Module 3

Groups

Definition:-

If G is a nonempty set and $\circ$ is a binary operation on G, then $(G, \circ)$ is called a group, if the following conditions are satisfied:-

1) for all $a, b \in G$, $a \circ b \in G$ (closure property)

2) for all $a, b, c \in G$, $a \circ (b \circ c) = (a \circ b) \circ c$ (Associative property)

3) There exist $e \in G$ with $a \circ e = e \circ a = a$, for all $a \in G$.
(Existence of identity)

4) For each $a \in G$, there is an element $b \in G$ such that $a \circ b = b \circ a = e$. (Existence of Inverse).

Note:- If together with the above 4 conditions, if $(G, \circ)$ satisfies the property, ~~if $a, b \in G$~~ for all $a, b \in G$, $a \circ b = b \circ a$ (Commutative property), then G is called Commutative or abelian group.

Q) P.T the set Q of all rational numbers ~~other than~~ with operation defined by $a \circ b = a + b - ab$ constitutes an abelian group?

A) To S.T $(Q, \circ)$ is ~~for~~ an abelian group, it should satisfy the conditions.

① Closure property

Let $a, b \in Q$, then

$a \circ b = a+b-ab$ is also rational number

(ie) $a \circ b \in Q$.

∴ closure property is satisfied.

② Associativity

Let $a, b, c \in Q$, then we have to P.T

$a \circ (b \circ c) = (a \circ b) \circ c$.

$L.H.S = a \circ (b \circ c)$

$= a \circ [b+c-bc]$

$= a + [b+c-bc] - a[b+c-bc]$

$= a+b+c-bc-ab-ac+abc \rightarrow ①$

$R.H.S = (a \circ b) \circ c$

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

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

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

$= a+b+c-bc-ab-ac+abc \rightarrow ②$

from ① & ②,

$a \circ (b \circ c) = (a \circ b) \circ c$.

Hence Associativity holds.

③ Existence of identity

Let $e \in Q$ be the identity and ~~$a \in Q$~~ for let $a \in Q$, we have to s.t $a \circ e = a$. [e should be determined]

(i) ~~$a \circ e = a + e - ae$ [by definition]~~

~~$= a + e(1-a)$~~

(ii) $a \circ e = a$

$\Rightarrow a + e - ae = a$, by definition of $a \circ b$.

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

$\Rightarrow e = \frac{0}{1-a} = 0 \in Q$.

Hence the identity exists.

④ Existence of Inverse

Let $a \in Q$, we have to find an element $b \in Q$ such that $a \circ b = e$

(ie) $a \circ b = 0$ [since $e = 0$]

$\Rightarrow a + b - ab = 0$

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

$\Rightarrow b = \frac{-a}{1-a} = \frac{a}{a-1} \in Q$.

∴ the inverse of a (arbitrary) exist in Q.

∴ $(Q, 0)$ is group.

Now $(Q, 0)$ to be an abelian group, it should

Satisfy commutative property.

(ii) for $a, b \in Q$. we have to S.T $a \circ b = b \circ a$.

$L.H.S = a \circ b$

$= a + b - ab \rightarrow (3)$

$R.H.S = b \circ a$

$= b + a - ba \rightarrow (4)$

$\therefore a \circ b = b \circ a$.

$\therefore$ Commutative property holds.

$\therefore (Q, \circ)$ is an abelian group.

Remark:-

1) $(Z, +)$ → set of integers with binary operation addition.

$(R, +)$ → Set of real numbers with binary operation addition.

$(Q, +)$ → set of rational numbers with binary operation addition

These are all abelian groups.

2) $(Z, \cdot)$ → set of integers with binary operation multiplication

This is not a ~~xx~~ group, since no ~~multip~~ inverse exist in Z.

(*) $a * b$ can be also denoted by ab in a group $(G, *)$.

Z_n is the set of all remainders when each $a \in Z$ is divided by n.

(ii) $Z_n = \{0, 1, 2, \ldots, (n-1)\}$ for eg: $Z_3 = \{0, 1, 2\}$

$Z_5 = \{0, 1, 2, 3, 4\}$

4) Addition modulo n denoted by $+_n$ is the remainder obtained when $a+b$ is divided by n.

5) Multiplication modulo n denoted by $\times_n$ is the remainder obtained when $a \cdot b$ is divided by n.

~~Properties of Group~~

~~Properties~~

eg: The set of $n \times n$ non singular matrices $[|A| \neq 0]$ is a group under matrix multiplication with identity matrix of order n as the identity. This group is not abelian because matrix multiplication is not commutative. eg: $A = \begin{bmatrix} 2 & 4 \\ 3 & 2 \end{bmatrix}$ $|A| = -8 \neq 0$ non singular.

Order of a Group

For every group G, the number of elements in G is called the order of G. This is denoted by $|(G, *)|$ or $O(G)$.

When the number of elements in a group is not finite, we say that G has infinite order.

eg: $|(Z, +)|$ has infinite order.

$|(Z_n, +_n)|$ has finite order.

Properties of a Group

Theorem 1] For every group $(G,*)$, P.T

(a) the identity of G is unique.

(b) the inverse of each element of G is unique.

(c) If $a,b,c \in G$ & $ab = ac$, then $b = c$ (left cancellation property)

(d) If $a,b,c \in G$ & $ba = ca$, then $b = c$. (right cancellation property).

Proof:

(a) If possible, let e_1 and e_2 be two identity elements of $(G,*)$. (ii) $e_1, e_2 \in G$. We have to P.T $e_1 = e_2$.

By definition, since e_1 is an identity

$\Rightarrow \forall\ a \in G,\ a * e_1 = a = e_1 * a$.

In particular, let $a = e_2 \in G$, then the above definition can be rewritten as,

$$e_2 * e_1 = e_2 = e_1 * e_2 \longrightarrow (1)$$

Since e_2 is an identity,

$\Rightarrow \forall\ a \in G,\ a * e_2 = a = e_2 * a$.

In particular, let $a = e_1 \in G$, then the above definition can be rewritten as,

$$e_1 * e_2 = e_1 = e_2 * e_1 \longrightarrow (2)$$

From (1) and (2), we have $e_1 = e_2$.

$\therefore$ The identity of G is unique.

Let e be the identity of G.

If possible, let a' and a'' be two inverse of $a \in G$. Then by definition, we have

$$a * a' = e = a' * a \rightarrow (1)$$

so, $$a * a'' = e = a'' * a \rightarrow (2)$$

Now we have to P.T $a' = a''$.

$\therefore a' = a' * e$ (since e is the identity & $a' \in G$.)

$= a' * (a * a'')$, from (2).

$= (a' * a) * a''$, by Associativity property.

$= e * a''$, by (1).

$= a''$, ($\because e$ is the identity)

$\therefore a' = a''$.

$\therefore$ The inverse of each element of G is unique.

(c) Given $a, b, c \in G$ and $ab = ac$.

we have to P.T $b = c$.

$ab = ac \Rightarrow a^{-1}(ab) = a^{-1}(ac)$, (multiplication by a^{-1} on both sides and a^{-1} is the inverse of a)

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

$\rightarrow eb = ec$, (since e is the identity & by definition of inverse)

$\rightarrow b = c$, (by definition of identity).

(d) Given $a, b, c \in G$ and $ba = ca$.

we have to P.T $b = c$.

~~$ba = ba$~~

$ba = ca \Rightarrow (ba)a^{-1} = (ca)a^{-1}$, [multiplication by a^{-1} on both sides and a^{-1} is the inverse of a]

$\Rightarrow b(aa^{-1}) = c(aa^{-1})$, Associativity.

$\Rightarrow be = ce$, [by definition of inverse $\&$ e is the identity]

$\Rightarrow b = c$, by definition of identity.

Theorem 2| For every group $(G, *)$, P.T

~~(a) $(a^{-1})^{-1} = a$, $\forall a \in G$~~

(a) $(ab)^{-1} = b^{-1}a^{-1}$, $\forall a, b \in G$.

Proof.

(a) Let $a^{-1} = b$. ~~$\forall a, b \in G$~~

Then by definition of inverse, we ~~have~~

~~$a * b = e = b * a$.~~

(a) we have to P.T $(ab)^{-1} = b^{-1}a^{-1}$. $\forall a, b \in G$.

(ii) we have to P.T the inverse of ab is $b^{-1}a^{-1}$.

or it is enough if we P.T $(ab)(b^{-1}a^{-1}) = e$, the identity.

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

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

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

$= e$, & $\because a a^{-1} = e$.

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

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

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

Theorem 3 The group $(G,*)$ cannot have an idempotent element except the identity element.

Proof:

[According to idempotent law, $\forall a \in G$, $a * a = a$]

we have to s.t $(G,*)$ cannot have any other idempotent element other than e.

If possible, let a be an idempotent element of $(G,*)$ other than e.

Then $a * a = a$, (by ① idempotent law)

Now, $e = a * a^{-1}$

$= (a * a) * a^{-1}$, by ①

$= a * (a * a^{-1})$, by Associativity

$= a * e$

$= a$.

$\therefore e = a$.

Hence the only idempotent element of G is its identity element.

Remark:

For an abelian group, $(ab)^n = a^n b^n$ and

$n(a+b) = na + nb$, $\forall a, b \in G$ and n is any integer.

Q) Show that any group G is abelian iff $(ab)^2 = a^2 b^2$, for all $a, b \in G$.

A) Given that G is abelian.

we have to P.T $(ab)^2 = a^2 b^2$.

$$(ab)^2 = (ab)(ab)$$
$$= a(ba)b \text{ , (Associativity)}$$
$$= a(ab)b \text{ , (abelian)}$$
$$= (aa)(bb) \text{ , (Associativity)}$$
$$= a^2 b^2.$$

Conversely, Suppose $(ab)^2 = a^2 b^2$.

we have P.T G is abelian.

(ie) we have to P.T $ab = ba$, $\forall a, b \in G$.

~~$(ab)^2 = (ab)(ab)$~~

$(ab)^2 = a^2 b^2 \Rightarrow (ab)(ab) = (aa)(bb)$

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

$\Rightarrow (ba)b = (ab)b$, by left cancellation.

$\Rightarrow ba = ab$, by right cancellation

$\Rightarrow G$ is abelian.

P.T $(Z_6, +_6)$ is an abelian group?

i) We have $Z_6 = \{0, 1, 2, 3, 4, 5\}$.

The composition table is given by,

$+_6$	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

From, the table,

Closure property is attained.

Associative property holds.

Identity element is 0

The inverse of each element is given below,

inverse of 0 is 0
inverse of 1 is 5
inverse of 2 is 4
inverse of 3 is 3
inverse of 4 is 2
inverse of 5 is 1.

Hence $(Z_6, +_6)$ is a group.

Since rows & columns of the table are transpose to each other, $(Z_6, +_6)$ satisfies commutative property.

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

Subgroups

Let $(G, *)$ be a group and $H \subseteq G$ be a non-empty subset of G.

If H is a group under the binary operation of G, then we call H a subgroup of G.

Trivial subgroup

Every group G has $\{e\}$ and G as subgroups. These are called trivial subgroups of G.

All other subgroups are called nontrivial or proper subgroups.

Q) Let G be the set of integers and H be the set of even integers.
S.T $(H, +)$ is a subgroup of $(G, +)$
or H is a subgroup of G.

A) clearly H is a non empty subset of G.
Next to prove H is a subgroup of G, it is enough if we P.T H is a group under addition.

closure property

~~Every even~~ Addition of even integers always given an even integer.
Hence closure property is satisfied.

Associative property

$\forall a, b, c \in H$, set of even integers,

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

$\therefore$ Associativity holds.

Existence of Identity

let $a \in H$., then we have to find an identity element in H under addition and that must be the identity of G.

$$a + e = a$$

$$\Rightarrow a e = a - a = 0.$$

$e = 0$ is also the identity of G.

Hence identity exists in H.

Existence of Inverse

Let $a \in H$ and 0 is the identity of H.

Then $a + a^{-1} = 0$

$$\therefore a^{-1} = -a \in H.$$

$\therefore$ Inverse exists H.

$\therefore$ $(H, +)$ is a group

$\therefore$ H is a subgroup of G.

Theorem 4

If H is a non-empty subset of a group G, then H is a subgroup of G if and only if
(a) for all $a, b \in H$, $ab \in H$ (closure property)
(b) for all $a \in H$, $a^{-1} \in H$. (Existence of Inverse).

Proof:

Given that, H is a non-empty subset of group G.
Suppose that H is a subgroup of G.
∴ we have to P.T the above mentioned two conditions are holding.
Since H is a subgroup of G, by definition of subgroup, H is a group under the same binary operation.
Hence it satisfies all the group conditions, including the two mentioned here.
Conversely,
let the two conditions are holding.
we have to P.T H is a subgroup of G.
According to definition, we have to P.T,
① H is a non-empty subset of G
② H is a group under the same binary operation in G

- H is a non-empty subset of G is already given as hypothesis.
- by (a), closure property is attained.

~~For Associativity~~

associativity,

let $a, b, c \in H \Rightarrow a, b, c \in G$, since $H \subseteq G$

since G is a group, $a*(b*c) = (a*b)*c$ in G

and hence $a*(b*c) = (a*b)*c$ in H.

$\therefore$ Associativity holds in H.

- as $H \neq \phi$, let $a \in H$, by (b), $a^{-1} \in H$ and hence inverse exist in H.

Also by (a), we have $a\,a^{-1} \in H$

$\Rightarrow e \in H$

$\therefore H$ has the identity element.

$\therefore H$ is a group.

$\therefore H$ is a subgroup of G.

Theorem 5 Let $(G, \circ)$ and $(H, *)$ be groups. Define the binary operation $\cdot$ on $G \times H$ by

$(g_1, h_1) \cdot (g_2, h_2) = (g_1 \circ g_2, h_1 * h_2)$. Then

P.T $(G \times H, \cdot)$ is a group.

Proof

Given that $(G, \circ)$ and $(H, *)$ are groups.

we have to S.T $(G \times H, \cdot)$ is a group.

(ie) it is enough to S.T $(G \times H, \cdot)$ satisfies all the four properties.

① Closure Property

let (g_1,h_1) and $(g_2,h_2) \in G \times H$.

we have to P.T $(g_1,h_1)\cdot(g_2,h_2) \in G \times H$.

$g_1, g_2 \in G \Longrightarrow g_1 \circ g_2 \in G \rightarrow$ ①, Since $(G,\circ)$ is a group.

$h_1, h_2 \in H \Longrightarrow h_1 * h_2 \in H \rightarrow$ ②, Since $(H,*)$ is a group.

From ① & ②, we have

$$(g_1 \circ g_2, h_1 * h_2) \in G \times H.$$

$$\Longrightarrow (g_1,h_1)\cdot(g_2,h_2) \in G \times H \text{ [by definition of } \cdot\text{]}$$

∴ closure property is attained.

② Associative Property

let (g_1,h_1), (g_2,h_2) & (g_3,h_3) belongs to $G \times H$.

we have to P.T

$$[(g_1,h_1)\cdot(g_2,h_2)]\cdot(g_3,h_3) = (g_1,h_1)\cdot[(g_2,h_2)\cdot(g_3,h_3)]$$

$$L.H.S = [(g_1,h_1)\cdot(g_2,h_2)]\cdot(g_3,h_3)$$

$$= (g_1 \circ g_2, h_1 * h_2)\cdot(g_3,h_3)$$

$$= (g_1 \circ g_2 \circ g_3, h_1 * h_2 * h_3) \rightarrow ①$$

~~Closed~~, ~~Since $g_1 \circ g_2 \circ g_3 \in G$ & $h_1 * h_2 * h_3 \in H$.~~

$$R.H.S = (g_1,h_1)\cdot[(g_2,h_2)\cdot(g_3,h_3)]$$

$$= (g_1,h_1)\cdot[(g_2 \circ g_3, h_2 * h_3)]$$

$$= (g_1 \circ g_2 \circ g_3, h_1 * h_2 * h_3) \rightarrow ②.$$

from ① & ②,

$$[(g_1,h_1)\cdot(g_2,h_2)]\cdot(g_3,h_3)$$
$$=(g_1,h_1)\cdot[(g_2,h_2)\cdot(g_3,h_3)].$$

∴ Associativity holds.

③ Existence of Identity

Let e_G be the identity of $(G,\circ)$ &
Let e_H be the identity of $(H,*)$.

let $(g,h)\in G\times H$, where $g\in G$ & $h\in H$.

$$(g,h)\cdot(e_G,e_H) = (g\circ e_G, h * e_H)$$
$$= (g,h).$$

Also,
$$(e_G,e_H)\cdot(g,h) = (e_G\circ g, e_H * h)$$
$$= (g,h)$$

∴ $(e_G,e_H)\in G\times H$ is the identity element.

④ Existence of Inverse

Since $(G,\circ)$ is a group, for every $g\in G$, there exist a $g^{-1}\in G$ such that $g\circ g^{-1} = e_G = g^{-1}\circ g$.

Since $(H,*)$ is a group, for every $h\in H$, there exist a $h^{-1}\in H$ such that $h * h^{-1} = e_H = h^{-1} * h$.

Now,
$$(g,h)\cdot(g^{-1},h^{-1}) = (g\circ g^{-1}, h * h^{-1})$$
$$= (e_G,e_H)$$

Also,

$$(g^{-1}, h^{-1}) \cdot (g, h) = (g^{-1} \circ g, h^{-1} * h)$$

$$= (e_G, e_H)$$

Thus, $(g^{-1}, h^{-1}) \in G \times H$ is the inverse of (g, h).

Hence $(G \times H, \cdot)$ is a group.

Remark: The group $(G \times H, \cdot)$ defined above is called a direct product of G & H.

Q) Consider the groups $(Z_2, +_2)$ and $(Z_3, +_3)$. S.T $(Z_2 \times Z_3, \cdot)$ is group, where $\cdot$ is defined as $(a_1, b_1) \cdot (a_2, b_2) = (a_1 +_2 a_2, b_1 +_3 b_2)$, where $a_1, a_2 \in Z_2$ & $b_1, b_2 \in Z_3$.

A) $Z_2 = \{0, 1\}$, $Z_3 = \{0, 1, 2\}$

$Z_2 \times Z_3 = \{(0,0), (0,1), (0,2), (1,0), (1,1), (1,2)\}$.

The Composition Table is given by,

$\cdot$	(0,0)	(0,1)	(0,2)	(1,0)	(1,1)	(1,2)
(0,0)	(0,0)	(0,1)	(0,2)	(1,0)	(1,1)	(1,2)
(0,1)	(0,1)	(0,2)	(0,0)	(1,1)	(1,2)	(1,0)
(0,2)	(0,2)	(0,0)	(0,1)	(1,2)	(1,0)	(1,1)
(1,0)	(1,0)	(1,1)	(1,2)	(0,0)	(0,1)	(0,2)
(1,1)	(1,1)	(1,2)	(1,0)	(0,1)	(0,2)	(0,0)
(1,2)	(1,2)	(1,0)	(1,1)	(0,2)	(0,0)	(0,1).

From the composition table,
closure property is satisfied.
Associative property is satisfied.
The identity element is (0,0).
The inverse of each element is as follows:-

inverse of (0,0) is (0,0)
inverse of (0,1) is (0,2)
inverse of (0,2) is (0,1)
inverse of (1,0) is (1,0)
inverse of (1,1) is (1,2).
inverse of (1,2) is (1,1).

$\therefore [(Z_2 \times Z_3), \cdot]$ is a group.

Q) If G is a group, let $H = \{a \in G \mid ag = ga, \forall g \in G\}$.
P.T H is a subgroup of G.

A) By theorem 4, to prove that H is a subgroup, we need only to prove the closure property and inverse existence in H.

To prove H is closed

let $a_1, a_2 \in H$, we have to P.T $a_1 * a_2 \in H$.

$a_1 \in H \Rightarrow a_1 g = g a_1$, by def^n of H & $g \in G$.

$a_2 \in H \Rightarrow a_2 g = g a_2$, by def^n of H & $g \in G$.

So to P.T $a_1 a_2 \in H$, we need to P.T

$(a_1 a_2) g = g(a_1 a_2)$.

$(a_1 a_2) g = a_1 (a_2 g)$

$= a_1 (g a_2)$, $\because a_2 \in H$.

$= (a_1 g) a_2$, $\because$ Associativity

$= (g a_1) a_2$, $\because a_1 \in H$

$= g(a_1 a_2)$, Associativity

~~$= (a_1 a_2) g$, Commutativity~~

~~$= a_1 a_2$, by right Cancellation~~

$\therefore (a_1 a_2) g = g(a_1 a_2)$

$\Rightarrow (a_1 a_2) \in H$.

$\therefore H$ is closed. or satisfies closure property.

To prove H posses inverse

Let $a \in H$, then $ag = ga$, $\forall g \in G$, by definition of H.

Since G is a group, for $g \in G$, $\exists\ g^{-1} \in G$ s. $gg^{-1} = e$, identity of G.

we have to P.T $a^{-1} \in H$.

(ie) by definition we have to P.T $a^{-1} g = g a^{-1}$.

$a \in H \Rightarrow ag^{-1} = g^{-1} a \Rightarrow (ag^{-1})^{-1} = (g^{-1} a)^{-1}$

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

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

H is a subgroup of G.

3) what is the order of the group $Z_6 \times Z_6 \times Z_6$? Determine the inverse of (2,3,4), (4,0,2) & (5,1,2)?

A) $O(Z_6) = 6 \quad \because Z_6 = \{0,1,2,3,4,5\}$.

$\therefore O(Z_6 \times Z_6 \times Z_6) = O(Z_6) \times O(Z_6) \times O(Z_6)$

$= 6 \times 6 \times 6$

$= 216$

$(2,3,4)^{-1} = (4,3,2)$ $\left[\because \begin{array}{l} 2 +_6 4 = 0 \\ 3 +_6 3 = 0 \\ 4 +_6 2 = 0 \end{array}\right]$

$(4,0,2)^{-1} = (2,0,4)$

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

2) (a) if H, K are subgroups of group G, P.T $H \cap K$ is also a subgroup of G.

(b) Give an example of a group G with subgroups H, K such that $H \cup K$ is not a subgroup of G.

1) (a) Given that H and K are subgroups of G.

Then H is closed and inverse exists

Illly K is closed & inverse exists

since H is closed and K closed

$\Rightarrow H \cap K$ is closed.

Homomorphisms & Isomorphisms

Defn: If $(G,\circ)$ & $(H,*)$ are groups, and $f: G \to H$ be a function.
Then f is called group homomorphism, if for all $a,b \in G$, $f(a \circ b) = f(a) * f(b)$.

Theorem 6
Let $(G,\circ)$ & $(H,*)$ be groups with respective identities e_G & e_H. If $f: G \to H$ is a homomorphism, then

(a) $f(e_G) = e_H$
(b) $f(a^{-1}) = [f(a)]^{-1}$, $\forall\, a \in G$.
(c) $f(a^n) = [f(a)]^n$, $\forall\, a \in G$, and all $n \in \mathbb{Z}$.
(d) $f(S)$ is a subgroup of H, for each subgroup S of G.

Proof:
Given that $(G,\circ)$ and $(H,*)$ be groups.
and $e_G \in G$ be the identity of G &
$e_H \in H$ be the identity of H.
If $e_G \in G$ then $f(e_G) \in H$, since $f: G \to H$.

(a) $e_H * f(e_G) = f(e_G)$, since $e_H, f(e_G) \in H$ & $(H,*)$ is a group with identity e_H
$= f(e_G \circ e_G)$, since $e_G \in G$ and e_G is identity $(G,\circ)$
$= f(e_G) * f(e_G)$, since f is a homomorphism
$= f(e_G)$, by right cancellation.

$e_H = f(e_G)$. or $f(e_G) = e_H$).

$f(a) * f(a^{-1}) = f(a \circ a^{-1})$, since f is homomorphism

$= f(e_G)$, since e_G is the identity of $(G, \circ)$

$= e_H$, by (a).

$\therefore f(a) * f(a^{-1}) = e_H$

$\Rightarrow f(a)$ has the inverse $f(a^{-1})$.

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

(b) To prove this, we use the method of induction.

For $n=1$, $f(a) = [f(a)]^1$

$\Rightarrow f(a) = f(a)$, the result is true.

Assume the result is true for $n-1$.

(ie) $f(a^{n-1}) = [f(a)]^{n-1}$

Now, we will prove that the result is true for n.

(ie) we have to P.T $f(a^n) = [f(a)]^n$.

$\therefore f(a^n) = f(a^{n-1} \circ a)$

$= f(a^{n-1}) * f(a)$, since f is homomorphism

$= [f(a)]^{n-1} * [f(a)]^1$, by assumption

$= [f(a)]^n$.

(a). If S is a subgroup of G, then $S \neq \phi$ and hence $f(S) \neq \phi$.

Now we have to P.T $f(S)$ is a subgroup of H.

by thm 4, we have to P.T $f(S)$ is closed and the inverse exists in H.

To P.T $f(S)$ is closed in H.

let $x, y \in f(S)$, then ~~$x * y \in f(S)$~~. we have to P.T $x * y \in f(S)$.

$x, y \in f(S)$, then $x = f(a)$ and $y = f(b)$, where $a, b \in S$.

Since S is a subgroup of G, $a, b \in S \Rightarrow a \circ b \in S$.

$$x * y = f(a) * f(b) = f(a \circ b), \text{ if is homomorphism}$$

$$\in f(S).$$

$\therefore f(S)$ is closed.

To P.T $f(S)$ posses inverse

let $x \in f(S)$, then we P.T $x^{-1} \in f(S)$.

$x^{-1} = [f(a)]^{-1} = f(a^{-1})$, by (c) and $a \in S$.

$\in f(S)$, since $a \in S$ and S subgroup, hence $a^{-1} \in S$.

$\therefore$ Inverse exists in $f(S)$.

$\therefore f(S)$ is a subgroup of H.

If $f:(G,o)\to(H,*)$ is a homomorphism, we call f an isomorphism if it is one-to-one and onto. In this case, G & H are said to be isomorphic groups.

Cyclic groups

A group G is called cyclic if there is an element $x \in G$ such that for each $a \in G$, $a = x^n$, for some $n \in \mathbb{Z}$.

($a = nx$, if the operation is addition).

Then x is known as the generator of G and is denoted by $G = \langle x \rangle$

Q) S.T the group $(Z_4, +)$ is cyclic.

A) To show that the group $(Z_4, +)$ is cyclic, we have to find atleast one generator for Z_4 under $+_4$ (means $+_4$).

[Since $(Z_4, +)$ is given to be group, no need for checking group].

Since addition, the generator will be that element $x \in Z_4$ that generators the entire set $Z_4 = \{0, 1, 2, 3\}$ using $a = nx$, n is an integer.

The possible generators are 0, 1, 2 & 3.

Consider 0.

$1 \cdot 0 = 0$

$2 \cdot 0 = 0 +_4 0 = 0$

$\therefore$ 0 is not a generator.

Consider 1

$1 \cdot 1 = 1$

$2 \cdot 1 = 1 +_4 1 = 2$

$3 \cdot 1 = 1 +_4 1 +_4 1 = 3$

$4 \cdot 1 = 1 +_4 1 +_4 1 +_4 1 = 0$

$\therefore$ 1 is a generator.

Consider 2

$1 \cdot 2 = 2$

$2 \cdot 2 = 2 +_4 2 = 0$

$3 \cdot 2 = 2 +_4 2 +_4 2 = 2$.

$4 \cdot 2 = 2 +_4 2 +_4 2 +_4 2 = 0$.

$\therefore$ 2 is not a generator.

Consider 3

$1 \cdot 3 = 3$

$2 \cdot 3 = 3 +_4 3 = 2$

$3 \cdot 3 = 3 +_4 3 +_4 3 = 1$

$4 \cdot 3 = 3 +_4 3 +_4 3 +_4 3 = 0$

$\therefore$ 3 is a generator

$\therefore$ The only generators of $(Z_4, +_4)$ is 1 & 3.

$\therefore \langle (Z_4, +_4) \rangle = \langle 1 \rangle = \langle 3 \rangle$.

$\therefore (Z_4, +_4)$ is a cyclic group.

Definition

If G is a group, & $a \in G$, the order of the element, a denoted by $O(a)$ is the smallest positive integer n for which $a^n = e$.

($na = e$ in the case of additive operation).

mark: The order of an element in a cyclic group generated by a is $|\langle a \rangle|$.

Q) write the order of elements of the group $(W_4, \cdot)$

A) $W_4 = \{1, -1, i, -i\}$.

The order of the element is the smallest positive integer n s.t $a^n = 1$ (identity of W_4), $a \in W_4$.

Consider 1

$1^1 = 1$

$\therefore O(1) = 1$

consider -1

$(-1)^1 = -1$

$(-1)^2 = 1$

$\therefore O(-1) = 2$.

consider i

$i^1 = i$

$i^2 = -1$

$i^3 = -i$

$i^4 = 1$

$\therefore O(i) = 4$

consider $-i$

$(-i)^1 = -i$

$(-i)^2 = -1$

$(-i)^3 = i$

$(-i)^4 = 1$

$\therefore O(-i) = 4$.

$\therefore O(1) = 1$

$O(-1) = 2$

$O(i) = 4$

$O(-i) = 4$

Q) Consider the group $(Z_4, +)$. Write the order of the elements of Z_4.

A) $Z_4 = \{0, 1, 2, 3\}$.

The identity element is 0.

∴ The order is the least positive integer such that $na = 0$, $a \in Z_4$.

Consider 0

$1 \cdot 0 = 0$

∴ $O(0) = 1$

Consider 1

$1 \cdot 1 = 1$

$2 \cdot 1 = 1 +_4 1 = 2$

$3 \cdot 1 = 1 +_4 1 +_4 1 = 3$

$4 \cdot 1 = 1 +_4 1 +_4 1 +_4 1 = 0$

∴ $O(1) = 4$

~~Consider 2~~

~~$2 \cdot 1 = 2$~~

~~$3 \cdot 1$~~

Consider 2

$1 \cdot 2 = 2$

$2 \cdot 2 = 2 +_4 2 = 0$

∴ $O(2) = 2$

Consider 3

$1 \cdot 3 = 3$

$2 \cdot 3 = 3 +_4 3 = 2$

$3 \cdot 3 = 3 +_4 3 +_4 3 = 1$

$4 \cdot 3 = 3 +_4 3 +_4 3 +_4 3 = 0$

∴ $O(3) = 4$.

∴ order of the elements of $(Z_4, +_4)$ are

$O(0) = 1$; $O(1) = 4$; $O(2) = 2$; $O(3) = 4$.

~~$O(2)$~~

Note: If $|\langle a \rangle|$ is infinite, we say that a has infinite order.

Mark:-

Every subgroup of a cyclic group is cyclic.

Theorem

A cyclic group is abelian.

Proof:

Let $(G,*)$ be a cyclic group with $a \in G$ as generator.

Let $b,c \in G$, we have to P.T $b*c = c*b$.

Since $b \in G \Rightarrow b = a^n$ } $\rightarrow$ (1)

$c \in G \Rightarrow c = a^m$ }

$b*c = a^n * a^m$, by (1)

$= a^{n+m}$

$= a^{m+n} = a^m . a^n = c*b.$

$\therefore b*c = c*b.$

$\therefore G$ is abelian

Remark:-

1) Every subgroup of a cyclic group is cyclic

2) If 'a' is a generator of a cyclic group, $\{G,*\}$, then 'a^{-1}' is also a generator of $\{G,*\}$.

3) An abelian group need not be cyclic.

Cosets & Lagrange's Theorem

Definition:-

If H is a subgroup of G, then for each $a \in G$, the set $aH = \{ah \mid h \in H\}$ is called the left coset of H in G. The set $Ha = \{ha \mid h \in H\}$ is called the right coset of H in G.

If the operation is addition, we write $a+H = \{a+h \mid h \in H\}$ is the left coset of H in G and $H+a = \{h+a \mid h \in H\}$ is the right coset of H in G.

Remark:-

For an abelian group, $aH = Ha$.
(i.e) left coset = right coset).

Q) Let $(\mathbb{Z}, +)$ and its subgroup $(3\mathbb{Z}, +)$. Find the left & right cosets of $3\mathbb{Z}$ in $\mathbb{Z}$?

~~A) the left cosets~~

A) we have,

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

$$3\mathbb{Z} = \{\ldots, -9, -6, -3, 0, 3, 6, 9, \ldots\}.$$

The left cosets of $(3\mathbb{Z}, +)$ in $(\mathbb{Z}, +)$ are

$$0+3\mathbb{Z} = \{\ldots, -9, -6, -3, 0, 3, 6, 9, \ldots\}$$

$$1+3\mathbb{Z} = \{\ldots, -8, -5, -2, 1, 4, 7, 10, \ldots\}$$

~~$2+3\mathbb{Z} = \{\ldots, -6, -3, 0, 3, 6, 9, 12, \ldots\}$~~

$$2+3\mathbb{Z} = \{\ldots, -7, -4, -1, 2, 5, 8, 11, \ldots\}$$

$0+3\mathbb{Z} = \{\ldots, -6, -3, 0, 3, 6, 9, \ldots\} = 0+3\mathbb{Z}$

Thus we can see that $0+3\mathbb{Z}$, $1+3\mathbb{Z}$ and $2+3\mathbb{Z}$ are the distinct left cosets of $3\mathbb{Z}$ in $\mathbb{Z}$.

The right cosets are,

$3\mathbb{Z}+0 = \{\ldots, -9, -6, -3, 0, 3, 6, 9, \ldots\}$

$3\mathbb{Z}+1 = \{\ldots, -8, -5, -2, 1, 4, 7, 10, \ldots\}$

$3\mathbb{Z}+2 = \{\ldots, -7, -4, -1, 2, 5, 8, 11, \ldots\}$

$3\mathbb{Z}+3 = \{\ldots, -6, -3, 0, 3, 6, 9, \ldots\} = 3\mathbb{Z}+0.$

∴ The distinct right cosets are

$3\mathbb{Z}+0$, $3\mathbb{Z}+1$ and $3\mathbb{Z}+2$.

Remark:

From the above problem, we can see that the union of distinct (left) or right cosets gives the entire set $\mathbb{Z}$.

(ie) $\mathbb{Z} = (0+3\mathbb{Z}) \cup (1+3\mathbb{Z}) \cup (2+3\mathbb{Z})$

Illly, the intersection of distinct left or right cosets is empty.

(ie) $(0+3\mathbb{Z}) \cap (1+3\mathbb{Z}) \cap (2+3\mathbb{Z}) = \phi$.

Thus we can say that "the set of all left (right) cosets of a subgroup H in G forms a partition of G.

Lagrange's Theorem

If G is a finite group of order n with H a subgp of order m, then m divides n.

or

The order of a subgroup H of a finite group G is a divisor of the order of the group G.

Proof:

Given $|G| = n$ & $|H| = m$.

If $H = G$, then the result follows.

Otherwise, if $H \subset G$, (ie) $m < n$ $[o(H) \leq o(G)]$

Then there exist an element $a \in G$ but not in H.

(ie) $a \in G - H$.

Since $a \notin H$, it follows that $aH \neq H$.

which implies $aH \cap H = \phi$.

If $G = aH \cup H$, then $|G| = |aH| + |H| = m + m = 2m = 2|H|$

(ie) $|G| = 2|H| \Rightarrow |G|$ is a multiple of $|H|$.

$\Rightarrow |H|$ divides $|G|$

$\Rightarrow m$ divides n.

∴ The theorem follows.

If not, (ie) $G \neq aH \cup H$.

$\Rightarrow$ There exist an element $b \in G - (H \cup aH)$, with

$bH \cap H = \phi = bH \cap aH$ and $|bH| = |H|$

If $G = bH \cup aH \cup H$, then $|G| = |bH| + |aH| + |H| = 3m = 3|H|$

(ie) $|G|$ is a multiple of $|H|$.

(ii) $|H|$ divides $|G|$.

Otherwise, we are back to an element $c \in G$ with $c \notin bH \cup aH \cup H$. and proceeds as above.
Since the group G is finite, this process terminat
and we find that $G = a_1H \cup a_2H \cup \ldots \cup a_kH$.

$\therefore |G| = k|H|$.

$\therefore |G|$ is a multiple of $|H|$.

$\therefore |H|$ divides $|G|$

(ie) m divides n.

corollary 1: If G is a finite group & $a \in G$, then $O(a)$ divides $|G|$.

corollary 2: Every group of prime order is cyclic.

Algebraic Systems

- A Binary operation on a set A is a function $f: A \times A \to A$
- In general, n-ary operation on A is a function f from $\underbrace{A \times A \times \cdots \times A}_{n \text{ times}} \to A$. (ie) $f: A^n \to A$.
- A set A is said to be **closed** with respect to an operation, if applying the operation on members of A always produce another member of A.
- An algebraic system or algebraic structure is a system consisting of a non-empty set A and one or more n-ary operations on the set A. It is denoted by $(A, f_1, f_2, \ldots, f_n)$, where $f_1, f_2, \ldots, f_n$ are the operations on A.
- Homomorphisms & Isomorphisms

Let $(X, \cdot)$ & $(Y, *)$ be two algebraic system where $\cdot$ & $*$ are both n-ary operations.
A function $f: X \to Y$ is called a homomorphism from $(X, \cdot)$ to $(Y, *)$, if for any $x_1, x_2 \in X$, we have

$$f(x_1 \cdot x_2) = f(x_1) * f(x_2).$$

A homomorphism is known as isomorphism if f is onto & one-to-one. ~~& or~~

If between two algebraic systems $(X, \cdot)$ & $(Y, *)$ an isomorphism exists, then $(X, \cdot)$ & $(Y, *)$ are said to be isomorphic and then the two algebraic systems are structurally indistinguishable.

Binary Operation

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

A) Given $A = \{1,2,3\}$ & $a*b = 2a+2b$.

$1*1 = 2\times1+2\times1 = 4$
$1*2 = 2\times1+2\times2 = 6$
$1*3 = 2\times1+2\times3 = 8$
$2*1 = 4+2 = 6$
$2*2 = 4+4 = 8$
$2*3 = 4+6 = 10$
$3*1 = 6+2 = 8$
$3*2 = 6+4 = 10$
$3*3 = 6+6 = 12$

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

This table is also known as Composition Table.

Closure Property

) Consider the set $A = \{-1,0,1\}$. Determine whether A is closed under ① Addition ② multiplication.

1) ① Here $(-1)+(-1) = -2 \notin A$

Hence A is not closed under addition.

② $-1\times-1 = 1 \in A$ $0\times0 = 0 \in A$ $1\times1 = 1 \in A$
$-1\times0 = 0 \in A$ $0\times-1 = 0 \in A$ $1\times-1 = -1 \in A$
$-1\times1 = -1 \in A$ $0\times-1 = 0 \in A$ $1\times0 = 0 \in A$.

∴ A is closed under multiplication.

W.

Q) Consider the set $A = \{1,3,5,7,9,\ldots\}$, the set of odd +ve integers. Determine whether A is closed under ① addition ② Multiplication.

(1) Here $1+3 = 4 \notin A$ (ii) adding 2 odd no.'s gives an even no.
Hence A is not closed under addition.

(2) The set A is closed under multiplication because multiplication of two odd numbers gives an odd number.

Associative Property

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

3) Consider the binary operation $*$ on Q, the set of rational no.'s, defined by

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

Determine whether $*$ is associative.

4) Let $a, b, c \in Q$; then we have to P.T

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

$L.H.S = (a*b)*c$

$= \underset{a}{(a+b-ab)} * c$, by defn. of $*$

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

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

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

$R.H.S = a*(b*c)$

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

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

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

$= a+b+c-ab-ac-bc+abc \rightarrow ②$

From ① & ②,

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

2)

) Consider the binary operation * & Q, the set of rational no.'s defined by $a*b = \frac{ab}{2}, \forall a,b \in Q.$ Determine Associativity?.

) Let $a,b,c \in Q.$

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

$= \frac{abc}{4} \rightarrow ①$

$R.H.S = a*(b*c) = a*\left(\frac{bc}{2}\right) = \frac{abc}{4} \rightarrow ②$

From ① & ②, $a*(b*c) = (a*b)*c.$

Commutative Property

Consider a non-empty set A and a binary operation * on A. Then * on A is commutative, if $\forall a,b \in A, a*b = b*a.$

1 Consider the binary operation * on Q, set of rational numbers defined by $a*b = a^2+b^2, \forall a,b \in Q.$ Determine Commutivity?

Let $a, b \in A$.

Check $a * b = b * a$.

~~LHS~~ $= a * b = a^2 + b^2 = b^2 + a^2 = b * a$.

$\therefore$ Commutativity holds.

Identity

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

$a * e$ (right identity) $= a = e * a$ (left identity), $\forall a \in A$.

Q) Consider the binary operation * on I_+, the set of positive integers defined by $a * b = \frac{ab}{2}$

Determine the identity for the binary operation *, if exists.

A) Let assume $a \in I_+$ and e be any +ve ~~non~~ integer, then we have to ~~find~~ find e s.t $a * e = a$.

By def^n. $a * e = ad \Longrightarrow \frac{ae}{2} = a$

$\Longrightarrow ae = 2a$

$\Longrightarrow e = \frac{2a}{a} = 2$.

$\therefore$ The identity element $e = 2$.

Inverse

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

$a * b$ (right inverse) $= b * a$ (left inverse) $= e$, then b

is called an inverse of a.

Q) Consider the binary operation * on Q, defined by ~~a*b = a+b-ab, ∀a,b∈Q.~~ $a * b = \frac{ab}{4}$, Determine the inverse, if exists.

A) To find inverse, 1st we have to find the identity element e.

(ie) $a * e = a$.

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

For inverse,

$a * a^{-1} = e \Rightarrow a * a^{-1} = 4$

$\Rightarrow \frac{a a^{-1}}{4} = 4$

$\Rightarrow a a^{-1} = 16$

$\Rightarrow a^{-1} = \frac{16}{a}$.

∴ Inverse of a in Q is 16/a.

Semigroups and Monoids

The algebraic system $(S, *)$ is known as a semigroup, where S is a non-empty set & * is a binary operation which is associative.

If * is commutative, then the semigroup is said to be commutative (or abelian) semigroup.

monoid is a semigroup with the identity

If * is commutative, then monoid is known as commutative or abelian monoid.

or

An algebraic system (A,*), where * is a binary operation on A. Then, the system (A,*) is said to be a Semi-group if it satisfies the following properties:-

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

Q) Consider an algebraic system $(\{0,1\},*)$, where * is a multiplication operation. Determine whether $(\{0,1\},*)$ is a semi group.

A) To check the * is a semigroup, the operation * is closure & Associativity.

Closure property:-

$0*0=0\in\{0,1\}$; $0*1=0\in\{0,1\}$; $1*0=0\in\{0,1\}$;

$1*1=1\in\{0,1\}$.

∴ The operation * is closed.

Associative property —

The operation * is associative, since we have.

$(a*b)*c = a*(b*c)$, $\forall\ a,b,c\in\{0,1\}$.

∴ Since the algebraic system is closed & Associative

Hence * is a semi group

Monoid

Let $N = \{0, 1, 2, 3, \ldots\}$ be the set of Natural Numbers.

Then S.T $(N, +)$ is a monoid.

For a set $(N, +)$ to be monoid, it should satisfy, ① $(N, +)$ must be semigroup

② $(N, +)$ must have an identity element e.

) $(N, +)$ be a Semigroup

closure property

when two natural numbers are added, then the result will be always a natural number.

∴ closure property is satisfied.

Associativity

The operation + defined on the set N is always associative, since

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

∴ Associativity is attained.

② Checking for identity

Let $a \in N$, then by definition of identity,

$a * e = a \implies e = a - a = 0 \in N$.

∴ 0 is the identity element and it is a member of N.

∴ property of identity is attained.

Let Z^+ be the set of positive integers

Then ST $(Z^+, +)$ is not a monoid?

A) ① $(Z^+, +)$ be a semigroup.

closure property

Any ~~post~~ two positive integer in Z^+ when added will again give a positive integer in Z^+.

∴ closure property is attained.

Associative property

Associativity always holds for the set of positive integers, Z^+, since $(a+b)+c = a+(b+c)$, $\forall\ a, b, c \in Z^+$

② checking for identity

Let $a \in N$, then by definition of identity,

$a + e = a \implies e = a - a = 0 \notin Z^+$.

∴ Identity doesnot belong to Z^+.

∴ $(Z^+, +)$ is not a monoid

Result::

Every semigroup need not be monoid.

Subsemigroups

Let $(S, *)$ be a semigroup & $T \subseteq S$. Then $(T, *)$ is said to be a subsemigroup of $(S, *)$, if T is closed under the operation $*$.

Similarly,

Let $(M,*,e)$ be a monoid & $T \subseteq M$. Then $(T,*,e)$ is known as a submonoid of $(M,*,e)$, if T is closed under the operation $*$ and the identity $e \in T$.

Q) Consider the semigroup $(N,+)$.
S.T $(Z^+,+)$ is a subsemigroup of $(N,+)$.

A) Since Z^+ is the set of positive integers $\{1,2,3,\ldots\}$ is a subset of N and
$(Z^+,+)$ is closed under addition,
$(Z^+,+) \subseteq (N,+)$ is a subsemigroup.

Q) Consider the semigroup $(N,+)$. S.T $(T,+)$, where T is the set of odd integers is a subsemigroup?

A) $T = \{1,3,5,\ldots\} \subseteq N = \{1,2,3,\ldots\}$.
Here $(T,+)$ is a not a subsemigroup, since T is not closed under the binary operation $+$.

Q) Consider the monoid $(R,\cdot,1)$, where R is the set of Real no.s. S.T $(N,\cdot,1)$ is a submonoid.

A) $N = \{1,2,3,\ldots\} \subseteq R$.
N is closed under the operation $\cdot$ (multiplication), since when any 2 natural no.s are multiplied, the result will be a natural number.

Now, we have to check whether the identity element of R is an identity element of N and also that element belongs to N.

By defn of identity, e, we have

$\forall a \in N$, $a \cdot e = a$.

$\Rightarrow e = a/a = 1 \in N$.

$\therefore (N, \cdot)$ is a submonoid.

Remark: The set of even positive integer under multiplication is not a submonoid of $(R, \cdot, 1)$.

Homomorphism of Semigroup & Monoids

Let $(S, *)$ and (T, Δ) be any two semigroup. A function $f: S \to T$ is called semigroup homomorphism if for any two elements $a, b \in S$, we have

$$f(a * b) = f(a) \Delta f(b).$$

If f is one-one and onto, then the above semigroup homomorphism can be called as subsemigroup isomorphism.

Let $(M, *, e_M)$ and (T, Δ, e_T) be any two monoids. A function $f: M \to T$ is known as monoid homomorphism if for any $a, b \in M$, we have

$$f(a * b) = f(a) \Delta f(b) \text{ \& } f(e_M) = e_T.$$

5) Let $(N, +, 0)$ and $(N, \cdot, 1)$ be two semigroups. Let $f: N \to N$ be defined as $f(m) = 3^m$, for any $m \in N$.

Then f is a semigroup homomorphism, because $f(m+n) = f(m) \cdot f(n)$ should be satisfied.

$f(m+n) = 3^{m+n} = 3^m \cdot 3^n = f(m) \cdot f(n)$.

Also,

$(N, +)$ and $(N, \cdot)$ are two monoids. and let $f: N \to N$ be defined by $f(m) = 3^m$, for any $m \in N$.

Then f is a monoid homomorphism, because

$f(m+n) = 3^{m+n} = 3^m \cdot 3^n = f(m) \cdot f(n)$

and the identity element for $(N, +)$ is 0 and that of $(N, \cdot)$ is 1.

$\therefore f(0) = 3^0 = 1$ [identity element of $(N, \cdot)$]

Algebraic System with two Operations

Rings

Definition: Let R be a non-empty set together with two closed binary operations '+' & '·'. Then $(R, +, \cdot)$ is a ring if for all $a, b, c \in R$, the following conditions are satisfied:-

(a) $a + b = b + a$ [commutative law of +]

(b) $a + (b + c) = (a + b) + c$ [Associative law of +]

(c) There exist $z \in R$ such that $a + z = z + a = a$, for every $a \in R$. (existence of identity for +)

(d) For each $a \in R$ there is an element $b \in R$ with $a + b = b + a = z$. (Existence of Inverse under +)

(e) $a \cdot (b \cdot c) = (a \cdot b) \cdot c$ [Associative law for ·]

(f) $a \cdot (b + c) = (a \cdot b) + (a \cdot c)$
~~$a + (b \cdot c) = a + b$~~
$(b + c) \cdot a = (b \cdot a) + (c \cdot a)$
} Distributive law of · over +.

Remark: The Properties from (a) to (d) shows that $(R, +)$ is an abelian group.

Q) For the set $I_4 = \{0, 1, 2, 3\}$, show that modulo 4 system is a ring.

A). we have to S.T $(I_4, +_4, \times_4)$ is a ring.

so we have to S.T ① I_4 is closed under $+_4$ & $\times_4$

② I_4 is abelian group under $+_4$

③ I_4 satisfies Associativity & distributive law of $\times_4$.

Composition table for $+_4$ and $\times_4$ is given below

$+_4$	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

$\times_4$	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	0	2
3	0	3	2	1

∴ From the Composition table for $+_4$, we have closure property is attained.
Associativity holds.
The identity is 0
The Inverses are :-
Inverse for 0 is 0
Inverse for 1 is 3
Inverse for 2 is 2
Inverse for 3 is 1.
From the composition table of $+_4$, the rows & columns are transpose to each other, hence commutative.
∴ $(I_4, +_4)$ is an abelian group.
From the composition table of $\times_4$, it is clear that $\times_4$ satisfies closure property.
since I_4 is a number system and $\times_4$ under it is always associative and satisfies distributive law of $\times_4$ over $+_4$.

Q) S.T $(\mathbb{Z}, \oplus, \odot)$ is a ring where $a \oplus b = a+b-1$ and $a \odot b = a+b-ab$. (3)

A) Here $\mathbb{Z}$ is the set of Integers and the operations $\oplus$ & $\odot$ are defined.

To Show that $(\mathbb{Z}, \oplus, \odot)$ is a ring, we have to S.T $(\mathbb{Z}, \oplus)$ is an abelian group & $(\mathbb{Z}, \odot)$ satisfies closure property, Associativity & distributive law for $\odot$ over $\oplus$

1st we S.T $(\mathbb{Z}, \oplus)$ is an abelian group

closure property

Let $a, b \in \mathbb{Z}$, then $a \oplus b = a+b-1 \in \mathbb{Z}$.

∴ closure property is attained.

Associativity

Let $a, b, c \in \mathbb{Z}$, we have to P.T

$(a \oplus b) \oplus c = a \oplus (b \oplus c)$.

L.H.S $= (a \oplus b) \oplus c = (a+b-1) \oplus c$

$= a+b-1+c-1 = a+b+c-2 \rightarrow (1)$

R.H.S $= a \oplus (b \oplus c)$

$= a \oplus (b+c-1) = a+b+c-1-1$

$= a+b+c-2 \rightarrow (2)$

From (1) & (2), L.H.S = R.H.S

∴ $(a \oplus b) \oplus c = a \oplus (b \oplus c)$

∴ Associativity holds.

Existence of Identity

For this, we have to find an element $e \in \mathbb{Z}$ such that $a \odot e = a$.

$\Rightarrow a + e - 1 = a$ [by definition of $\odot$]

$\Rightarrow e = a - a + 1$

$\Rightarrow e = 1 \in \mathbb{Z}$.

$\therefore e = 1$ is the identity

Existence of Inverse

For this, we have to P.T for $a \in \mathbb{Z}$, we have to find an $a^{-1} \in \mathbb{Z}$ such $a \odot a^{-1} = e$.

(ie) $a \odot a^{-1} = 1$ [$\because e = 1$]

$\Rightarrow a + a^{-1} - 1 = 1$ [by definition of $\odot$]

$\Rightarrow a^{-1} = 1 + 1 - a$

$= 2 - a$.

$\therefore$ The inverse a is $(2-a) \in \mathbb{Z}$, since $a \in \mathbb{Z}$.

$\therefore$ Inverse exists.

Commutative property

Let $a, b \in \mathbb{Z}$, we have to S.T $a \odot b = b \odot a$

L.H.S $= a \odot b = a + b - 1 \rightarrow (a)$

R.H.S $= b \odot a = b + a - 1 = a + b - 1 \rightarrow (b)$

From (a) & (b), R.H.S = L.H.S. (ie) $a \odot b = b \odot a$.

$\therefore$ Commutative law holds.

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

Consider $(Z, \odot)$ Let $a, b, c \in Z$.

Associative law for $\odot$

we have to P.T $a \odot (b \odot c) = (a \odot b) \odot c$

L.H.S $= a \odot (b \odot c)$

$= a \odot [b + c - bc]$, by definition of $\odot$.

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

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

R.H.S $= [a \odot b] \odot c$

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

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

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

From (a) & (b), R.H.S = L.H.S.

$\therefore a \odot (b \odot c) = (a \odot b) \odot c$.

$\therefore$ Associativity holds for $\odot$.

Distributive law for $\odot$ over $\oplus$.

we have to P.T $a \odot (b \oplus c) = (a \odot b) \oplus (a \odot c)$ and

$(b \oplus c) \odot a = (b \odot a) \oplus (c \odot a)$

1st we prove $a \odot (b \oplus c) = (a \odot b) \oplus (a \odot c)$

L.H.S $= a \odot (b \oplus c) = a \odot (b + c - 1)$

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

$= a + b + c - 1 - ab - ac + a$

$= 2a + b + c - ab - ac - 1. \longrightarrow (a)$.

$R.H.S = (a \odot b) \oplus (a \odot c)$

$= (a+b-ab) \oplus (a+c-ac)$

$= a+b-ab+a+c-ac-1 = 2a+b+c-ab-ac-1 \rightarrow (b)$

~~$2a+b-ab-ac+$~~

From (a) & (b), $L.H.S = R.H.S$.

(ii) $a \odot (b \oplus c) = (a \odot b) \oplus (a \odot c)$ is proved.

~~Next we prove $(b \oplus c) \odot a = (b \odot a) \odot (c$~~

Next we prove $(b \oplus c) \odot a = (b \odot a) \oplus (c \odot a)$

$L.H.S = (b \oplus c) \odot a$

$= (b+c-1) \odot a$

$= b+c-1+a-(b+c-1)\,a$

$= b+c-1+a-ab-ac+a$

$= 2a+b+c-ab-ac-1 \rightarrow (a)$

$R.H.S = (b \odot a) \oplus (c \odot a)$

$= (b+a-ab) \oplus (c+a-ca)$

$= b+a-ab+c+a-ca-1$

$= 2a+b+c-ab-ac-1 \rightarrow (b)$

From (a) & (b), $L.H.S = R.H.S$.

$\therefore (b \oplus c) \odot a = (b \odot a) \oplus (c \odot a)$ is proved.

$\therefore$ Distributive law of $\odot$ over $\oplus$ is attained.

$\therefore (\mathbb{Z}, \oplus, \odot)$ is a Ring.

Definition

Let $(R,+,\cdot)$ is a ring.

(a) If $ab=ba$, for all $a,b\in R$, then R is called a commutative ring.

(b) The ring R is said to have no proper divisors of zero, if for all $a,b\in R$, $ab=e \Rightarrow a=e$ or $b=e$, where e is the additive identity, (normally 0).
[(ii) $ab=0 \rightarrow$ either $a=0$ or $b=0$].

(c) If an element $u\in R$ is such that $u\neq e$ (identity) and $au=ua=a$, for all $a\in R$, we call u a unity, or multiplicative identity, of R.
Hence R is called a ring with unity.

eg: Consider the above problem, $(Z,\ominus,\odot)$, where $\ominus$ and $\odot$ is defined by, for all $a,b,c\in Z$.
$a\ominus b=a+b-1$ & $a\odot b=a+b-ab$.
we are going to verify that whether ~~this~~ $(Z,\ominus,\odot)$ which is a ring satisfy,

(a) Commutative ring.

(b) no proper divisors of zero

(c) ring with identity.

A)(a) In order, to verify commutative ring, we have to S.T
$a\odot b=b\odot a$, for $a,b\in Z$.

~~a⊙b~~ L.H.S $=a\odot b=a+b-ab$

R.H.S $=b\odot a=b+a-ba=a+b-ab$

Here, L.H.S = R.H.S $\therefore a\odot b=b\odot a$.

$\therefore (Z, \oplus, \odot)$ is a commutative ring.

(b) In order to P.T no proper divisors of zero, we have to P.T $a \odot b = 1 \odot$ (since $\odot 1$ is the identity element of $\odot$) we have to S.T either $a=1$ or $b=1$.

$$a \odot b = 1 \implies a+b-ab = 1$$

if $a=1$, then $1+b-b=1$

$1+0=1$

$1=1$, which is true.

if $b=1$, then $a+1-a=1$

$0+1=1$

$1=1$, which is true.

$\therefore$ if $a \odot b = 1$, then either $a=1$ or $b=1$.

$\therefore (Z, \oplus, \odot)$ has no proper divisors of zero.

(c) In order to P.T ring with unity, we have to find an element $u \in R$ such that $u \neq e$ & $a \odot u = u \odot a = a$, for $a \in R$.

Here $e=1$.

$\therefore a \odot u = a$

$\implies a+u-au = a$

$\implies a+u(1-a) = a$

$\implies u(1-a) = 0$

$\implies u = 0 \neq 1 = e$.

$\therefore$ The integer $u=0$ is the unity of Z.

$\therefore (Z, \oplus, \odot)$ is a ring with unity.

Definition

Let R be a ring with unity u. If $a \in R$ and there exist $b \in R$ such that $ab = ba = u$, then b is called a multiplicative inverse of a and a is called a unit of R.

Definition

Let R be a commutative ring with unity. Then

(a) R is called an integral domain of R if R has no proper divisors of zero.

(b) R is called a field if every non-zero element of R is a unit.

Note :-

1. Every field is a ring.
2. Every field is an integral domain but every integral domain is not a field.
3. Every finite integral domain is a field.

Subring

A subset A of a ring $(R, +, \cdot)$ is called a subring of R, if it satisfies following conditions:-

(i) $(A, +)$ is a subgroup of a group $(R, +)$.

(ii) A is closed under the multiplication operation.

(ii) if $a, b \in A$, then $a \cdot b \in A$.

Note :-

1) If R is a ring, then $\{0\}$ & R are subrings of R.

2) Sum of two subrings may not be subring.

3) Intersection of subrings is a subring.

Ring Homomorphisms

Definition :-

Let $(R,+,\cdot)$ and $(S,\oplus,\odot)$ be rings.

A function $f: R \to S$ is called a ring homomorphism, if for all $a, b \in R$,

(a) $f(a+b) = f(a) \oplus f(b)$ &

(b) $f(a \cdot b) = f(a) \odot f(b)$.

when the function f is onto we say that S is a homomorphic image of R.

Definition :-

Let $f: (R,+,\cdot) \to (S,\oplus,\odot)$ be a ring homomorphism. If f is one-to-one and onto, then f is a called a ring isomorphism and we say that R & S are isomorphic rings.

Extra Questions

Q) A finite Integral Domain $(D, +, \cdot)$ is a field.

A) Since D is finite, we can list the element of D as $\{d_1, d_2, \ldots, d_n\}$.

For $d \in D$, where $d \neq e$ (identity element of +), we have $dD = \{dd_1, dd_2, \ldots, ddn\} \subseteq D$, because D is closed under multiplication.

Now, $|D| = n$ and $dD \subseteq D$, so if we could show that dD contains n elements, we would have $dD = D$.

If $|dD| < n$, then $dd_i = dd_j$, for some $1 \leq i < j \leq n$.

But since D is an integral Domain and $d \neq e$, we have $d_i = d_j$, when they are supposed to be distinct.

So $dD = D$ and for some $1 \leq k \leq n$, $dd_k = u$, the unity of D.

Then $dd_k = u \Rightarrow d$ is a unit of D. Since d is chosen arbitrarily, it follows that $(D, +, \cdot)$ is a field.