab \neq 0$$

(ii) Associativity : Let a, b, c $\in$ G

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

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

$\Rightarrow$ * is associative in G.

(iii) Existence of the identity : Let $a \in G$ and $\exists$ e such that

$$a * e = \frac{ae}{2} = a$$

$\Rightarrow$ $ae = 2a$

$\Rightarrow$ $e = 2$

$\therefore$ 2 is the identity element in G.

(iv) Existence of the inverse : Let $a \in G$ and $b \in G$ such that $a * b = e = 2$.

$\Rightarrow$ $\frac{ab}{2} = 2$

$\Rightarrow$ $ab = 4$

$\Rightarrow$ $b = \frac{4}{a}$

$\therefore$ The inverse of a is $\frac{4}{a}$, $\forall\, a \in G$.

(v) Commutativity : Let $a, b \in G$

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

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

$\Rightarrow$ * is commutative

Thus, (G, *) is an abelian group.

Ex.5.4.13 : Show that the four fourth roots of unity namely 1, –1, i, –i form a group w.r.t. multiplication.

Sol. : Let $G = \{ 1, -1, i, -i \}$. Consider the following table.

X	1	–1	i	–i
1	1	–1	i	–i
–1	–1	1	–i	i
i	i	– i	–1	1
–i	–i	i	1	–1

(i) Closure property : All elements of table belongs to G.

$\therefore$ G is closed w.r.t. multiplication.

(ii) Associativity : We know that multiplication of complex numbers is associative.

(iii) Existence of the identity : From table

$(1)\,(1) = 1$ $\qquad$ $(-1)\,1 = -1$

$(i)\,1 = i$ and $(-i)\,1 = -i$

$\therefore$ 1 is the identity element in G.

(iv) Existence of the inverse : From table,

$$1^{-1} = 1,$$

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

$$(i)^{-1} = -i,$$

and $$(-i)^{-1} = i$$

$\therefore$ The inverse exists for all elements of G. Thus, 'G' is a group.

Ex.5.4.14 : Show that the set $G = \{1, w, w^2\}$ where w is the cube root of unity is a group with respect to multiplication.

Sol. : Consider the following composition table of G.

X	1	w	w^2
1	1	w	w^2
w	w	w^2	1
w^2	w^2	1	w

(i) Closure property : From table all elements belong to G.

$\therefore$ G is closed w.r.t. multiplication.

(ii) Associativity : As all elements of G are complex numbers and multiplication of complex numbers is associative.

$\therefore$ (G, x) is associative.

(iii) Existence of the identity : From the composition table

$$1\,(1) = 1\,,\ 1\,(w) = 1\,,\ 1\,(w^2) = w^2$$

$\therefore$ 1 is multiplicative identity in G.

(iv) Existence of the inverse : From table, the inverses of 1, w, w^2 are 1, w^2, w respectively. Thus (G, x) is a group.

Ex.5.4.15 : Prove that $G = \{0, 1, 2, 3, 4, 5\} = Z_6$ is an abelian group of order 6. w.r.t. addition modulo 6.

Sol. : Let us consider the composition table

$+_6$	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

(i) Closure property : From the composition table all elements belong to Z_6.

$\therefore$ Z_6 is closed w.r.t. $+_6$

(ii) Associativity : Let $a, b, c \in Z_6$

$a +_6 (b +_6 c)$ = The smallest non zero remainder when $a + (b + c)$ is divided by 6.

= The smallest non zero remainder when $(a + b) + c$ is divided by 6.

$= (a +_6 b) +_6 c$

$\therefore$ $+_6$ is associative.

(iii) Existence of the identity : We have $0 \in Z_6$

If $a \in Z_6$ then $a +_6 0 = a = 0 +_6 a$

$\therefore$ 0 is the additive identity.

(iv) Existence of the inverse : From the composition table, the inverses 0, 1, 2, 3, 4, 5 are 0, 5, 4, 3, 2, 1 respectively.

(v) Commutativity : Let $a, b \in Z_6$

$a +_6 b = b +_6 a$ ... ($\because$ From table)

Thus $(Z_6, +_6)$ is an abelian group.

Ex.5.4.16 : Suppose (G, *) be a group. Show that if (G, *) is an abelian group then $a^3 * b^3 = (a * b)^3$ for all a, b $\in$ G.

Sol. : Suppose (G, *) is an abelian group.

i.e. $a * b = b * a$; $\forall$ a, b $\in$ G

Consider, $a^3 * b^3 = (a * a * a) * (b * b * b)$

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

($\because$ * is associating)

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

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

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

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

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

$a^3 * b^3 = (a * b)^3$

Ex. 5.4.17 : Show that the set of all idempotents in a commutative monoid S is a submonoid of S.

Sol. : We know that an element $x \in S$ is called an idempotent if $x * x = x$. Let T be the set of all idempotents in S.

i) For any $x, y \in T$, Consider

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

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

$= (y * x) * y$

$= (x * y) * y$

$= x * (y * y)$

$= x * y$

$\therefore$ $x * y \in T$ for all $x, y \in T$

T is closed w.r.t. '*'

ii) Associativity, Let $x, y, z \in T \subseteq S$

$\therefore$ $x * (y * z) = (x * y) * z$ in T

* is associative in T

iii) Existence of the identity :

Let e be the identity element in S

As $e * e = e$ $\therefore$ $e \in T$

$\therefore$ e is the identity element in T.

$\therefore$ T is a monoid

Thus T is a submonoid of S.

Ex.5.4.18 : Prove that the set Z of all integers with binary operation * defined by $a * b = a + b + 1$ such that $\forall\ a, b \in Z$ is an abelian group :

Sol. :

We have $a*b = a + b + 1\ ,\ \forall\ a, b \in Z$

i) Closure property

For $a, b \in Z \Rightarrow a+b+1 \in Z \Rightarrow a * b \in Z$

$\therefore$ Z is closed w.r.t. *

ii) Associative : Let $a, b, c \in Z$

$$(a*b)*c = (a + b + 1) * c$$
$$= a + b + 1 + c + 1$$
$$= a + b + c + 2 \quad \ldots (1)$$

and $$a*(b*c) = a*(b+c+1)$$
$$= a + b + c + 1 + 1$$
$$= a + b + c + 2 \quad \ldots (2)$$

From equation (1) and equation (2)
$(a * b) * c = a * (b * c)$

$\therefore$ * is associative in Z

iii) Existence of the identity :

Let e be the identity in Z

$\therefore$ For any $a \in Z$, $a*e = e*a = a$

$$\Rightarrow a + e + 1 = a$$
$$\Rightarrow e + 1 = a$$
$$\Rightarrow e = -1 \text{ is the identity element in } Z$$

iv) Existence of the inverse :

Let $a \in Z$. Suppose $b \in Z$ is the inverse of a in Z

$\therefore$ $$a*b = e$$
$$a + b + 1 = -1$$
$$a + b = -2$$
$$b = -a - 2 \in Z$$

$\therefore$ The inverse exists for all $a \in Z$

Thus (Z, *) is a group.

Now consider

$$a*b = a + b + 1 \qquad (\because a + b = b + a)$$
$$= b + a + 1$$
$$= b*a\ ,\ \forall\ a, b \in Z$$

$\therefore$ * is commutative in Z

$\therefore$ (Z, *) is an abelian group.

Ex.5.4.19 : Let (Z, *) be an algebraic strcuture, where Z is the set of integers and the operation * is defined by x * y = maximum {x, y}. Determine whether (Z, *) is a monoid or a group or an abelian group.

Sol. : i) Closure property : For any $x, y \in z$

$$x * y = \max\{x, y\} \in z$$

$\therefore$ '*' is closed in z

ii) Associative property : Let $x, y, z \in z$

We have

$$x * (y * z) = x * \max(y, z)$$
$$= \max\{x, \max\{y, z\}\}$$
$$= \max\{x, y, z\} \quad \ldots (1)$$

Similarly

$$(x * y) * z = \max\{x, y, z\} \quad \ldots (2)$$

From (1) and (2),

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

Hence * is associative.

iii) Existence of the identity :

Let e be the ideentity element then $a * e = \max\{a, e\} = a$

Hence, the maximum element is the identity element in z.

iv) Existence of the inverse : For $z, 3 \in z$

$$2 * 3 = \max\{2, 3\} = 3$$

∴ The inverse of any element does not exist.

Hence $(Z, *)$ is not a group or not an abelian group.

But $(Z, *)$ is a monoid.

5.5 Modulo m

I) Let and b are any integers and m is a fixed positive integer then the **addition modulo m** denoted by $a +_m b$ and defined as $a +_m b = r$; $0 \le r \le m$

Where r is the least non negative remainder when a + b is divided by m.

e.g.

$5 +_3 9 = 2$ as $5 + 9 = 14$ and $14 = 3 \times 4 + 2$

$15 +_5 25 = 0$ as $15 + 25 = 40$ and $40 = 5 \times 8 + 0$

II) Let a and b be any integers and m is a fixed positive integer. Then the **multiplication modulo m** is denoted by $a \times_m b$ and defined as

$$a \times_m b = r \; ; \; 0 \le r \le m$$

Where r is the least non negative remainder when a × b is divided by m.

e.g.

$3 \times_4 5 = 3$ as $3 \times 5 = 15$ and $15 = 4 \times 3 + 3$

$9 \times_6 4 = 0$ as $9 \times 4 = 36$ and $36 = 6 \times 6 + 0$

III) If a and be are any two integers such that a – b is divisible by a fixed positive integer m, is called **"a congruent to b modulo m".**

It is denoted by $a \equiv b \pmod m$

Note :

1) If $a \equiv b \pmod m$ iff a – b is divisible by m

i.e. $a - b = pm$; for some integer p.

$$a = pm + b$$

2) If $a \equiv b \pmod m$ then $b \equiv a \pmod m$

3) For any $a \in Z$, $a \equiv a \pmod m$

e.g.

i) $5|(12-2)| \Rightarrow 12 \equiv 2 \pmod 5$

$5|(12-2)| \Rightarrow 2 \equiv 12 \pmod 5$

ii) $8|(30-6)| \Rightarrow 30 \equiv 6 \pmod 8$

iii) $5|(9-9)| \Rightarrow 9 \equiv 9 \pmod 5$

Examples

Ex.5.5.1 : Show that $(G, +_8)$ is an abelian group where G = {0, 1, 2, 3, 4, 5, 6, 7}

Sol. : Consider the following table for $+_8$

$+_8$	0	1	2	3	4	5	6	7
0	[0]	1	2	3	4	5	6	7
1	1	2	3	4	5	6	7	[0]
2	2	3	4	5	6	7	[0]	1
3	3	4	5	6	7	[0]	1	2
4	4	5	6	7	[0]	1	2	3
5	5	6	7	[0]	1	2	3	4
6	6	7	[0]	1	2	3	4	5
7	7	[0]	1	2	3	4	5	6

1) Closure property : Every element of the table belongs to G

i.e. $a +_8 b \in G$; $\forall\, a, b \in G$

∴ $+_8$ is closed in G.

2) Associativity : For any $a, b, c \in G$

$$a +_8 (b +_8 c) = (a +_8 b) +_8 c$$

∴ $+_8$ is associative in G.

3) Existence of the identity

By observing first row and first column,

For any $a \in G$, $\exists\, 0 \in G$ such that

$$a +_8 0 = 0 +_8 a = a$$

Hence 0 is the identity element for '$+_8$' in G

4) Existence of the inverse

Identify the identity element 0 from table.

∴ By table ;

As $0 +_8 0 = 0$; 0 is the inverse of 0

As $1 +_8 7 = 0$; 1 is the inverse of 7

As $7 +_8 1 = 0$; 7 is the inverse of 1

As $2 +_8 6 = 0$; 2 is the inverse of 6

As $6 +_8 2 = 0$; 6 is the inverse of 2

As $3 +_8 5 = 0$; 5 is the inverse of 3

As $5 +_8 3 = 0$; 3 is the inverse of 4

As $4 +_8 4 = 0$; 4 is the inverse of 4

Hence, inverse exists in G for all $a \in G$

5) Commutative property : From table, $\forall$ a, b $\in$ G

$$a +_8 b = b +_8 a$$

$\therefore$ '$+_8$' is commutative in G.

Hence, $(G, +_8)$ is an abelian group.

Ex.5.5.2 : Show that $(G, \times_7)$ is an abelian group, where G = {1, 2, 3, 4, 5, 6}

Sol. : Consider the following table

$\times_7$	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]

i) Closure Property

Every element of table belongs to G

i.e. $a \times_7 b \in G$ for all a, b $\in$ G

$\therefore \times_7$ is closed in G.

ii) Associativity

For any a, b, c $\in$ G

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

$\therefore \times_7$ is associative in G.

iii) Existence of the Indentity

By observing the first row and the first column,

For any $a \in G$, $\exists\ 1 \in G$ such that

$$a \times_7 1 = 1 \times_7 a = a$$

$\therefore$ 1 is the identity element in G.

iv) Existence of the Inverse

Identify the identity elements from table

$\therefore$ By table,

As $1 \times_7 1 = 1$, 1 is the inverse of 1

As $2 \times_7 4\ 4 \times_7 2 = 1$, $\therefore$2 is the inverse of 4 and 4 is the inverse of 2

As $3 \times_7 5 = 5 \times_7 3 = 1$, $\therefore$3 is the inverse of 5 and 5 is the inverse of 3

As $6 \times_7 6 = 1$, $\therefore$6 is the inverse of 6

Hence, inverse exists in G for all $a \in G$

v) Commutative Property

From table, for all a, b $\in$ G

$$a \times_7 b = b \times_7 a$$

$\therefore \times_7$ is commutative in G.

Hence $(G, \times_7)$ is an abelian group.

Ex. 5.5.3 : Is $(G, \times_6)$ an abelian group? Where G = {1, 2, 3, 4, 5}

Sol. : Here 2, 3 $\in$ G but $2 \times_6 3 = 0 \notin G$

$\therefore \times_6$ is not binary operation in G

i.e. $\times_6$ is not closed in G.

Hence $(G, \times_6)$ is not a group.

Thus $(G, \times_6)$ is not a abelian group.

Ex. 5.5.4 : Let S = {0, 1, 2, 3, 4, 5, 6, 7} and multiplication modulo 8, i.e. x $\otimes$ y = (xy) modulo 8 = (xy) mod 8

i) Prove that {{0, 1}, $\otimes$} is not a group

ii) Write three distinct groups (G, *)

Sol. i) We have {{0, 1}, $\otimes$}

a) Closure property : The set {0, 1} is closed under the operation $\otimes$, as shown in table

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

b) Associative property : The operation $\otimes$ is associative i.e. for any, a, b, c $\in$ {0, 1}

$$a \otimes (b \otimes c) = (a \otimes b) \otimes c$$

c) **Existence of the identity :**

For any $a \in \{0, 1\}$, $\exists\ 1 \in \{0, 1\}$ such that

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

$\therefore 1$ is the identity element in $\{0, 1\}$

d) **Existence of the inverse :** for $a \in \{0, 1\}$

$$0 \otimes a = a \otimes 0 \neq 1$$

So, the inverse of 0 does not exist.

Hence $\{\{0, 1\}, \otimes\}$ is not a group

ii) A group with two elements, must contain one identity element and other non identity element.

A group with two elements is an abelian group and $x = x^{-1} \forall x$.

Therefore the second element of group is such that

$$x \otimes x = 1 \text{ for } x \in s$$

Here $2 \otimes 2 = 4, 3 \otimes 3 = 1, 4 \otimes 4 = 0, 5 \otimes 5 = 1, 6 \otimes 6 = 4, 7 \otimes 7 = 1$

Thus, $\{\{1, 3\}, \otimes\}$, $\{\{1, 5\}, \otimes\}$, $\{\{1, 7\}, \otimes\}$ are groups of order 2.

Ex. 5.5.5 : a) Show that $(z_6, +)$ is an abelian group. AKTU : 2014-15

b) Obtain the left cosets of {[0], [3]} in group (Z_6, t_6) AKTU : 2016-17

Sol. : a) Let z_6 be the set of residue classes modul o6.

$$\therefore \quad z_6 = \{[0], [1], [2], [3], [4], [5]\}$$

$$\text{Or} \quad z_6 = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}, \bar{5}\}$$

Consider the following table

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

i) Closure Property

Every element of a table belongs to z_6

i.e. $\bar{a} + \bar{b} \in z_6 \quad \forall\ \bar{a}, \bar{b} \in z_6$

$\therefore +$ is closed in z_6

ii) Associativity

By table, for any $\bar{a}, \bar{b}, \bar{c} \in z_6$

$$\bar{a} + (\bar{b} + \bar{c}) = (\bar{a} + \bar{b}) + \bar{c}$$

$\therefore$ '+' is associative in z_6

iii) Existence of the Identity

By observing the first row and the first column,

For any $\bar{a} \in z_6$, $\exists\ \bar{0} \in z_6$ such that

$$\bar{a} + \bar{0} = \bar{0} + \bar{a} = \bar{a}$$

$\therefore$ $\bar{0}$ is the identity element in z_6.

iv) Existence of the Inverse

From table, identify the identity elements

As $\bar{0} + \bar{0} = \bar{0}$, $\bar{0}$ is the inverse of $\bar{0}$

As $\bar{1} + \bar{5} = \bar{5} + \bar{1} = \bar{0}$, $\bar{1}$ is the inverse of $\bar{5}$ and $\bar{5}$ is the inverse of $\bar{1}$

As $\bar{2} + \bar{4} = \bar{4} + \bar{2} = \bar{0}$, $\bar{2}$ is the inverse of $\bar{4}$ and $\bar{4}$ is the inverse of $\bar{2}$

As $\bar{3} + \bar{3} = \bar{0}$, $\bar{3}$ is the inverse of $\bar{3}$

$\therefore$ Every element of z_6 has inverse in z_6.

v) Commutative Property

From table, For all $\bar{a}, \bar{b} \in z_6$

$$\bar{a} + \bar{b} = \bar{b} + \bar{a}$$

$\therefore$ '+' is commutative in z_6.

Hence $(z_6, +)$ is an abelian group.

b)

Let $H = \{[0],[3]\} = \{\bar{0}, \bar{3}\}$ is a subgroup of $(z_6, +_6)$.

We have $\bar{0}, \bar{3} \in H$

$\therefore$ the left cosets of H are

$$a +_6 H = \{a +_6 h / h \in H\}$$

$$\bar{0} +_6 H = \{\bar{0}, \bar{3}\}$$

$$\bar{1} +_6 H = \{\bar{1}, \bar{4}\}$$

$\bar{2} +_6 H = \{\bar{2}, \bar{5}\}$

$\bar{3} +_6 H = \{\bar{3}, \bar{0}\} = H$

$\bar{4} +_6 H = \{\bar{4}, \bar{1}\}$

$\bar{5} +_6 H = \{\bar{5}, \bar{2}\}$

$\bar{6} +_6 H = \{\bar{6}=\bar{0}, \bar{3}\} = H$.

All these are left cosets of H in z_6.

Among all these left cosets, distinct left cosets are $\bar{0}+H, \bar{1}+H, \bar{2}+H$.

Ex. 5.5.6 : Let z = {0, 1, 2, 3, 4, ... (n – 1)} and '◊' be a binary operation such that $a \lozenge b$ = remainder of $a \cdot b$ when divided by n. Construct a table for n = 4, Is $(z_4, \lozenge)$ is groupoid, monoid, semigroup and abelian group ?

Sol. :

We have $z_4 = \{0, 1, 2, 3\}$

Table of z_4 is

◊	0	1	2	3
0	[0]	0	0	0
1	0	1	2	3
2	0	2	[0]	2
3	0	3	2	1

i) From table, for any $a, b \in z_4$, $a \lozenge b \in z_4$

$\therefore$ $(z_4, \lozenge)$ is a groupoid and ◊ is a binary operation in z_4 i.e. ◊ is closed in z_4.

ii) Semigroup : By table for any $a, b, c, \in z_4$

$$a \lozenge (b \lozenge c) = (a \lozenge b) \lozenge c$$

$\therefore$ ◊ is associative in z_4

OR Let $a \lozenge b = r$ and $b \lozenge c = t$

$\therefore$ $ab = 4p + r$ and $bc = 4l + t$

$\therefore$ $(a \lozenge b) \lozenge c = r \lozenge c = s$ where $rc = 4q + s$

$a \lozenge (b \lozenge c) = a \lozenge t = k$ where $at = 4m + k$

Prove that $s = k$

$$a(bc) = 4al + at = 4al + 4m + k \quad \ldots (1)$$

$$(ab)c = (4p + r)c = 4pc + rc$$

$$= 4pc + 4q + s \quad \ldots (2)$$

Equations (1) and equation (2) are equal

$$\Rightarrow 4al + 4m + k = 4pc + 4q + s$$

$$\Rightarrow k = s$$

Hence $(a \lozenge b) \lozenge c = a \lozenge (b \lozenge c)$

Thus $(z_4, \lozenge)$ is a semigroup

iii) Monoid

By observing the first row and the first column of table

For any $a \in z_4$, $\exists\ 0 \in z_4$ such that

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

$\therefore$ 0 is the identity element in z_4

Thus from (i), (ii) and (iii), $(z_4, +)$ is a monoid.

iv) Existence of the inverse

From table, identify the identity elements.

x is the inverse of 3 in z_4

$\therefore$ $x \lozenge 3 = 0$ and $x \lozenge 3 = 4$ if $3x = 4m + r$

$\therefore$ $3x - 4m = 0$

$\Rightarrow$ $3x = 4m$

$\Rightarrow$ $x = \frac{4m}{3}$ which is an integer

For $m = 1, 2,$ x is not an integer

For $m = 3,$ $x = 4$ which is an integer

But $x = 4 \notin z_4$

Thus 3 does not have inverse in z_4

$\therefore$ $(z_4, \lozenge)$ is not a group

Hence $(z_4, \lozenge)$ is not an abelian group.

5.6 Permutation Group

1) Let $S = \{1, 2, 3, \ldots n\}$ be a finite set with n distinct elements. If $f : S \to S$ is a bijective function then f is called a **permutation of degree n**. The number of elements in the finite set S is known as the degree of permutation.

Let $f(a_1) = b_1,\ f(a_2) = b_2, f(a_3) = b_3, \ldots f(a_n) = b_n$ Then the permutation is denoted by

$$f = \begin{pmatrix} a_1 & a_2 & a_3 & \cdots & a_n \\ b_1 & b_2 & b_3 & \cdots & b_n \end{pmatrix}$$

e.g. If $S = \{1, 2, 3\}$ then

$$f = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix},\ g = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$$ are permutations of degree 3.

2) Equality of two permutations :

Two permutations f and g of degree n are said to be equal if $f(a) = g(a)$;
$\forall\ a \in S$

e.g. If $$f = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 1 & 4 \end{pmatrix}$$ and

$$g = \begin{pmatrix} 3 & 4 & 2 & 1 \\ 1 & 4 & 2 & 3 \end{pmatrix}$$ then $f = g$

3) If S is a finite set having n distinct elements and P_n be the set of all permutations of degree n then the P_n will have n ! distinct elements. This set P_n is called the symmetric set of permutations of degree. It is denoted by S_n.

4) Identity permutation : The permutation corresponding to the identity function, is called the identity permutation.

$$I = \begin{pmatrix} a_1 & a_2 & a_3 & a_y & a_n \\ b_1 & b_2 & b_3 & b_y & b_n \end{pmatrix}$$ is the identity permutation of of degree n.

5) The product or composition of two permutations

Let $$f = \begin{pmatrix} a_1 & a_2 & a_3 & \cdots & a_n \\ b_1 & b_2 & b_3 & \cdots & b_n \end{pmatrix}$$

and $$g = \begin{pmatrix} b_1 & b_2 & b_3 & \cdots & b_n \\ c_1 & c_2 & c_3 & \cdots & c_n \end{pmatrix}$$

the product of two permutations is given by

$$fg = \begin{pmatrix} a_1 & a_2 & a_3 & \cdots & a_n \\ c_1 & c_2 & c_3 & \cdots & c_n \end{pmatrix}$$

To write product use as $a_1 \xrightarrow{f} b_1 \xrightarrow{g} c_1 \ \therefore$
$a_1 \xrightarrow{fg} c_1$ similarly $a_n \to c_n\ \forall_n$

6) Groups of permutations : The set P_n at all permutations of degree n is a finite group of order n ! with respect to product of permutations or composite mapping as the operation. For $n \leq 2$, this group is abelian and for $n \geq 3$ it is non abelian group.

7) Cyclic permutations : Let f be a permutation of degree n. If it is possible to arrange m elements of the set S in a row in such a way that the f–image of each element in the row is the element which follows it, the f image of the last element is the first element and the remaining n – m elements are left unchanged by f. Then f is called a cyclic permutation or cycle of length m or an m–cycle.

for example i) $$f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 4 & 3 & 1 & 5 \end{pmatrix}$$

Here $1 \to 2 \to 4 \to 1$ and $3 \to 3$ and $5 \to 5$

$\therefore$ cycle is (1 2 4) (3) (5) $\equiv$ (1 2 4)

ii) $$g = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 3 & 4 & 5 & 6 & 1 \end{pmatrix} = (1\ 2\ 3\ 4\ 5\ 6)$$

g is a cycle of length 6.

8) A cycle of length two is called a transposition.

9) Two cycles are said to be disjoint cycles if they have no symbols in common.

e.g. (1 3 4) and (2 5 6) are disjoint cycles.

10) Inverse permutations

Let $$f = \begin{pmatrix} a_1 & a_2 & a_3 & \cdots & a_n \\ b_1 & b_2 & b_3 & \cdots & b_n \end{pmatrix}$$ then inverse permutation is $$f^{-1} = \begin{pmatrix} b_1 & b_2 & b_3 & \cdots & b_n \\ a_1 & a_2 & a_3 & \cdots & a_n \end{pmatrix}$$

11) Every permutation can be expressed as a product of disjoint cycles

eg $$f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 4 & 3 & 1 & 6 & 5 \end{pmatrix}$$

$= (1\ 2\ 4)\ (3)\ (5\ 6)$

12) Every permutation can be expressed as a product of transpositions.

i.e. $(1\ 2\ 3\ 4\ \ldots\ n) = (1\ 2)\ (1\ 3)\ (1\ 4) \quad \ldots (1\ n)$

13) Even and odd permutations : A permutation is said to be an even permutation if it can be expressed as product of an even number of transpositions, otherwise it is said to be an odd permutation.

14) a) Identify permutation is always an even permutation.

b) The product of an even permutations is an even permutation.

c) The product of an odd permutations is an odd permutations.

Theorem 1 : Prove that the set S_n is a symmetric group with respect to composite of permutations as the compositions OR prove that the n! permutations of n – objects form a finite group with respect to permutation multiplication

Proof : Let $X = \{a_1, a_2, \cdots a_n\}$ be a finite set having n distinct elements. Let $S_n = \{f, g, h, \ldots (n!\ \text{terms})\}$ be the set of all permutations of degree n having n! permutations of X. Then we have

i) Closure property : Let $f, g \in S_n$ $\therefore$ f and g are bijective functions. We know that fog is also bijective. Thus $fog \in S_n\ \forall\ f, g \in S_n$. Hence S_n is closed w.r.t. product.

ii) Associative Law : The compositions of mapping is associative, so it is also associative in case of permutations. i.e. $fo(goh) = (fog)oh\ \forall\ f, g, h \in S_n$

iii) Existence of the identity. The identity permutation is the identity element in S_n w.r.t. composition.

i.e.

$$FoI = Iof = f\ ;\ \forall\ f \in s \text{ and } I = \begin{pmatrix} a_1 & a_2 & \cdots & a_n \\ a_1 & a_2 & \cdots & a_n \end{pmatrix} \in S_n$$

iv) Existence of the inverse : Let $f = \begin{pmatrix} a_1 & a_2 & \cdots & a_n \\ b_1 & b_2 & \cdots & b_n \end{pmatrix}$

for each $f \in S_n\ \exists\ g$

$$= \begin{pmatrix} b_1 & b_2 & \cdots & b_n \\ a_1 & a_2 & \cdots & a_n \end{pmatrix}$$

Such that $fog = gof = I$, so $f^{-1} = g$.

Thus f^{-1} exists $\forall\ f \in S_n$.

Hence $(S_n, 0)$ is a finite group of order n. But $fog \neq gof$. Hence it is non abelian group.

Theorem 2 : Of the n! permutations on n symbols, $\frac{1}{2}n!$ are even permutations and $\frac{1}{2}n!$ are odd permutations.

Proof : Out of the n! permutations on n symbols, let the even permutations be $e_1, e_2, e_3 \cdots e_m$ and odd permutations be $0_1, 0_2, 0_3, \cdots 0_k$.

But the permutation is either even or odd but not both, therefore $m + k = n!$

Let $S_n = \{e_1, e_2, \cdots e_m, 0_1, 0_2, 0_3 \cdots 0_k\}$

Let $t \in S_n$ and suppose t is a transposition. As S_n is a group with respect to the permutation multiplication. Therefore $te_1, te_2, te_3, \cdots te_m$, $t0_1, t0_2, t0_3 \cdots t0_k$ are all elements of S_n. But $te_1, te_2, te_3, \cdots te_m$ are all odd permutations and $t0_1, t0_2, t0_3, \cdots t0_k$ are all even permutations. All permutations $te_1, te_2, te_3, \cdots te_m$ are distinct because $tei = tej \Rightarrow ei = ej$ which is contradiction. Thus m odd permutations $te_1, te_2, \ldots . te_m$ are distinct elements of S_n. But we have assumed that S_n contains exactly k odd permutations. Therefore $m \leq k$ ... (1)

Similarly, we can show that k even permutations $t0_1, t0_2 \cdots t0_k$ are distinct elements of S_n.

Therefore $k \leq m$ ... (2)

From (1) and (2), $\Rightarrow m = k = \frac{n!}{2}$

Theorem 3) The set A_n of all even permutations of degree n forms a finite group of order $\frac{n!}{2}$ w.r.t. multiplication

Examples :

Ex.5.6.1 : Express the permutation $F = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 6 & 5 & 3 & 4 & 2 \end{pmatrix}$ **as a product of transpositions**

Sol. : We have

$$f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 6 & 5 & 3 & 4 & 2 \end{pmatrix}$$

$$= (1)\ (2\ 6)\ (3\ 5\ 4)$$

$$= (1\ 2)\ (2\ 1)\ (2\ 6)\ (3\ 5)\ (3\ 4)$$

Ex.5.6.2 : Determine which of the following are even permutations a) (1 2 3) (4 5)
b) (1 2 3 4 5 6) (7 8)

Sol. : a) $(1\ 2\ 3)\ (4\ 5) = (1\ 2)\ (1\ 3)\ (4\ 5)$

∴ It is an odd permutation

b) $f = (1\ 2\ 3\ 4\ 5\ 6)\ (7\ 8) = (1\ 2)\ (1\ 3)\ (1\ 4)\ (1\ 5)\ (1\ 6)\ (7\ 8)$

∴ f is an even permutation

Ex.5.6.3 : Show that the set of all permutations on S = {1, 2, 3} forms a group w.r.t. permutation multiplication.

Sol. : Let

$P_3 = \{f/f$ is a permutation of degree 3$\}$

$$P_3 = \left\{ \underset{\downarrow}{\begin{pmatrix} 123 \\ 123 \end{pmatrix}}, \underset{\downarrow}{\begin{pmatrix} 123 \\ 132 \end{pmatrix}}, \underset{\downarrow}{\begin{pmatrix} 123 \\ 213 \end{pmatrix}}, \underset{\downarrow}{\begin{pmatrix} 123 \\ 231 \end{pmatrix}}, \underset{\downarrow}{\begin{pmatrix} 123 \\ 312 \end{pmatrix}}, \underset{\downarrow}{\begin{pmatrix} 123 \\ 321 \end{pmatrix}} \right\}$$

$$I \quad f_1 \quad f_2 \quad f_3 \quad f_4 \quad f_5$$

Consider the following table

o	I	f_1	f_2	f_3	f_4	f_5
I	Ⓘ	f_1	f_2	f_3	f_4	f_5
f_1	f_1	Ⓘ	f_3	f_2	f_5	f_4
f_2	f_2	f_4	Ⓘ	f_5	f_1	f_3
f_3	f_3	f_5	f_1	f_4	Ⓘ	f_2
f_4	f_4	f_2	f_5	Ⓘ	f_3	f_1
f_5	f_5	f_3	f_4	f_1	f_2	Ⓘ

i) Closure Property : Each element of a table belongs to P_3

e.g. for any $f, g \in P_3$, $fog \in P_3$

∴ P is closed w.r.t. composition of permutations.

ii) Associativity

For any $f, g, h \in P_3$

$$f\,o\,(g\,o\,h) = (fog) \cdot h$$

Hence it is associative

iii) Existence of the Identity Element

By observing, first row and the first column of table

For any $f \in P_3$, $\exists\ I \in P_3$

such that $foI = Iof = f$

∴ I is the identity permutation.

iv) Existence of the Inverse

From table, identify the identity element I,

As $I\,o\,I = I \Rightarrow I^{-1} = I$

$f_1 o f_1 = I \Rightarrow f_1^{-1} = f_1$

$f_2 o f_2 = I \Rightarrow f_2^{-1} = f_2$

$f_3 o f_4 = I = f_4 o f_3 \Rightarrow f_3^{-1} = f_4$ and $f_4^{-1} = f_3$

$f_5 o f_5 = I \Rightarrow f_5^{-1} = f_5$

∴ Every element of P has inverse in P_3.

Hence $(P_3, \cdot)$ is a group.

But $f_1 o f_2 \neq f_3$ and $f_2 o f_1 = f_4$

$\Rightarrow$ $f_1 o f_2 \neq f_2 o f_1 \Rightarrow$ It is not commutative.

$\Rightarrow (P_3, o)$ is not abelian group.

(P_3, o) is the smallest non abelian group.

5.7 Complexes and Subgroups

- Depending upon the nature of subset of a group there are two types of subsets, which are given below.

5.7.1 Complex of a Group

- Let $(G, *)$ be a group. Any non empty subset of a group G is called a complex of the group.

e.g. $H_1 = \{1, 2, 3, 4, 5\}$,

$H_2 = \{1, 2, 3, ...\}$, $H_3 = Z$

are complexes of a group $(\Re +)$

5.7.2 Subgroup

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

Examples

1) $(Z, +)$ is a subgroup of $(\Re +)$
2) $(\Re +)$ is a subgroup of $(\mathbb{C}, +)$
3) $(N, +)$ is not a subgroup of $(Z, +)$
4) $(\Re_0, \cdot)$ is a subgroup of $(\mathbb{C}_0, \cdot)$
5) $(\{1\}, \cdot)$ is a subgroup of $(Q_0, \cdot), (\Re_0, \cdot), (\mathbb{C}_0, \cdot)$
6) $(\Re +)$ is a subgroup of $(\Re +)$

Note :

1) {e} and {G} are subgroups of group G : These subgroups are called improper subgroups.
2) Subgroups which are not improper are called proper subgroups.

5.7.3 Properties of Subgroup

Theorem I) : Prove that the identity element of a subgroup is the same as that of the group.

Proof : Let H be a subgroup of the group G.
Let e and e' be the identities of G and H respectively.

Now, $a \in H \Rightarrow e' a = a$ ... [$\because$ e' is identity of H]

also $a \in H \Rightarrow a \in G \Rightarrow ea = a$

$e'a = ea$ [$\because$ e is identity of G]

$\therefore$ in G we have,

$\Rightarrow$ $e' = e$

... [by right cancellation law in G]

Theorem II) : Prove that the inverse of any element of a subgroup is the same as the inverse of the same regarded as an element of the group.

Proof : Let H be a subgroup of the group G.
Let e be the identity of G as well as of H.

Let $a \in H$, suppose b is the inverse of a in H and c is the inverse of a in G. Then we have,

$ba = e$

and $ca = e$

$\therefore$ in G we have, $ba = ca \Rightarrow b = c$

Theorem III) : Prove that the order of any element of a subgroup is the same as the order of the element regarded as a member of the group.

Proof : Let H be a subgroup of the group G.
Let $a \in H$, But $a \in G$ and $a^n = e$ in G.

$a^n = e$ in H also. Hence the proof.

Theorem IV) : A necessary and sufficient condition for a non-empty subset H of a group G to be a subgroup is that $a \in H, b \quad H \Rightarrow ab^{-1} \in H$ where b^{-1} is the inverse of b in G.

Proof : Suppose H is a subgroup of G.
Let $a \in H$, $b \in H$. Now each element of H must possesses inverse because H itself is a group.

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

Further H must be closed with respect to multiplication i.e. the composition in G.

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

Sufficient condition : Now it is given that $a \in H, b \in H \Rightarrow ab^{-1} \in H$. We have to prove that H is a subgroup of G.

(i) Existence of identity :

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

... By given condition

$\Rightarrow e \in H$

Thus the identity e is an element of H.

(ii) Existence of inverse : Let a be any element of H. Then by the given condition, we have,

$e \in H, a \in H \Rightarrow ea^{-1} \in H \Rightarrow a^{-1} \in H.$

Thus each element of H possesses inverse.

(iii) **Closure property :** Let $a, b \in H$. Then as shown above $b \in H \Rightarrow b^{-1} \in H$. Therefore applying the given condition we have,

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

(iv) **Associativity :** The elements of H are also the elements of G. The composition in G is associative. Therefore, it must also be associative in H.

Hence H itself is a group for the composition in G. Therefore, H is a subgroup of G.

Theorem V) : If H and K are any two elements of a group G, prove that $(HK)^{-1} = K^{-1} H^{-1}$

Proof : Let $h k \in HK \Rightarrow h \in H$ and $k \in K$

$\Rightarrow h, k \in G$ as $H \subseteq G, k \subseteq G$

$\Rightarrow h k \in G$

$\Rightarrow (hk)^{-1} = k^{-1} h^{-1} \in G$

Consider

$$(HK)^{-1} = \{(hk)^{-1} / h k \in HK\}$$

$$= \{k^{-1}h^{-1} / h \in H \text{ and } k \in K\}$$

$$= \{k^{-1}h^{-1} / h^{-1} \in H \text{ and } k^{-1} \in K\}$$

$$= K^{-1} H^{-1}$$

Theorem VI : If H and K are subgroups of G, then H K is a subgroup of G iff

$$HK = KH$$

Proof : Let H and K be subgroups of G, then we know that

$$HH^{-1} = H \text{ and } K K^{-1} = K$$

and $$H^{-1} = H \text{ and } K^{-1} = K \quad \ldots (5.7.1)$$

Part 1) Suppose HK is a subgroup of G

Claim : Prove that HK = KH

HK is a subgroup of G $\therefore (HK)^{-1} = HK$

$\Rightarrow$ $$K^{-1} H^{-1} = H K \quad \ldots \text{by (5.7.1)}$$

$$K H = H K$$

Part 2) conversely, suppose KH = HK

Claim : Prove that HK is a subgroup of G. we know that H is a subgroup of G

We know that H is a subgroup of G iff $HH^{-1} = H$

$\therefore$ prove that $(HK)(Hk)^{-1} = HK$

consider L.H.S $= (HK)(HK)^{-1} = (HK)(K^{-1} H^{-1})$

$= H(k K^{-1}) H^{-1}$

$= H(K) H^{-1}$ $(\because k k^{-1} = k)$

$= (HK) H^{-1}$ $(\because$ By associativity$)$

$= (KH) H^{-1}$ $(\because H K = K H)$

$= K(HH^{-1})$

$= K H = HK$

Hence HK is a subgroup of G.

Theorem VII) : If H_1 and H_2 are two subgroups of a group G, then $H_1 \cap H_2$ is also a subgroup of G.

AKTU : 2014-15

Proof : Let H_1 and H_2 be any two subgroups of G. Then $H_1 \cap H_2 \neq \phi$ Since at least the identity element e is common to both H_1 and H_2.

In order to prove that $H_1 \cap H_2$ is a subgroup it is sufficient to prove that

$$a \in H_1 \cap H_2, b \in H_1 \cap H_2 \Rightarrow ab^{-1} H_1 \cap H_2$$

Now, $a \in H_1 \cap H_2 \Rightarrow a \in H_1$ and $a \in H_2$

$a \in H_1 \cap H_2 \Rightarrow b \in H_1$ and $b \in H_2$

But H_1, H_2 are subgroups.

$\therefore$ $a \in H_1, b \in H_1, \Rightarrow ab^{-1} \in H_1$

$a \in H_2, b \in H_2 \Rightarrow ab^{-1} \in H_2$

Finally $ab^{-1} \in H_1$, $ab^{-1} \in H_2 \Rightarrow ab^{-1} \in H_1 \cap H_2$

Thus, we have shown that, $a \in H_1 \cap H_2$, $b \in H_1 \cap H_2 \Rightarrow ab^{-1} \in H_1 \cap H_2$ Hence $H_1 \cap H_2$ is a subgroup of G.

Theorem VIII) : Show that the union of two subgroups is a subgroup if and only if one is contained in the other.

Proof : Suppose H_1 and H_2 are two subgroups of a group G.

Let $H_1 \subseteq H_2$ or $H_2 \subseteq H_1$

Then $H_1 \cup H_2 = H_2$ or H_1.

But H_1, H_2 are subgroups and therefore, $H_1 \cup H_2$ is also a subgroup. **Conversly** suppose $H_1 \cup H_2$ is a subgroup. To prove that $H_1 \subseteq H_2$ or $H_2 \subseteq H_1$.

Let us assume that H_1 is not a subset of H_2 and H_2 is also not a subset of H_1.

Now H_1 is not a subset of $H_2 \Rightarrow \exists\ a \in H_1$ and $a \notin H_2$ (5.7.2)

and H_2 is not a subset of $H_1 \Rightarrow \exists\ b \in H_2$ and $B \notin H_1$ (5.7.3)

From equation (5.7.2) and (5.7.3).

We have, $a \in H_1 \cup H_2$ and $b \in H_1 \cup H_2$

Since $H_1 \cup H_2$ is a subgroup, therefore $ab = c$ (say) is also an element of $H_1 \cup H_2$.

But $ab = c \in H_1 \cup H_2 \Rightarrow ab = c \in H_1$ or H_2

Suppose $ab = c \in H_1$

Then $b = a^{-1} c \in H_1$, ... [$\because H_1$ is a subgroup. $\therefore a \in H_1 \Rightarrow a^{-1} \in H_1$]

But from (5.7.3), we have $b \in H_1$. Thus we get the contradiction.

Again suppose $ab = c \in H_2$

Then, $a = cb^{-1} \in H_2$ ... [$\because H_2$ is a subgroup, therefore $b \in H_2, \Rightarrow b^{-1} \in H_2$]

But from (5.7.2), we have $a \notin H_2$. Thus here also we get a contradiction.

Hence either $H_1 \subseteq H_2$ or $H_2 \subseteq H_1$

Ex. 5.7.1 : Is union of two subgroups is a subgroup ? If not, give example.

Sol . : The union of two subgroups is not necessarily a subgroup.

Let $H_1 = \{\ldots, -4, -2, 0, 2, 4, 6, \ldots\}$

$H_2 = \{\ldots, -6, -3, 0, 3, 6, \ldots\}$ are subgroup of $(\mathbf{Z}, +)$

Now $H_1 \cup H_2 = \{-6, -4, -3, -2, 0, 2, 3, 4, 6, \ldots\}$

$2, 3 \in H_1 \cup H_2$ but $2 + 3 = 5 \notin H_1 \cup H_2$

$\therefore$ + is not binary operation on $H_1 \cup H_2$

$\Rightarrow$ $H_1 \cup H_2$ is not a subgroup of G.

Ex. 5.7.2 : If a is any element of a group G then prove that $\{a^n / a \in \mathbf{Z}\}$ is a subgroup of G.

Sol. : Let a be an arbitrary element of a group G.

Let $H = \{a^n / n \in \mathbf{Z}\}$

We know that H is a subgroup of G iff $ab^{-1} \in H \forall\ a, b \in H$

Let $x = a^n, y = a^m, m, n \in Z$

Consider $xy^{-1} = a^n(a^m)^{-1}$

$= a^{n-m} \in H$ as $n - m \in Z$

$\therefore H$ is a subgroup of G

5.8 Cosets

Let $(G, *)$ be a group and H be any subgroup of G. Let $a \in G$ be any element, then the set

$H*a = \{h*a / \forall h \in H\}$ is called a right coset of H in G.

and

$a*H = \{a*h / \forall h \in H\}$ is called a left coset of H in G.

Note :

1) $H*a$ and $a*H$ are subsets of G.
2) If $(G, *)$ is an abelian group then $H*a = a*H$ in G.

e.g. 1) Let $(Z, +)$ is a group and

$H = \{...., -10, -5, 0, 5, 10, ...\}$ is a subgroup of $G = Z$

$\therefore$ For $1 \in Z$, $H+1 = \{...., -9, -4, 1, 6, 11, ...\}$

$3 \in Z$, $H+3 = \{...., -7, -2, 3, 8, 13, ...\}$

$5 \in Z$, $H+5 = \{...., -5, 0, 5, 10, ...\} = H$

are right cosets of H in G.

$2 + H = \{...., -8, -3, 2, 7, 12, ...\}$

and $1 + H = \{...., -9, -4, 1, 6, ...\}$

are left cosets of H in G.

Theorem 1 : Any two right cosets of a group are either identical or disjoint.

Proof : Let Ha and Hb be any two right cosets of H in G, where $b \in G$

Claim : Prove that $Ha \cap Hb = \phi$ or $Ha = Hb$

Suppose Ha and Hb are not disjoint i.e. $Ha \cap Hb = \phi$

$\therefore \exists x \in Ha \cap Hb \Rightarrow x \in Ha$ and $x \in Hb$

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

$\Rightarrow x = h_1 a = h_2 b$

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

$\Rightarrow Ha = H(h_1^{-1} h_2) b = (Hh_1^{-1} h_2) b$

$\Rightarrow Ha = Hb$ $(\because H = Hh_1^{-1} h_2)$

i.e. If two right cosets are not disjoint then they are identical.

Hence either $Ha \cap Hb = \phi$ or $Ha = Hb$

Theorem 2 : If H is any subgroup of a group G then G is equal to the union of all right cosets of H in G i.e. $G = H \cup Ha \cup Hb \cup Hc$ where a, b, c ... $\in G$.

Proof : Let $x \in G$ and $e \in H$ then $ex \in Hx$

$\therefore x \in Hx$, Thus for any $x \in G$, x belongs to any one of the right coset of H.

$\therefore G \subseteq H \cup Ha \cup Hb \cup \cdots \cup Hx \cdots$ ... (5.8.1)

where a, b, c, ... x ..., $\in G$

Let $y \in H \cup Ha \cup Hb \cup \cdots$

$\therefore \exists$ some $d \in G$ such that $y \in Hd$

As $H \subseteq G$ and $d \in G$, therefore $y \in Hd \Rightarrow y \in G$

$\therefore H \cup Ha \cup Hb \cup \cdots \subseteq G$ ... (5.8.2)

From (5.8.1) and (5.8.2), we get $G = H \cup Ha \cup Hb \cup \cdots$

Theorem 3 : Show that the set of the inverse of the elements of a right coset is a left coset or more precisely show that $(Ha)^{-1} = a^{-1}H$

Proof : We have $Ha = \{ha / h \in H \text{ and } a \in G\}$

Consider : $(Ha)^{-1} = \{(ha)^{-1} / h \in H, a \in G\}$

$= \{a^{-1}h^{-1} / h \in H, a \in G\}$

$= \{a^{-1}h^{-1} / h^{-1} \in H, a^{-1} \in G\}$

$= \{a^{-1}h, / h^{-1} = h_1 \in H, a^{-1} \in G\}$

$= a^{-1}H$ Hence the proof

5.9 Order of an Element of a Group

- Let $(G, \cdot)$ be a group. The smallest positive integer is called the order of an element $a \in G$ if

$$a^n = e \text{(identity element in G)}$$

If is denoted by $o(a) = n$.

- If no such positive number exists, then we say that a is of infinite order or zero order.

Note :

1) For the order of the group is the number of distinct elements in G.
2) The order of the identity element is 1 i.e. $o(e) = 1$
3) In a group G, $o(a) = o(a^{-1})$; $\forall a \in G$
4) In a group G, $o(a) \leq o(G)$

Examples

Ex.5.9.1 : If $G = \{1, -1, i, -i\}$ is a multiplicative group. Find order of each element of G.

Sol. : We have,

1 = Identity element in G and $o(G) = 4$

$o(1) = 1$

$o(-1) = 2$ as $(-1)^2 = 1$

$o(i) = 4$ as $(i)^4 = 1$

$o(-i) = 4$ as $(-i)^4 = 1$

2) $(Z, +)$ is a group of infinite order

o is the identity element, $o(O) = 1$

We have $5 \in Z$ and $5^n = 5 + 5 + \ldots$ n times $= n5 \neq 0$

$\therefore o(5) =$ infinity or zero

5.10 Cyclic Group

AKTU : 2013-14

- A group G is called a cyclic group if $\exists$ at least one element $a \in G$ such that every element $x \in G$ can be written as $x = a^m$ where m is some integer.

The element a is called the generator of G and denoted by $G = \langle a \rangle$

Ex.5.10.1 : Show that four fourth roots of unity form a cyclic group with respect to multiplication.

AKTU : 2013-14

Sol. : We have,

$$G = \{1, -1, i, -i\}$$

We have $(i)^1 = i$, $(i)^2 = -1$, $(i)^3 = -i$, $(i)^4 = 1$

$\therefore$ i is the generator of $G \Rightarrow G$ is a cyclic group.

Moreover, $(-i)^1 = -i$, $(-i)^2 = -1$, $(-i)^3 = i$, $(-i)^4 = 1$

$\therefore$ $-i$ is also generator of G

$\therefore$ $G = \langle i \rangle = \langle -i \rangle$

Ex.5.10.2 : Show that $G = \{(1, 2, 4, 5, 7, 8), X_9\}$ cyclic. How many generators are there ? What are they ?

AKTU : 2015-16

Sol. : Consider the following table.

X	1	2	4	5	7	8
1	[1]	2	4	5	7	8
2	2	4	8	[1]	5	7
4	4	8	7	2	[1]	5
5	5	[1]	2	7	8	4
7	7	5	[1]	8	4	2
8	8	7	5	4	2	[1]

By this table,

i) X_9 is closed in G.

ii) X_9 is associative in G.

iii) Existance of the identity in G. 1 is the identity element.

iv) Existance of the inverse of each element in G.

$1^{-1} = 1$, $2^{-1} = 5$, $5^{-1} = 2$, $4^{-1} = 7$,

$7^{-1} = 4$, $8^{-1} = 8$

$\therefore$ G is a group w.r.t. X_9.

Moreover, G is an abelian group.

Now,

$2^1 = 2$, $2^2 = 4$, $2^3 = 8$, $2^4 = 7$, $2^5 = 5$, $2^6 = 1$

Hence 2 is the generator of G.

Thus G is a cyclic group.

2 is the only one generator of G.

5.11 Normal Subgroups

- A subgroup H of a group $(G, *)$ is said to be a normal subgroup of G if for all $g \in G$ and for all $h \in H$

$g * h * g^{-1} \in H$ (We may write $g\,h\,g^{-1} \in H$)

- Every group G possesses at least two normal subgroups namely {e} and G. These groups are called improper normal subgroups.

Simple Group : A group G is said to be simple group if it has only two normal subgroups, {e} and G.

Notes :

1) Every subgroup of an abelian group is normal.
2) The intersection of normal subgroups is a normal subgroup.

Example 1 : $(Z, +)$ is an abelian group.
$\therefore (2Z, +), (3Z, +)$ are normal subgroups of $(Z, +)$

Theorem 1 : Lagranges theorem : The order of each subgroup of a finite group is a divisor of the order of the group. **AKTU : 2013-14, 2014-15, 2016-17**

Proof : Let G be a group of finite order n. Let H be a subgroup of G and let O (H) = m. Suppose $h_1, h_2 \ldots h_m$ are the m members of H.
Let $a \in G$. Then Ha is a right coset of H in G and we have

$$Ha = \{h_1 a, h_2 a, \ldots\ldots, h_m a\}$$

Ha has m distinct members, since $h_i a = h_j a \Rightarrow h_i = h_j$.

Therefore each right coset of H in G has m distinct members. Any two distinct right cosets of H in G are disjoint i.e. they have no element in common. Since G is a finite group, the number of distinct right cosets of H in G will be finite, say equal to K. The union of these K distinct right cosets of H in G is equal to G.

Thus, if $Ha_1, Ha_2, \ldots\ldots Ha_k$ are the K distinct right cosets of H in G, then

$$G = Ha_1 \cup Ha_2 \cup \ldots\ldots\ldots \cup Ha_k$$

$\Rightarrow$ The number of elements in G = The number of elements in Ha_1 + The number of elements in Ha_2 + ... + The number of elements in Ha_k

... [$\because$ two distinct right cosets are mutually disjoint]

$\Rightarrow$ O (G) = Km $\Rightarrow$ n = Km

$\Rightarrow$ $K = \frac{n}{m} \Rightarrow$ m is a divisor of n

$\Rightarrow$ O (H) is a divisor of O (G).

Theorem 2 : The order of every element of a finite group is a divisor of the order of the group.

Proof : Suppose G is a finite group of order n.
Let $a \in G$ and O (a) = m. Prove that m is a divisor of n.

Let $H = \{\ldots\ldots, a^{-3}, a^{-2}, a^{-1}, a^0, a^1, a^2, a^3, \ldots..\}$ be the subset of G consisting of all integral powers of a.

We know that H is a subgroup of G.

We have to show that H contains only m distinct elements and that they are $a, a, a^2, a^3, \ldots\ldots, a^m$

$= e\ a^0$

Let $1 \le r \le m$, $1 \le s \le m$, and $r > s$.

then
$a^r = a^s \Rightarrow a^r a^{-s} = a^s a^{-s} \Rightarrow a^{r-s} \Rightarrow a^0 \Rightarrow a^{r-s} = e$

Thus there exists a positive integer r – s less than m such that $a^{r-s} = e$. m is the least positive integer such that $a^m = e$.

$\therefore$ $a^r \neq a^s$

$\therefore$ $a, a^2, a^3, \ldots\ldots, a^m = a^0 = e$ are all distinct elements of H.

Now suppose at is any element of H where t is any integer.

By division algorithm,

We have, $t = mp + q$

... [p and q are some integers, $0 \le q < m$]

We have, $a^t = a^{mp+q}$

$= a^{mp} a^q$

$= (a^m)^p a^q = a^q \quad \ldots (0 \le q < m)$

$\therefore a^q$ is one of the m element $a, a^2, \ldots\ldots, a^m = a^0$

Hence, H has only m distinct elements. Thus order of H is m.

By Lagrange's theorem m is a divisor of n.

Theorem 3 : If G is a finite group of order n and $a \in G$, then $a^n = e$.

Proof : In a finite group, the order of each element is finite. Let O (a) = m. The subset H of G consisting of all integral powers of a is a subgroup of G and the order of H is m.

By Lagrange's theorem, m is a divisor of n.

Let $k = \frac{n}{m}$ then $n = mk$

Now, $a^n = a^{mk} = (a^m)^k = e^k$

$\ldots O(a) = m \Rightarrow am = e$

$= e$

Theorem 4 : Every cyclic group is an abelian group.

AKTU : 2016-17

Proof : 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 $x = a^1$, $y = a^s$.

Now, $xy = a^r a^s = a^{r+s} = a^{s+r} = a^s a^r = yx$

Thus, we have, $xy = yx \; \forall \; x, y \in G$.

Therefore G is abelian.

Theorem 5 : If a is a generator of a cyclic group G, then a^{-1} is also a generator of G.

Proof : Let G = {a} be a cyclic group generated by a.

Let a^1 be any element of G, where r is some integer.

as $a^r = (a^{-1})^{-r}$

$\therefore -r$ is also some integer.

$\therefore$ Each element of G, is generated by a^{-1}

Thus, a^{-1} is also a generator of G.

Theorem 6 : Every group of order 3 is cyclic.

AKTU : 2014-15

OR

Every group of prime order is cyclic.

Proof : Suppose G is a finite group whose order is a prime number P, then to prove that G is a cyclic group. As an integer P is said to be a prime number if $P \neq 0$, $P \neq \pm 1$, and if the only divisors of P are ± 1, $\pm P$.

$\because$ G is a group of prime order, therefore G must contain at least 2 elements.

As 2 is the least positive prime integer.

There must exist an element $a \in G$ such that $a \neq e$ the identity element e.

Since a is not the identity element, therefore O (a) is definitely ≥ 2.

Let O (a) = m, If H is the cyclic subgroup of G generated by a then

$$O(H) = O(a) = m.$$

By Lagrange's theorem m must be divisor of P.

But P is prime and $m \ge 2$. Hence m = P

$\therefore$ H = G. Since H is cyclic. Therefore G is cyclic and a is a generator of G.

Theorem 7 : Every subgroup of a cyclic group is cyclic.

Proof : Suppose G = {a} is a cyclic group generated by a. If H = G or {e}, then obviously H is cyclic. So let H be a proper subgroup of G. The elements of H are integral powers of a. If $a^s \in H$, then the inverse of a^s.

i.e. $a^{-s} \in H$.

$\therefore$ H contains elements which are positive as well as negative integral powers of a.

Let m be the least positive integer such that $a^m \in H$.

Then we shall prove that $H = \{a^m\}$

i.e. H is cyclic and is generated by a^m.

Let a^1 be any arbitrary element H.

By division algorithm,

there exist integers q and r such that

$t = mq + r,\ 0 \le r < m.$

Now, $a^m \in H \Rightarrow (a^m)^q \in H$

... by closure property

$\Rightarrow a^{mq} \in H \Rightarrow (a^{mq})^{-1} \in H$

$\Rightarrow a^{-mq} \in H$

Also, $a^t \in H \cdot a^{-mq} \in H \Rightarrow a^t q^{-mq} \in H$

$\Rightarrow a^{t-mq} \in H$

$\Rightarrow a^r \in H.$

Now m is the least positive integer such that $a^m \in H$ and $0 \le r < m$.

Therefore r must be equal to 0. Hence $t = mq$.

$\therefore \quad a^t = a^{mq} = (a^m)^q$

Thus every element $a^t \in H$ is of the form $(a^m)\ q$.

Therefore H is cyclic and a^m is a generator of H.

Theorem 8 : A subgroup H of a group G is normal iff

$$xHx^{-1} = H\ ;\ \forall x \in G$$

Proof : Let H be a normal subgroup of a group G. Let $x \in G$ be an arbitrary element then $x^{-1} \in G$.

Claim : Prove that $xHx^{-1} = H$

As H is a normal subgroup of G, $xhx^{-1} \in H\ ;\ \forall h \in H$ and $x \in G$

$\therefore \quad xHx^{-1} \subseteq H$ ... (5.11.1)

Now, Let $x^{-1} \in G$

$\therefore \quad x^{-1}H(x^{-1})^{-1} \subseteq H$

$\Rightarrow x^{-1}Hx \subseteq H$

$\Rightarrow xx^{-1}Hxx^{-1} \subseteq xHx^{-1}$

$\Rightarrow \quad eHe = H \subseteq xHx^{-1}$ ... (5.11.2)

$\therefore$ from (5.11.1) and (5.11.2) $H = xHx^{-1}$

Conversely suppose H is a subgroup of a group G such that

$$xHx^{-1} = H,\ \forall x \in G$$

$\therefore$ For any $x \in H$ and $h \in H$

$xhx^{-1} \in xHx^{-1} = H$

Hence H is a normal subgroup of G.

Theorem 9 : Let $(H, \cdot)$ be a normal subgroup of a group $(G, \cdot)$ and

$N = \{ x / x \in G \text{ and } xHx^{-1} = H \}$. Show that $(N, \cdot)$ is a subgroup of $(G, \cdot)$

Proof : Given that $(H, \cdot)$ is a normal subgroup of $(G, \cdot)$ and

$$N = \{ x / x \in G \text{ and } xHx^{-1} = H \}$$

Claim : Prove that N is a subgroup of G.

i.e. prove that $x, y \in N \Rightarrow xy \in N$ and $x^{-1} \in N$.

Let $x, y \in N \therefore xHx^{-1} = H$ and $yHy^{-1} = H$

$\Rightarrow \quad x(yHy^{-1})\ x^{-1} = H \qquad (\because H = yHy^{-1})$

$\Rightarrow \quad (xy)\ H(y^{-1}x^{-1}) = H$

$\Rightarrow \quad (x\ y)\ H(x\ y)^{-1} = H$

$\Rightarrow \quad xy \in N$

Now, let $x \in N \Rightarrow xHx^{-1} = H$

$\Rightarrow \quad (x^{-1})\ H(x^{-1})^{-1} = H \quad (\because x \in G \Rightarrow x^{-1} \in G)$

$\Rightarrow \quad x^{-1} \in N$

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

Hence N is a subgroup of G.

Theorem 10 : A subgroup H of a group G is a normal subgroup of G iff each left coset of H in G is a right coset of H in G.

Proof : Let H be a normal subgroup of group G.

Claim : Prove that $xH = Hx\ \forall x \in G$

As H is a normal subgroup in $G \Rightarrow xHx^{-1}$

$= H, \forall x \in G$

$(xHx^{-1})x = Hx \Rightarrow xH(x^{-1}x) = Hx$

$\Rightarrow xH = Hx$

Conversely, suppose $xH = Hx$

$\Rightarrow xHx^{-1} = Hxx^{-1} = He = H$

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

Theorem 11 : The intersection of any two normal subgroups of a group G is a normal subgroup of G.

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

$\therefore$ $H \cap K$ is a subgroup of G

Let $x \in H \cap K \Rightarrow x \in H$ and $x \in K$

$\Rightarrow gxg^{-1} \in H$ and $gxg^{-1} \in k$; $\forall g \in G$

$\Rightarrow gxg^{-1} \in H \cap K$; $\forall g \in G$

Hence $H \cap k$ is a normal subgroup of G

Theorem 12 : If H is a subgroup of index 2 in a group G, then H is a normal subgroup of G.

Proof : Given that a subgroup H is of index 2 in G so, the number of distinct right cosets of H in G is 2. i.e. [G ; H] = 2

Claim : Prove that H is a normal subgroup of G i.e. show that $Hx = XH$; $\forall x \in G$

Let $x \in G$ then $x \in H$ or $x \notin H$

If $x \in H$ then $xH = H = Hx \Rightarrow Hx = xH$

If $x \notin H$ then $Hx \neq H$,

But $G = H \cup Hx = He \cup Hx = H \cup xH$

$\Rightarrow$ $H \cup Hx = G$ and $xH \cup H = G$

$\Rightarrow$ $Hx = G - H$ and $xH = G - H$

$\Rightarrow$ $Hx = xH$

Hence H is a normal subgroup of G

Theorem 13 : Prove that every subgroup of a cyclic group is normal.

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

Let $H = \{g^n / n \in z\}$

Let $a \in G$ then $a = g^m$, $m \in z$ as $H \subseteq G$

Now $aH = \{ah / h \in H\}$

$= \{g^m g^k / g^k \in H \text{ and } k \in z\}$

$= \{g^{m+k} / g^k \in H \text{ and } k \in z\}$

$= \{g^{k+m} / g^k \in H \text{ and } k \in z\}$

$= \{g^k g^m / g^k \in H \text{ and } k \in z\}$

$= \{ha / h \in H \text{ and } a \in G\}$

$= Ha$

Hence H is a normal subgroup of G.

Theorem 14 : Prove that every subgroup of an abelian group is normal subgroup.

Proof : Let G be an abelian group and H is a normal subgroup of G.

Let $x \in G$ and $h \in H$

Consider $xhx^{-1} = xx^{-1}h = eh = h \in H$

i.e. for any $x \in G$, $h \in H \Rightarrow xhx^{-1} \in H$

Hence H is a normal subgroup of G.

Examples :

Ex.5.11.1 : Give an example of a finite abelian group which is not cyclic.

Sol. : Let G be the set of the four real matrices.

$I = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$, $A = \begin{bmatrix} -1 & 0 \\ 0 & 1 \end{bmatrix}$, $B = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$, $C = \begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix}$

It can be easily seen that G is an abelian group with respect to multiplication of matrices.

The identity element of this group is the identity matrix I.

Let us find the order of each element of G.

We have, $O(I) = I$

Also,

$$A^2 = \begin{bmatrix} -1 & 0 \\ 0 & 1 \end{bmatrix}\begin{bmatrix} -1 & 0 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} = I \qquad [\because O(A) = 2]$$

$$B^2 = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}\begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} = I \qquad [\because O(B) = 2]$$

$$C^2 = \begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix}\begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} = I \qquad [\because O(C) = 2]$$

Now G is a group of order 4 and G contains no element of order 4.

Therefore G is not a cyclic group. Hence G is a finite abelian group which is not cyclic.

Ex.5.11.2 : Show that the multiplicative group {1, –1} is a subgroup of the multiplicative group {1, –1, i, –i}

Sol. : Let H = {1, –1} and G = {1, –1, i, –i}, H ⊂ G.

Consider the composition table

X	1	–1
1	1	–1
–1	–1	1

(i) **Closure property :** All elements of a table belong to H. Hence it is closed w.r.t. multiplication.

(ii) **Multiplication** of complex numbers is associative.

(iii) **Existence of the identity :** 1 ∈ H, is the identity element.

(iv) **Existence of the inverse :** We have, $(1)^{-1} = 1$ and $(-1)^{-1} = -1$.

Therefore, (H, X) is a subgroup of a group (G, X).

Ex.5.11.3 : Define the subgroup of a group. Let (G, 0) be a group. Let H = {a | a ∈ G and aob = boa for all b in G}. Show that H is normal subgroup of G. AKTU : 2012-13

Sol. : Let (G, x) be a group. A non empty subset H of a group G is said to be a subgroup of G if (H, *) itself is a group.

Given that,

$H = \{a \mid a \in G \text{ and } a \circ b = b \circ a ;\ \forall\, b \in G\}$

Let

$$a, b \in H \Rightarrow a \circ x = x \circ a$$

and $b \circ x = x \circ b, \ \forall\, x \in G.$

$$\Rightarrow (b \circ x)^{-1} = (x \circ b)^{-1}$$

$$\Rightarrow x^{-1} \circ b^{-1} = b^{-1} \circ x^1 \qquad \ldots (1)$$

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

Now,

$$(a \circ b^{-1}) \circ x = a \circ (b^{-1} \circ x) \qquad [\because \circ \text{ is associative}]$$

$$= a \circ (x \circ b^{-1}) \qquad [\because \text{use (1) or } b^{-1} \in H]$$

$$= (a \circ x) \circ b^{-1} \qquad [\because a \in H]$$

$$= (x \circ a) \circ b^{-1}$$

$$= x \circ (a \circ b^{-1})$$

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

Therefore H is a subgroup of group G.

Let h ∈ H and g ∈ G and any x in G.

Consider,

$$(g \circ h \circ g^{-1}) \circ x = (g \circ g^{-1} \circ h) \circ x \qquad [\because h \in H]$$

$$= (e \circ h) \circ x = h \circ x$$

$$= x \circ h \qquad (\because h \in H)$$

$$= x \circ (h \circ g \circ g^{-1})$$

$$= x \circ (g \circ h \circ g^{-1}) \qquad (\because h \in H)$$

$$\Rightarrow \quad g \circ h \circ g^{-1} \in H \text{ for any } g \in G$$

∴ H is a normal subgroup of G.

Ex.5.11.4 : Show that the set {1, w, w^2} is a cyclic group of order 3 with respect to multiplication, w is the cube root of unity.

Sol.: Let G = {1, w, w^2} and $w^3 = 1$

We have,

$$1 = 1^1 = w^3 = (w^2)^3$$

$$w = w^1 = (w^2)^2$$

$$w^2 = w^2 = (w^2)^1$$

Thus every element of G can be expressed in the powers of w or w^2. Therefore G is cyclic group and its generators are w and w^2.

Ex.5.11.5 : Let G = {1, – 1, i, – i} where $i = \sqrt{-1}$ and multiplication is the binary operation in G.

(I) Determine whether G is an abelian group.

(II) If G is a cyclic group then find its generators.

(III) Find the order of each element of G.

Sol. :

(I) Let $G = \{1, -1, i, -i\}$.

The composition table of G with respect to multiplication is given below.

X	1	–1	i	–i
1	(1)	–1	i	–i
–1	–1	(1)	–i	i
i	i	– i	–1	(1)
–i	–i	i	(1)	–1

(i) Closure property : All elements of the table belong to G. Therefore G is closed w.r.t. X.

(ii) Associativity : The multiplication of complex numbers is associative. ∴ (G, X) is associative.

(iii) Existence of the identity : 1 ∈ G is the identity element.

(iv) Existence of the inverse : From table

$(1)^{-1} = 1$, $(i)^{-1} = -i$, $(-1)^{-1} = -1$, $(-i)^{-1} = i$

(v) Commutativity : The composition table is symmetric about main diagonal.

∴ (G, X) is commutative.

Thus (G, X) is an abelian group.

(II) We have, $(i)^4 = 1$, $(i)^1 = i$, $(i)^2 = -1$, $(i)^3 = -i$

$(-i)^4 = 1$, $(-i)^1 = -i$, $(-i)^2 = -1$, $(-i)^3 = -i$

Thus every element of G can be expressed as i^n or $(-i)^n$

∴ (G, X) is a cyclic group with i and – i generators.

(III) We have, $1^1 = 1$, $(-1)^2 = 1$, $(i)^4 = 1$ and $(-i)^4 = 1$.

∴ The orders of 1, –1, i, –i are 1, 2, 4, 4 respectively.

Ex.5.11.6 : Show that the four permutations I, (a b), (c d), (a b) (c d) on four symbols a, b, c, d form a finite abelian group with respect to the multiplication.

Sol. :

Let $f_1 = I = \begin{pmatrix} a & b & c & d \\ a & b & c & d \end{pmatrix}$

$f_2 = (a\ b) = \begin{pmatrix} a & b & c & d \\ b & a & c & d \end{pmatrix}$

$f_3 = (c\ d) = \begin{pmatrix} a & b & c & d \\ a & b & d & c \end{pmatrix}$

$f_4 = (a\ b)\ (c\ d) = \begin{pmatrix} a & b & c & d \\ b & a & d & c \end{pmatrix}$

Let $G = \{f_1, f_2, f_3, f_4\}$

Consider the multiplication table

X	f_1	f_2	f_3	f_4
f_1	(f_1)	f_2	f_3	f_4
f_2	f_2	(f_1)	f_4	f_3
f_3	f_3	f_4	(f_1)	f_2
f_4	f_4	f_3	f_2	(f_1)

(i) Closure property : All elements of table belong to G. (G, x) is closed w.r.t. x.

(ii) Multiplication of permutations is associative.

(iii) $f_1 = I$ is the identity element in G.

(iv) In G, $f_1^{-1} = f_1$, $f_2^{-1} = f_2$, $f_3^{-1} = f_3$ and $f_4^{-1} = f_4$

v) Multiplication table is symmetric about main diagonal ∴ (G, x) is commutative.

Hence (G, x) is an ablein group of order 4.

5.12 Factor Group (Quotient Group)

- Let (G, *) be a group and N be a normal subgroup of G. Let G/N be the collection of all cosets of N in G.

$$G/N = \{N*a / a \in G\}$$

- (G/N, *) is called the quotient group or factor group.

Theorem 1) Prove that (G/N, *) is a group.

Sol. : Let (G, *) be a group and N is the normal subgroup at G

∴ $G/N = \{N*a / \forall a \in G\}$

i) Closure Property : Let $a, b \in G, \therefore N*a, N*b \in G/N$

$(N*a)*(N*b) = N*(a*N)*b$ ($\because$ N is normal)

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

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

$= N*c$ ($\because$ $N*N = N$ and $a*b = c \in G$)

$\therefore (N*a)*(N*b) \in G/N$

$\therefore$ G/N is closed w.r.t. *

ii) Associativity : Let $a, b, c \in G$

and $N*a$, $N*b$ and $N*c \in G/N$

$\therefore (N*a)*[(N*b)*(N*c)] = N*a*[N*(b*c)]$

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

$= N*(a*b)*c)$ (* is associative in G)

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

$= [(N*a)*(N*b)]*(N*c)$

$= [(N*a)*(N*b)]*(N*c)$

Thus * is associative in G/N

iii) Existence of the identity :

We have $N = N*e \in G/N$ and for any $N*a \in G/N$

$(N*a)*(N*e) = N*(a*e)$ (by (1))

$= N*a$

$\therefore$ $N*e = N$ is the identity element in G/N.

iv) Existence of the inverse : Let $a \in G$, $N*a \in G/N$

$\therefore \exists\ a^{-1} \in G$ and $N*a^{-1} \in G/N$ such that

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

Hence $N*a^{-1}$ is the inverse of $N*a$ in G/N

Thus (G/N, *) is a group, known as quotient group.

5.13 Homomorphism of Groups

Let $(G_1, *)$ and (G_2, o) be two groups. A function $f : (G_1, *) \to (G_2, o)$ is said to be homomorphism, if $f(a*b) = f(a)\ o\ f(b)$ for all $a, b \in G_1$.

i.e. $a*b$ in $G_1 \to f(a)\ o\ f(b)$ in G_2

Remarks :

i) A one-one homomorphism is called **Monomorphism**

ii) A homomorphism from G to itself is called as **Endomorphism.**

iii) An onto homomorphism is called **Epimorphism.**

Properties of Group Homomorphism

1) Let $f : G_1 \to G_2$ be group homomorphism and $(G_1, *)$ and (G_2, o) are groups then

i) $f(e_1) = (e_2)$

ii) $f(a^{-1}) = [f(a)]^{-1}$

iii) If o(a) is finite, then o(a) is a divisor of o[f(a)]

Proof : i) Let $a \in G_1$ and $f(a) \in G_1$ and e_2 is the identity element in G_2.

$\therefore$ $f(a)oe_2 = f(a)$

$= f(a*e_1)$

$f(a)oe_2 = f(a)\ o\ f(e_1)$

$\Rightarrow f(e_1) = e_2$

ii) Let $a \in G_1$ then $a^{-1} \in G$

and $e_2 = f(e_1)$

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

$e_2 = f(a)\ o\ f(a^{-1})$

($\because$ f is homomorphism)

$\Rightarrow$ $f(a^{-1}) = [f(a)]^{-1}$

iii) Let $a \in G$ and $o(a) = m$, we have

$a^m = e_1$

$f(a^m) = e_1$

$f(a,a, \ldots a) = f(e_1)$

$f(a)f(a) \ldots$ m times $= e_2$

$[f(a)]^m = e_2$

If n is the order of f(a) in G_2 then n is the divisor of m.

5.14 Isomorphism of Groups

- Let $(G_1, *)$ and (G_2, o) be two groups. A function $f : (G_1, *) \to (G_2, o)$ is said to be isomorphism if,

i) f is a homomorphism from $G_1 \to G_2$

ii) f is bijective function.

- If $f : G_1 \to G_2$ is an isomorphism of groups then G_1 and G_2 are called as isomorphic groups and denoted by $G_1 \cong G_2$.
- An isomorphism from G to itself is called as Automorphism of group G.

5.15 Kernel of Homomorphism

- If f is a homomorphism of a group G_1 into a group then $k = \{ x \in G / f(x) = e_2$ where e_2 is the identity of $G_2\}$ is called the Kernel of the homomorphism. It is also denoted by Ker(f)

Theorem 1 : If f is a homomorphism of a group G_1 into group then the kernel k of f is a normal subgroup of G_1.

Proof : Given that f $G_1 \to G_2$ is a homomorphism. Let e_1 and e_2 be the identity elements of G_1 and G_2 respectively.

$\therefore$ $\ker(f) = k = \{ x \in G_1 / f(x) = e_2\}$

We have,

$f(e_1) = e_2 \therefore e_1 \in K$ Therefore K is non empty set

Let a, b, $\in K$

$\therefore$ $f(a) = f(b) = e_2$

Consider :

$$f(ab^{-1}) = f(a) \cdot f(b^{-1})$$
$$= f(a) \cdot [f(b)]^{-1} \quad [\because f(x^{-1}) = [f(x)]^{-1}]$$
$$= e_2 \cdot [e_2]^{-1} \quad (\because e_2^{-1} = e_2)$$
$$= e_2 \cdot e_2 = e_2$$

Hence $f(ab^{-1}) = e_2$

Thus, for any $a, b \in k$, $ab^{-1} \in k$

Therefore k is a subgroup of G_1

Let x be any arbitrary element of G_1 and $a \in k$

$\therefore$ $f(x a x^{-1}) = f(x) \cdot f(a) f(x^{-1})$

$= f(x)\, e_2\, f(x^{-1}) \quad (\because f(a) = e_2)$

$= f(x)\, [f(x)]^{-1}$

$f(x a x^{-1}) = e_2$

$\therefore$ $x a x^{-1} \in k$

Thus for any $x \in G_1$ and $a \in K \Rightarrow x a x^{-1} \in k$

Hence K is a normal subgroup of G_1.

Theorem 2 : The homomorphism $f : G_1 \to G_2$ is an isomorphism if and only if kernel of f is $k = \{e_1\}$.

Proof : Let $f : G_1 \to G_2$ be a homomorphism. Let e_1, e_2 be the identify elements in G_1 and G_2 respectively.

Let $k = \{ x \in G / f(x) = e_2\}$

Suppose f is an isomorphism, we have to prove that $k = \{e_2\}$

Let $a \in k \Rightarrow f(a) = e_2$ and $f(e_1) = e_2$

$\Rightarrow$ $f(a) = f(e_1)$ ($\because$ f is 1 – 1 function)

$\Rightarrow$ $a = e_1$

2) $a = e$

i.e. $a \in k \Rightarrow a = e_1$

Hence $k = \{e_1\}$

Conversely, suppose $k = \{e_1\}$

Claim : prove that f is an isomorphism of G_1 into G_2

Let $a, b \in G_1$ and $f(a) = f(b)$

$\Rightarrow$ $f(a)\, [f(b)]^{-1} = f(b) [f(b)]^{-1}$

$\Rightarrow$ $f(a)\, f(b^{-1}) = e_2$

$\Rightarrow$ $f(ab^{-1}) = e_2$

$\Rightarrow$ $ab^{-1} \in k$, But $k = \{e_1\}$

$\Rightarrow$ $ab^{-1} = e_1$

$ab^{-1}b = e_1\, b$

$a = b$

$\therefore$ f is one - one function

Hence f is an isomorphism

Theorem 3 : Let f be an automorphism of G and N be a normal swbgroup of G, then show that f(N) is a normal subgroup G.

Proof : Given that N is a normal subgroup of G.

Claim : Prove thta f(N) is a normal subgroup of G.

Let $a, b \in f(N) \Rightarrow a = f(n_1)$ and $b = f(n_2)$ where $n_1, n_2 \in N$

$\Rightarrow n_1 n_2^{-1} \in N$

$\Rightarrow f(n_1 n_2^{-1}) \in f(N)$

$\Rightarrow f(n_1) f(n_2^{-1}) \in f(N)$

$\Rightarrow f(n_1)[f(n_2)]^{-1} \in f(N)$

$\Rightarrow a b^{-1} \in f(N)$

Hence, f (N) is a subgroup of G

Let $x \in G$ and $k = f(n) \in f(N)$; $n \in N$

Consider

$xkx^{-1} = x f(n) x^{-1}$ ($\because$ f is onto $\exists\, y \in G$ s.t. $x = f(y)$)

$= f(y) f(n) f(y)^{-1}$

$= f(y) f(n) f(y^{-1}) = f(y n y^{-1})$

As N is normal subgroup $y n y^{-1} \in N \Rightarrow f(y n y^{-1}) \in f(N)$

Hence $xKx^{-1} \in f(N)$

Thus f(N) is a normal subgroup of G.

Theorem 4 : Every homomorphic image of a group G_1 is isomorphic to some quotient group of G_1.

Proof : Let $f : G_1 \to G_2$ be a homomorphism and k be the kernel of f.

$\therefore$ $k = \{ a \in G_1 / f(a)$

$= e_2$ where e_2 is the identity in G_2 $\}$

We know that k is a normal subgroup of G_1

Let $G_1 / k = \{ka / a \in G_1\}$ be a quotient group or factor group.

Claim : prove that $G_1 / k \cong G_2$

Let $\phi : G_1 / k \to G_2$ defined as $\phi(ka) = f(a)$; $\forall a \in G_1$

If $a, b \in G_1$, supposer ka = kb

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

$\Rightarrow f(a) f(b^{-1}) = e_2$

$\Rightarrow f(a) [f(b)]^{-1} = e_2$

$\Rightarrow f(a) [f(b)]^{-1} f(b) = e_2 [f(b)]$

$\Rightarrow f(a) e_2 = f(b)$

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

$\therefore$ ϕ is well defined.

Now, show that ϕ is 1 - 1.

We have $\phi(ka) = \phi(kb)$

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

$f(a) [f(b)]^{-1} = f(b) [f(b)]^{-1}$

$f(a) f(b^{-1}) = e_2$

$f(ab^{-1}) = e_2$

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

$\Rightarrow ka = kb$

$\therefore \phi$ is 1 - 1 function

Now, show that ϕ is onto

Let $y \in G_2$ then $y = f(a)$ for some $a \in G_1$, because f is onto G_2, Now $ka \in G_1 / k$

$\phi(ka) = f(a) = y \Rightarrow \phi$ is onto G_2

consider $\phi[(ka)(kb)] = \phi(kab)$

$= f(ab)$

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

$= \phi(ka) \cdot \phi(kb)$

$\therefore \phi$ is a homomorphism

$\therefore \phi$ is an isomorphism of G_1 / k into G_2

Hence $G_1 / k \cong G_2$

Examples :

Ex.5.15.1 : Let G be a group with identity e show that a function f : G → G defined by f (a) = e, ∀ a ∈ G is a homomorphism (Endomorphism).

Sol. : We have f : G→G and f (a) = e, ∀ a ∈ G.

Let $a, b \in G \Rightarrow f(a), f(b) \in G$

$\therefore \quad f(a * b) = e \qquad$ (as $a * b \in G$)

$= e * e$

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

$\therefore$ f is a homomorphism.

Ex. 5.15.2 : Explain homomorphism and antomorphism of groups with examples.

Sol. : Please refer 5.13 and 5.14 for definition.

e.g. 1) The homomorphism f : (Z, +) → (Z, +) such that

f (n) = − n is an antomorphism of group.

2) The homomorphism f : $(R_o, o) \to (R_o, o)$ such that

f(x) = x; ∀ x ∈ $\Re_o$ is an antomorphism of groups.

Ex.5.15.3 : Let $\Re$ be the additive group of real numbers and $\Re$ + be the multiplicative group of positive real numbers. Prove that the mapping f : (R , +) → ($\Re_+$, X) defined by f (x) = e^x, ∀ x ∈ $\Re$ is an isomorphism of $\Re$ onto $\Re_+$

Sol. : If x is any real number, then e^x is always positive real number and e^x is unique. Therefore, f : $\Re \to R_+$ is a function such that $f(x) = e^x$.

Let $x_1, x_2 \in \Re$ then $f(x_1) = f(x_2)$

$\Rightarrow \quad e^{x1} = e^{x2} \Rightarrow x_1 = x_2$

$\therefore$ f is one to one mapping.

For any $y \in \Re_+$ then $\log y \in \Re$ such that

$f(\log y) = e^{\log y} = y$

$\therefore$ f is onto.

Now for any $x_1, x_2 \in \Re$

Consider, $f(x_1 + x_2) = e^{x_1 + x_2}$

$= e^{x_1 \times x_2}$

$= f(x_1) \times f(x_2)$

$\therefore$ f preserves compositions in $\Re$ and $\Re_+$

$\therefore$ f is an isomorphism of $\Re$ onto $\Re_+$.

Hence $\Re \cong \Re_+$

Ex. 5.15.4 : Show the, the additive group of integers. G = {...., −3, −2, −1, 0, 1, 2, 3, ...} is isomorphic to the additive group G' = {...., − 3m, − 2m, − 1m, 0, 1m, 2m, 3m, ...} where m is any fixed integer not equal to zero.

Sol. : If x ∈ G, then obviously mx ∈ G'

Let f : G → G' be defined by f(x) = mx ∀ x ∈ G

(i) f is one to one. Let $x_1, x_2 \in G$.

Then $f(x_1) = f(x_2)$

$\Rightarrow \quad mx_1 = mx_2$

$\Rightarrow \quad x_1 = x_2$

$\therefore$ f is one to one.

(ii) f is onto : Suppose y is any element of G'.

Then obviously $\frac{y}{m} \in G$. Also $f\left(\frac{y}{m}\right) = m\left(\frac{y}{m}\right) = y$

Thus $y \in G' \Rightarrow$ that there exists $\frac{y}{m} \in G$ such that $f\left(\frac{y}{m}\right) = y$.

$\therefore$ Each element of G' is the f image of some element of G. Hence f is onto. Again if x_1 and x_2 are any two elements of G, then

$f(x_1 + x_2) = m(x_1 + x_2)$ ... by definition of f.

$= mx_1 + mx_2$

... by distributive law for integers

$= f(x_1) + f(x_2)$

Thus f preserves compositions in G and G'. Therefore, f is an isomorphic mapping of G onto G'.

Hence G is isomorphic to G'.

Ex. 5.15.5 : Let f_1 and f_2 be homomorphisms from an algebraic system $(A, 0)$ to another algebraic system $(B, *)$. Let g be a function from A to B such that $g(a) = f_1(a) * f_2(a)$; $\forall a \in A$. Show that g is a homomorphism from $(A, 0)$ to $(B, *)$ if $(B, *)$ is a commutative semigroup.

AKTU : 2012-13

Sol. : Given that $g : (A, 0) \rightarrow (B, *)$ is a function such that $g(a) = f_1(a) * f_2(a)$; $\forall a \in A$.

Where f_1 and f_2 are homomorphism from A to B.

Consider $a, b \in A$ and

$$g(a \circ b) = f_1(a \circ b) * f_2(a \circ b)$$

$$= f_1(a) * f_1(b) * f_2(a) * f_2(b)$$

$$= f_1(a) * f_2(a) * f_1(b) * f_2(b)$$

... as $(B, *)$ is commutative.

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

Thus g is a homomorphism from $(A, 0)$ to $(B, *)$

5.16 Rings, Integral Domains and Fields

- In previous sections, we have discussed an algebraic structures with a single binary operation. Now, we will study an algebraic structures with two binary operations such as rings, integral domains and fields.

5.16.1 Rings

AKTU : 2012-13, 2016-17

- Let R be a non empty set equipped with two binary operations called addition and multiplication and denoted by '+' and '·' respectively.

An algebraic structure $(R, +, \cdot)$ is called a ring if it satisfies following axioms.

1) **$(R, +)$ is an abelian group i.e.**

i) **Closure property :** for $a, b \in R$, $a + b \in R$

ii) **Associativity :** for $a, b, c \in R$, $a + (b + c) = (a + b) + c$

iii) **Existence of the identity :** For any $a \in R, \exists\ o \in R$ s.t., $a + 0 = 0 + a = a$.

$\therefore$ 0 is called as the additive identity element of ring.

iv) **Existence of the inverse :** for each $a \in R, \exists\ -a \in R$ Such that $a + (-a) = -a + a = 0$

$-a$ is called the additive inverse of a

v) **Commutative property :** For $a, b \in R$

$$a + b = b + a$$

2) **$(R, \cdot)$ is semigroup i.e.**

i) Closure property : $\forall a, b \in R, a \cdot b \in R$

ii) Associativity : for $a, b, c \in R$,

$$a \cdot (b \cdot c) = (a \cdot b) \cdot c$$

3) **Multiplication distributes over addition :** $\forall a, b, c \in R$

i) $a \cdot (b + c) = a \cdot b + a \cdot c$ (Right distributive law)

ii) $(a + b) \cdot c = a \cdot c + b \cdot c$ (Left distributive law)

5.16.2 Commutative Ring

A ring $(R, +, \cdot)$ is said to be commutative ring if $\forall a, b \in R, a \cdot b = b \cdot a$

5.16.3 Ring with Unity

A ring $(R, +, \cdot)$ is said to be ring with unity if $\forall a \in R, \exists, 1 \in R$ such that $a \cdot 1 = 1 \cdot a = a$.

Examples :

1) $(Z, +, \cdot)$ is a commutative ring with unity.

2) $(2Z, +, \cdot)$ is a commutative ring without unity where $2Z$ = set of even integers.

3) The set of $n \times n$ matrices over real numbers with respect to usual matrix addition and multiplication is a non commutative ring with unity.

5.16.4 Properties of a Ring

Theorem : 1) If $(R, +, \cdot)$ is a ring with identity 0 and unit element 1 then prove the following result for $a, b, c \in R$.

i) $a \cdot 0 = 0 \cdot a = 0$

ii) $a \cdot (-b) = (-a) \cdot b = -(a \cdot b)$

iii) $(-a) \cdot (-b) = a \cdot b$

iv) $a(b - c) = ab - ac$

Proof : i) We have

$$0 + 0 = 0$$

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

$$a \cdot 0 + a \cdot 0 = a \cdot 0 + 0 \qquad \text{(by cancellation law)}$$

$$a \cdot 0 = 0 \qquad \ldots (5.16.1)$$

Again $0 + 0 = 0$

$$(0 + 0)\, a = 0 \cdot a$$

$$0 \cdot a + 0 \cdot a = 0 \cdot a + 0 \qquad \text{(by cancellation law)}$$

$$\Rightarrow \quad 0 \cdot a = 0 \qquad \ldots (5.16.2)$$

By (5.16.1) and (5.16.2)

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

Hence $a \cdot 0 = 0 \cdot a$

ii) We have $a0 = a(-b + b) \qquad (\because -b + b = 0)$

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

$\therefore$ $a(-b)$ is the additive inverse of ab.

$$\therefore \quad -(ab) = a(-b) \qquad \ldots (5.16.3)$$

Similarly, $0b = (-a + a)\, b$

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

$\therefore (-a)\, b$ is the additive inverse of ab

$$\Rightarrow \quad -(ab) = (-a)b \qquad \ldots (5.16.4)$$

By equations (5.16.3) and (5.16.4)

$$-(ab) = (-a)b = a(-b)$$

Hence the proof

iii) We have

$$(-a)(-b) = -[a(-b)]$$

$$= -[-(ab)] = ab$$

iv) $a(b - c) = a[b + (-c)]$

$$= ab + a(-c)$$

$$= ab + (-ac) = ab - ac$$

5.16.5 Subring

- Let $(R, +, \cdot)$ be a ring. A non empty subset S of R is said to be subring of R if $(S, +, \cdot)$ is a ring. e.g. $(Z, +, \cdot)$ is a subring of $(\Re, +, \cdot)$.

5.16.6 Zero Divisors

AKTU : 2016-17

- Let $(R, +, \cdot)$ be a commutative ring. An element $a \neq 0$ in R is said to be zero divisor if $\exists\ b \neq 0$ in R such that $a \cdot b = 0$.
- A ring $(R, +, \cdot)$ is said to be without zero divisors. if $a \cdot b = 0 \Rightarrow a = 0$ or $b = 0$, $\forall a, b \in R$.

e.g. 1) $\bar{2}$ is a zero divisor in $(Z_4, +, \cdot)$ as $\bar{2} \cdot \bar{2} = \bar{4} = 0$

2) $(M_{2\times 2}(\Re), +, \cdot 1)$ is a ring with zero divisors.

as $$A \cdot B = \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix} \begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix} = 0$$

but $A \neq 0$ and $B \neq 0$

3) $(Z, +, \cdot)$ is a ring without zero divisors i.e. $a \cdot b = 0 \Rightarrow a = 0$ or $b = 0$.

5.16.7 Integral Domain

AKTU : 2012-13

- A commutative ring with zero divisors is called an integral domain.

e.g. 1) $(\Re, +, \cdot)$, $(Z, +, \cdot)$, $(\mathbb{C}, +, \cdot)$ are integral domains.

2) $(Z_4, +, \cdot)$ is a ring with zero divisors

$\therefore$ It is not integral domain.

5.16.8 Field

AKTU : 2012-13

- A commutative ring with unity in which every non zero element possesses their mulplicative inverse, is called as field.

A field is an integral domain.

e.g. 1) $(\Re, +, \cdot)$, $(\mathbb{C}, +, \cdot)$, $(Q, +, \cdot)$ are fields.

2) $(Z, +, \cdot)$ is integral domain but not field.

5.16.9 Ring Homomorphism

- Let $(R, +, *)$ and $(S, +', *')$ be two rings.
- A function $\phi : R \to S$ is called a ring homomorphism
- If for any $a, b \in R$

i) $\phi(a + b) = \phi(a) +' \phi(b)$

ii) $\phi(a * b) = \phi(a) *' \phi(b)$

If ϕ is bijective then it is called as a ring isomorphism.

The kernal of ring homomorphism is defined as the set $\{a \in R / \phi(x) = 0'\}$.

It is denoted by ker (ϕ) or ker ϕ

Examples :

Ex.5.16.1 : Let $R = \left\{ \begin{bmatrix} a & b \\ b & a \end{bmatrix} : a, b \in z \right\}$ **f is the mapping that takes** $\begin{bmatrix} a & b \\ b & a \end{bmatrix}$ **to a – b.**

i) Show that f is a homomorphism.

ii) Find Kernel of f.

Sol. :

$$f = \left(\begin{bmatrix} a & b \\ b & a \end{bmatrix} + \begin{bmatrix} c & d \\ d & c \end{bmatrix} \right) = f \left(\begin{bmatrix} a+c & b+d \\ b+d & a+c \end{bmatrix} \right)$$

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

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

$$= f \left(\begin{bmatrix} a & b \\ b & a \end{bmatrix} \right) + f \left(\begin{bmatrix} c & d \\ d & c \end{bmatrix} \right)$$

Also $f \left(\begin{bmatrix} a & b \\ b & a \end{bmatrix} \right) \cdot \left(\begin{bmatrix} c & d \\ d & c \end{bmatrix} \right) = f \begin{bmatrix} ac+bd & ad+bc \\ bc+ad & bd+ac \end{bmatrix}$

$$= (ac+bd)-(ad+bc)$$

$$= (ac-bc)+(bd-ad)$$

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

$$= f \left(\begin{bmatrix} a & b \\ b & a \end{bmatrix} \right) \cdot f \left(\begin{bmatrix} c & d \\ d & c \end{bmatrix} \right)$$

ii) $\text{Ker } f = \left\{ \begin{bmatrix} a & b \\ b & a \end{bmatrix} : a-b=0 \right\}$

$$= \left\{ \begin{bmatrix} a & a \\ a & a \end{bmatrix} ; a \in z \right\}$$

Ex.5.16.2 : Define two compositions $\oplus$ and $\square$ in $\Re$ set of real number as follows $a \oplus b = a + b + 1$ and $a \square b = ab + a + b$; $\forall a, b \in \Re$ Prove that $(\Re, \oplus, \square)$ is a ring.

Sol. : We have

1) Show that $(\Re, \oplus)$ is an abelian group

a) Closure property : for $a, b \in \Re$, $a \oplus b = a + b + 1 \in \Re$

$\therefore \oplus$ is closed in $\Re$

b) Associativity : $(a \oplus b) \oplus c = (a+b+1) \oplus c$

$= a + b + 1 + c + 1$

$a \oplus (b \oplus c) = a \oplus (b + c + 1) = a + b + c + 1$

$\Rightarrow (a \oplus b) \oplus c = a \oplus (b \oplus c)$ $\therefore \oplus$ is associative in $\Re$

c) Existence of the identity : For any $a \in \Re a \oplus e$

$= e \oplus a = a$

$\Rightarrow a + e + 1 = a \Rightarrow e = -1$ is the identity in $\Re$

d) Existence of the inverse : for any $a \in \Re \exists$ b s t.

$a \oplus b = b \oplus a = e = -1$

$\Rightarrow a + b + 1 = -1 \Rightarrow b = -a - 2 \in \Re \therefore a^{-1} = -a - 2$

e) Commntative property : For any, $a, b \in \Re$

$a \oplus b = a + b + 1 = b + a + 1 = b \oplus a$

$\therefore \oplus$ is commntative in $\Re$

2) Show that $(\Re, \square)$ is a semigroup

a) Closure property : for any $a, b \in \Re$

$a \square b = ab + a + b \in \Re \therefore \square$ is closed in $\Re$

b) Associativity : $(a \square b) \square c = (ab+a+b) \square c$

$= abc + ac + bc + c + ab + a + b$ and $a \square (b \square c)$

$= a \square (bc + b + c) = abc + ab + ac + a + bc + b + c$

$\Rightarrow (a \square b) \square c = a \square (b \square c)$ $\therefore \square$ is associative in $\Re$.

c) Multiplication distributes over addition :

Show that

$a \square (b \oplus c) = (a \square c) \oplus (b \square c)$

L.H.S $= \square (b \oplus c) = a \square (b + c + 1)$

$= ab + ac + a + a + b + c + 1$

R.H.S $= (a \square c) \oplus (b \square c)$

$= (ac + a + c) \oplus (bc + b + c)$

$= ac + a + c + be + b + c + 1$

$\therefore$ L.H.S = R.H.S.

Hence $(\Re, \oplus, \square)$ is a ring.

Ex. 5.16.3 : If any element a has the multiplicative inverse than a can not be a divisor of zero, where the underlying set is a ring.

Sol. : Let R be a ring and $a \in R$ then $a^{-1} \in R$, so that $a \neq 0$.

Claim : Prove that a can not be a divisor of zero. If possible, supposer that a is a divisor of zero so that there exists another element b such that $b \neq 0$ and $ab = 0$

$\therefore$ $ab = 0 \Rightarrow a^{-1}(ab) = a^{-1}0 \Rightarrow (a^{-1}a)b = 0$

$\Rightarrow$ $1.b = 0 \Rightarrow b = 0$ which is the contradiction to the fact that $b \neq 0$.

Hence $a \in \Re$ is not divisor of zero

Ex. 5.16.4 : Prove that A ring R with out zero divisors iff the cancellation laws hold in R.

Sol. : Part I) Suppose that a ring R is without zero divisors so let $a, b, c \in R$ such that $ab = ac$ if $a \neq 0$

$\Rightarrow$ $ab - ac = 0$

$\Rightarrow$ $a(b - c) = 0$

$\Rightarrow$ $a^{-1}a(b-c) = 0$

$b - c = 0$ $\quad b = c$

i.e. $ab = ac \Rightarrow b = c$

$\therefore$ Left concellation law holds in R.

Similarly, we can prove that the right cancellation law also holds in R.

Conversely, suppose that cancellation law holds in R.

If possible suppose that $ab = 0$ and $a \neq 0, b \neq 0$

Now, $ab = 0 \Rightarrow ab = a0$

$\Rightarrow$ $b = 0$

Which is the contradiction.

Hence the ring R is without zero divisors.

Ex. 5.16.5 : Prove that every field is an integral domain,

Sol. : Let (F, +, ·) be a field so that following laws hold :

1) (F,+) is an abelian group

2) (F,·) is an abelian group

3) The distributive law holds

Therefore to prove that F is an integral domain. Show that F is without zero divisors.

Let $ab = 0$ and $a \neq 0$, $a, b \in F$

$\Rightarrow$ $a^{-1}(ab) = a^{-1}0$

$\Rightarrow$ $(a^{-1}a)b = 0$

$\Rightarrow$ $b = 0$

Now $ab = 0$ and $b \neq 0$

$\Rightarrow$ $(ab)b^{-1} = 0b^{-1}$ $\quad a(bb^{-1}) = 0$ $\quad a = 0$

i.e. If $ab = 0$ then either $a = 0$ or $b = 0$

$\therefore$ F is without zero divisors.

Ex. 5.16.6 : Prove that every finite integral domain, is a field.

Sol. : Let (F, +, ·) be a finite integral domain so that it satisfies the following properties.

1) (F, +) is an abelian group

2) F has unity

3) F is commutative

4) F has no zero divisors

5) (F, ·) is semigroup

6) The distributive laws holds in F.

To prove that F is a field, it is sufficient to prove that

a) $\exists$ unit element $1 \in F$ such that $1 \cdot a = a$, $\forall a \in F$

b) The non zero element of F is invertible with respect to multiplication.

Give that F is a finite integral domain

$\therefore$ $F = \{a_1, a_2, a_3, \cdots a_n\}$

$= \{a_i \ / 1 \leq i \leq n\}$

a) Let $a \neq 0 \in F$ then $aa_1, aa_2, aa_3 \ldots aa_n$ are distinct because if they are not distinct, then

$a a_i = a a_j$

$$a(a_i - a_j) = 0$$

$$a_i - a_j = 0$$

$a_i = a_j$ which is contradiction as $|F| = n$

Thus $aa_1, aa_2 \ldots aa_n$ are n distinct elements of F

Placed in some different order.

Now $a \neq 0 \in F \exists\ a a_k \in F$ such that $a a_k = a$

$\Rightarrow$ $a a_k = a \cdot 1$

$\Rightarrow$ $a_k = 1 \in F$

Hence $1 \in F$ is multiplicative identity of F.

b) Now, $1 \in F \Rightarrow \exists\, aa_k \in F$ such that $a a_k = 1$

$\therefore$ $a a_k = 1$

$a_k = a^{-1}1 = a^{-1} \in F$

$\therefore$ a has multiplicative inverse

Hence F is a field.

Ex. 5.16.7 : Show that $S = \{a+b\sqrt{2}\,;\ a, b \in z\}$ for the operations +, × is an integral domain but not a field.

Sol. : We have,

$$(a+b\sqrt{2})+(c+d\sqrt{2}) = (a + c) + (b + d)\sqrt{2}$$

$$(a+b\sqrt{2})+(c+d\sqrt{2}) = (ac + 2bd) + (bc + ad)\sqrt{2}$$

Clearly S is commutative ring with unit element 1.

We have to prove S is an integral domain.

Let $(a+b\sqrt{2})(c+d\sqrt{2}) = 0$

$\therefore$ $ac + 2bd = 0$ ... (1)

and $bc + ad = 0$ ... (2)

Suppose a = 0 ; then bd = bc = 0

either b = 0 or both d = c = 0

Hence, if a = 0, $a+b\sqrt{2} = 0$

or $c+d\sqrt{2} = 0$

Assume $a \neq 0$. Multiplying equation (1) by d

we have, $acd + 2bd^2 = 0$ ... (3)

From equation (2)

$ad = -bc$

Hence substituting this value in equation (3)

We have, $-bc^2 + 2bd^2 = 0$

$\Rightarrow b(2d^2 - c^2) = 0$

$\therefore b = 0$ or $c^2 = 2d^2$, i.e. $c = \sqrt{2}\, d$

Since c is an integer, $c^2 = 2d^2$ is true only if c = d = 0

Hence if $c^2 \neq 2d^2$, b = 0. But b = 0 implies a = 0

Hence, in any case either $a + b\sqrt{2} = 0$ or $c + d\sqrt{2} = 0$

Hence, S is an integral domain.

To show that S is not a field consider the element $2+\sqrt{2}$. It's multiplicative inverse does not exit in S, for $(2+\sqrt{2})(c+d\sqrt{2}) = 1$

$\Rightarrow$ $2c + 2d = 1 \Rightarrow c + d = \frac{1}{2}$

Absurd, since c, d ∈ z.

Ex. 5.16.8 : If R is a ring such that $a^2 = a$, ∀ a ∈ R then prove that a + a = 0 , ∀ a ∈ R. R is a commutative ring. AKTU : 2014-15

Sol. : (i) Let b = − a is the inverse of a,

Now prove that, a = b

Consider, $a - b = (a - b)(a - b)$

$\therefore$ $a - b = a^2 - ba - ab + b^2$

$= a - ba - ab + b$

$= (a + b) - ba - ab$

$\therefore$ $a - b = -ba - ab$

$= -(ba + ab)$ ... (1)

Now, $a + b = (a + b)\ (a + b)$

$= a^2 + ab + ba + b^2$

$= a + ab + ba + b$

$= a + b + (ab + ba)$

$= ab + ba$ ... (2)

But, $a + b = 0$

$\Rightarrow$ $ab + ba = 0$

$\therefore$ Equation (1) $\Rightarrow a - b = 0$

$\Rightarrow$ $a = b$

Ex. 5.16.9 : Consider a ring (R, +, *) defined by a * a = a. Determine whether ring is commutative or not ? AKTU : 2014-15

Sol. : Let $a, b \in R$

and $(a + b)^2 = a + b$

$(a + b)(a + b) = a + b$

$a^2 + ab + ba + b^2 = a + b$

$a + ab + ba + b = a + b$ ... ($\because$ aa = a)

$(a + b) + (ab + ba) = a + b$

$ab + ba = 0$

$\Rightarrow$ $a + b = 0$

$\Rightarrow$ $a + b = a + a$

$\Rightarrow$ $b = a$

$\Rightarrow$ $ab = ba$

$\therefore$ R is commutative ring.

Ex. 5.16.10 : Prove that the set E of all even integers is a commutative ring with respect to usual addition and multiplication, but it has no unit element.

Sol. : Let 2z, be the set of all even integers, then

(i) For any two elements $2m, 2n \in 2z$, $m, n \in z$;

$2m + 2n = 2(m + n) \in 2z$ and

$2m \cdot 2n = (2mn) \in 2z$ and

$2m \cdot 2n = (2mn) \in 2z$,

Since $m + n \in z$ and $2mn \in z$.

(ii) Since (z, +) (z, ·) are associative and commutative, $2z \in z$, so (2z, +) and (2z, ·) are also associative and commutative.

(iii) $0 \in 2z$ such that $a + 0 = 0 + a = a \ \forall\ a \in 2z$.

(iv) For any $2m \in 2z - 2m = (-m) \in 2z \in z$, so " · " is distributive on " + " over 2z.

Hence (2z, + , ·) is a commutative ring but it is not a ring with unity as it does not contain $1 \in E$. (Being the set of all even integers).

Ex. 5.16.11 : Prove that (R, +, *) is a ring with zero divisors, where R is 2 × 2 matrix and + and * are usual addition and multiplication operations.

Sol. : R = { a set of 2 × 2 matrices }

First we show that (R, t) is an abelian group.

(i) **Closure :** Since the sum of two 2 × 2 matrices is also a 2 × 2 matrix closure is satisfied.

(ii) **Associative :** If A, B and C are 2 × 2 matrices then

$$(A_{2\times2} + B_{2\times2}) + C_{2\times2} = A_{2\times2} + (B_{2\times2} + C_{2\times2})$$

always exists.

(iii) **Identity :** The identity element $\begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}_{2\times2}$ belong to R and

$$A + \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix} = A.$$ Identity is satisfied.

(iv) **Inverse :** The inverse of a 2 × 2 matrix say A is always – A which is also 2 × 2 matrix.

(v) **Commutative :** The sum of two matrices is always commutative.

$\therefore$ (R, +) is an abelian group. (R, ·) is also a semigroup w.r.t. multiplication and also multiplication is distributive with respect to addition. Hence (R, ·, +) is a ring.

Now, Let $A = \begin{bmatrix} 2 & 0 \\ 0 & 0 \end{bmatrix}$, $B = \begin{bmatrix} 0 & 0 \\ 0 & 3 \end{bmatrix}$ be two non zero elements of this ring.

Then, we have $AB = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$

Thus the product of two non-zero elements of the ring is equal to the zero element of the ring.

$\therefore$ AB is a ring with zero divisors.

Ex. 5.16.12 : Write out the operation table for $[z_2, +_2, X_2]$ Is z_2 a ring ? Is an integral domain ? Is a field ? Explain.

AKTU : 2011-12

Sol. : The operation tables are as follows :

We have, $z_2 = \{0, 1\}$

+	0	1
0	0	1
1	1	1

×	0	1
0	0	0
1	0	1

Since $(z_2, +_2, x_2)$ satisfies the following properties :

(i) **Closure axiom :** All the entries in both the tables belong to z_2. Hence closure is satisfied.

(ii) **Commutative :** In both the tables all the entries about the main diagonal are same, therefore comutativity is satisfied.

(iii) **Associative law :** The associative law for addition and multiplication are also satisfied.

(iv) **Identity :** Here 0 is the additive identity and 1 is the multiplicative identity. Identity property is satisfied.

(v) **Inverse :** Inverse exists in both the tables. The additive inverse of 0, 1 are 1, 0 and the multiplicative inverse of non-zero element of z_2 is 1.

(vi) **Multiplication :** It is distributive over addition. Hence, $(z_2, +_2, x_2)$ is a ring as well as field. Since we know that every field is an integral domain, therefore it is also an integral domain.

Ex. 5.16.13 : Let $z_8 = \{0, 1, 2, 3, 4, 5, 6, 7\}$. Let R is a relation under the operations addition modulo 7 and multiplication modulo 7. Does this system form a ring ? It is a commutative ring ?

Sol. : Consider the following tables,

Table 1 :

$\times_7$	0	1	2	3	4	5	6	7
0	0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6	0
2	0	2	4	6	1	3	5	0
3	0	3	6	2	5	1	4	0
4	0	4	1	5	2	6	3	0
5	0	5	3	1	6	4	2	0
6	0	6	5	4	3	2	1	0
7	0	0	0	0	0	0	0	0

Table 2 :

$+_7$	0	1	2	3	4	5	6	7
0	0	1	2	3	4	5	6	0
1	1	2	3	4	5	6	0	1
2	2	3	4	5	6	0	1	2
3	3	4	5	6	0	1	2	3
4	4	5	6	0	1	2	3	4
5	5	6	0	1	2	3	4	5
6	6	0	1	2	3	4	5	6
7	0	1	2	3	4	5	6	0

I) S.T. $(z_8, +_7)$ is an abelian group.

i) From table 2, all element are in z_8 $\therefore$ z_8 is closed w.r.t. $+_7$

ii) Associativity : for all a, b $c \in z_8$.

$$a +_7 (b +_7 c) = (a +_7 b) +_7 c$$

iii) By observing the first row of table 2. 0 is the additive identity in z_8.

❑❑❑