UNIT - IV

GROUP THEORY:-

GROUP THEORY:-

DEFINITION:-

Let 'S' be a non-empty set and '+' be a binary operation on 'S', then the algebraic system $\langle S, + \rangle$ is called a group iff it satisfies the following properties.

(1) Closure property

(2) Associative property

(3) Identity property.

(4) Inverse property.

(1) Closure property:-

For any two elements a, b; such that

$a + b \in S$ where $a, b \in S$

Eg; $S = \{0, \ldots \infty\}$

$a = 2$

$b = 3$.

$a + b = 2 + 3$

$= 5$.

$a + b \in S$, i.e, $5 \in S$.

(2) Associative property :-

For any three elements $a, b, c \in S$, such that

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

Eg; $S = \{0, \ldots \infty\}$

$a = 2, \; b = 3, \; c = 4$

$a+(b+c) = (a+b)+c = 9.$

$2+(3+4) = (2+3)+4 \Rightarrow 9.$

a belongs to set 'S'.

3) Identity property :-

There exists a distinguished element 'e', $e \in S$ such that

$$a+e = e+a = a. \quad \forall a \in S.$$

'e' is the identity element with respect to the addition operation. $\therefore e = 0.$ Multiplication aaku ayte $e = 1$

$S = \{0, \ldots \infty\}$

Eg; $a = 2, \; e = 0$

$a+e = e+a = a$

$2+0 = 0+2 = 2.$

4) Inverse property :-

For any element 'a', $a \in S$, there exists an element a^{-1}, $a^{-1} \in S$ such that,

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

(or)

$$a + (-a) = (-a) + a = e.$$

where 'e' is the identity element.

Eg; S = Integer numbers

$S = \{-\infty, \ldots -2, -1, 0, 1, 2, \ldots \infty\}$.

$a = 2$.

$e = 0$.

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

a = 2 aanu engil a inverse is '-2'

$a^{-1} = 2$

$2 + (-2) = (-2) + 2) = 0$

$0 = 0 = 0$.

Eg; $\langle I, + \rangle$ is a group where 'I' is the set of integers.

$I = \{-\infty, \ldots -2, -1, 0, 1, 2, \ldots \infty\}$.

the algebraic system $\langle I, + \rangle$ satisfy all the property so, $\langle I, + \rangle$ is a group.

Q) Where groups are used ?

*) Groups are used extensively in coding theory and cryptography.

*) The ultimate theory for symmetry, is a powerful tool that has a direct impact on research in Robotics, computer vision, computer graphics and medical image analysis.

*) So, in computer science, whenever you watch a video online, make a phone-call, purchase something over the internet, compress a file, send an email, or communicate with the mars rovers, lots of groups and fields are being used behind the scenes.

CYCLIC GROUP :-

A group $\langle G, * \rangle$ is said to be cyclic group, if it contains atleast one generator element.

Q) How to find generator elements in the group.

Sol Suppose $a \in G$.

We find integral powers $\{a^1, a^2, a^3, \ldots a^n\}$

The integral powers generates all the elements of given set 'G', then 'a' is called a generating elements.

Here, 'a' is a generator so, group 'G' is a cyclic group.

*) Any group contains atleast one generating elements then that group called a cyclic group.

Q) Prove that $\langle G, * \rangle$ is a cyclic group where $G = \{1, \omega, \omega^2\}$ (omega)

Sol $G = \{1, \omega, \omega^2\}$.

→ First construct composition table ;

*	1	ω	ω^2
1	1	ω	ω^2
ω	ω	ω^2	ω^3
ω^2	ω^2	ω^3	ω^4

We know that $\omega^3 = 1$., so, replace ω^3 as 1.

$\omega^4 = \omega^3 * \omega$

$= 1 * \omega = \underline{\omega}$.

So,

*	1	ω	ω^2
1	1	ω	ω^2
ω	ω	ω^2	1
ω^2	ω^2	1	ω

→ Find the integral powers of each and every element in the set.

*) 1

$1^1 = 1$

$1^2 = 1 * 1 = 1$

$1^3 = 1 * 1 * 1 = 1$

$1^4 = 1 * 1 * 1 * 1 = 1.$

Element '1' only geherates '1', but it is not generating ω & ω^2

∴ so, 1 is not a generator.

→ ω 2nd element

*) $\omega^1 = \underline{\omega}$

$\omega^2 = \omega * \omega$

$= \underline{\omega^2}$

$\omega^3 = \omega * \omega * \omega$

$= \underline{1}.$

$\omega^4 = \omega * \omega * \omega * \omega$

$= \omega^3 * \omega$

$= 1 * \omega$

$= \underline{\omega}.$

ω generates all elements in set, ie, 1, ω & ω^2.

so, ω is a generator.

*) ω^2

$(\omega^2)^1 = \underline{\omega^2}$

$(\omega^2)^2 = \omega^4$

$= \omega^3 * \omega$

$= 1 * \omega = \underline{\omega}$

$(\omega^2)^3 = \omega^6$

$= \omega^3 \times \omega^3$

$= 1 \times 1$

$= \underline{1}$.

$(\omega^4)^4 = \omega^8$

$= \omega^3 \times \omega^3 \times \omega^2$

$= 1 * 1 * \omega^2$

$= \underline{\omega^2}$.

ω^2 also generates all elements in set, ie, $1, \omega$, & ω^2

so, ω^2 is a generator.

∴ the group $\langle G, * \rangle$ contains two generators $\langle \omega, \omega^2 \rangle$

∴ $\langle G, * \rangle$ is a cyclic group.

HOMOMORPHISM IN GROUP THEORY:-

Let G and G' be any two groups with binary operations '*' and 'Δ' respectively, then mapping $f: G \to G'$ said to be homomorphism if,

$$\boxed{f(a * b) = f(a) \Delta f(b)}, \forall a, b \in G.$$

Q) Let $\langle Z, + \rangle$ be a group and $\langle G, * \rangle$ be another group. G can be defined as $G = \{2^n, n \in Z\}$. A function $f: Z \to G$ by $f(n) = 2^n, \forall n \in Z$. Show that $f: Z \to G$ is a homomorphism.

Sol. *) $\langle Z, + \rangle$ and $\langle G, * \rangle$ be two groups.

*) $G = \{2^n, n \in Z\}$

*) $f: Z \to G$ and $f(n) = 2^n, \forall n \in Z$.

Let us take 2 elements from 'Z', n_1 & n_2,

$$n_1, n_2 \in Z \Rightarrow f(n_1) = 2^{n_1}$$

$$f(n_2) = 2^{n_2}$$

$f: Z \to G \Rightarrow f(n_1 + n_2)$ → engare + vannu engil Z is addition in a group so, namuke + to * aanu edukand

$$= 2^{n_1+n_2} \quad (\because a^{m+n} = a^m * a^n)$$

$$= 2^{n_1} * 2^{n_2}$$

$$= f(n_1) * f(n_2)$$

$$f(n_1 + n_2) = f(n_1) * f(n_2).$$

$\therefore$ f is a homomorphism.

Q2) Let $\langle G, * \rangle$ be a group defined by $G = \{1, -1, i, -i\}$ and $\langle I, + \rangle$ be a group. Prove that $f: I \to G$ is a homomorphism where $f(n) = i^n \quad \forall n \in I$.

Sol. *) $\langle G, * \rangle \Rightarrow G = \{1, -1, i, -i\}$

*) $\langle I, + \rangle$

*) $f: I \to G \quad f(n) = i^n, \forall n \in I$

*) n_1 and n_2 are two elements in 'I' i.e, $n, n_2 \in I$.

$$f(n_1) = i^{n_1}$$

$$f(n_2) = i^{n_2}$$

$$f(n_1 + n_2) = i^{n_1 + n_2} \quad [\because a^{m+n} = a^m * a^n]$$

$$= i^{n_1} * i^{n_2}$$

$$= f(n_1) * f(n_2)$$

$\therefore f(n_1 + n_2) = f(n_1) * f(n_2)$.

$\therefore f: I \to G$ is a homomorphism.

Types of homomorphism :-

1) Monomorphism :-

A group homomorphism that is injective (or, one to one); ie, preserves distinctness.

A group should be homomorphism and one-one function means then it is monomorphism.

2) Epimorphism :- F is a function, ie, homomorphism and it is onto too then it is epimorphism

A function should not be 1-1 here.

*) A group homomorphism that is surjective (or onto); ie, reaches every point in the codomain

codomain

*) If 'f' is epimorphism then 'G'' is called a homomorphic image of G.

3) Endomorphism :-

A homomorphism, $h : G \to G$; the domain and codomain are the same, also called an endomorphism of G.

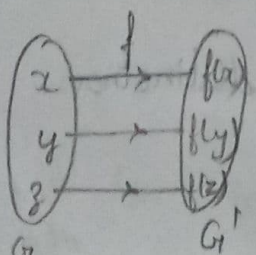
4) Isomorphism :-

A group homomorphism that is bijective; i.e, injective and surjective.

ISOMORPHISM :-

Let $\langle G, + \rangle$ and $\langle G', * \rangle$ are two groups, a function f mapping $f : G \to G'$ is called isomorphism iff it satisfies the following 3 conditions,

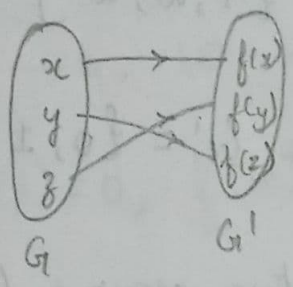
(i) f is one-one



$\forall x, y, z \in G$

$\forall f(x), f(y), f(z) \in G'$

(ii) f is onto

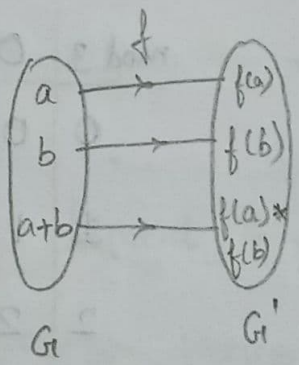


$\forall x, y, z \in G$

$\forall f(x), f(y), f(z) \in G'$

(iii) f is homomorphism from $G \to G'$

$f(a+b) = f(a) * f(b)$, $\forall a, b \in G$ & $f(a), f(b) \in G'$



$\therefore$ f satisfies the 3 conditions i.e, one to one, onto, homomorphism.

Hence we can say that $f: G \to G'$ is called Isomorphism

$\therefore G \cong G'$

The symbol $\cong$ represents isomorphism blw 2 groups $\langle G, + \rangle$ and $\langle G', * \rangle$.

Q) Let $\langle G, * \rangle$ and $\langle G', (\text{mod } 3) \rangle$ be two groups where $G = \{1, \omega, \omega^2\}$ (omega) and $G' = \{0, 1, 2\}$. Show that $G \cong G'$.

Sol. $\langle G, * \rangle$ is a group where $G = \{1, \omega, \omega^2\}$

$\langle G', (\text{Mod } 3) \rangle$ is a group where $G' = \{0, 1, 2\}$.

To prove the isomorphism blw two groups G and G', i.e., $G \cong G'$, the function $f : G \to G'$ satisfies 3 conditions.

(1) f is one-to-one :-

creating composition table,

*	1	ω	ω^2
1	1	ω	ω^2
ω	ω	ω^2	1
ω^2	ω^2	1	ω

$\langle G, * \rangle$

mod 3	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1.

one to one

$\langle G', (\text{mod } 3) \rangle$

$\omega \cdot \omega^2 = \omega^3 = 1$

$\omega^2 \cdot \omega^2 = \omega^4 = \omega^3 \cdot \omega$

$= 1 \cdot \omega$

$= \omega.$

$0 \overset{+}{\underset{0}{\curvearrowright}} \text{mod } 3^0 = 0 \quad \text{mod } 3 = 0.$

$0 \overset{+}{\underset{1}{\curvearrowright}} \text{mod } 3^1 = 1 \quad \text{mod } 3 = 1$

$0 \overset{+}{\underset{2}{\curvearrowright}} \text{mod } 3^2 = 2 \text{ mod } 3 = 2$

$1 \text{ mod } 3^0 = 1 \text{ mod } 3 = 1$

$1 \text{ mod } 3^1 = 2 \text{ mod } 3 = 2$

$1 \text{ mod } 3^2 = 3 \text{ mod } 3 = 0$

$2 \bmod 3^0 = 2 \bmod 3 = 2$

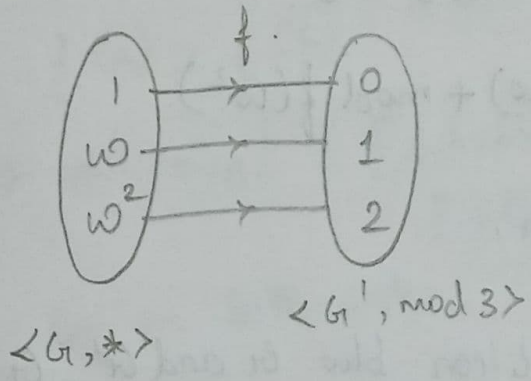
$2 \bmod 3^1 = 3 \bmod 3 = 0$

$2 \bmod 3^2 = 4 \bmod 3 = 1$

one to one means,

$1 \to 0$, $\omega \to 1$, $\omega^2 \to 2$.

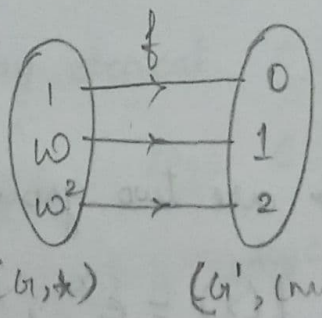
$\therefore f(1) = 0$, $f(\omega) = 1$, $f(\omega^2) = 2$.



$\therefore f$ is one to one.

(ii) f is onto :-

For every element x, $x \in G'$, then there exist an element x', $x' \in G$, Hence f is onto.



$\therefore f$ is onto.

(iii) f is homomorphism :-

For any two elements $w^a, w^b \in G$ then,

$f : G \to G'$

$f(w * w^2) = f(w^{1+\bmod 3\, 2})$ (we got $f(w) = 1$, see previous, 2; $*$ $\bmod 3$)

$= f(w) +_{\bmod 3} f(w^2)$ $\quad f(a*b) = f(a) \bmod 3\ f(b)$

$= 1 +_{\bmod 3} 2$ $\quad a, b \in G$

$= 3 \bmod 3 = 0.$

$\therefore f(w * w^2) = f(w) +_{\bmod} f(w^2).$

$\therefore f$ is homomorphism.

$\therefore f$ satisfies 3 condition blw G and G' $G \cong G'$.

Q)2) Let R be the additive group of real numbers $\langle R, + \rangle$ and R^+ be the multiplicative group of positive real numbers : $\langle R^+, * \rangle$ and a function f, $f : R \to R^+$ is defined by $f(x) = e^x \ \forall\ x \in R$ then show that $R \cong R^+$.

Sol Let $\langle R, + \rangle$ & $\langle R^+, * \rangle$ are two groups

$f : R \to R^+$ is defined by $f(x) = e^x$, $\forall\ x \in R$

Now $f : R \to R^+$ is Isomorphism iff f satisfies the following properties,

1) f is one to one

2) f is onto

3) f is homomorphism

(1) f is one to one :-

Let us consider any 2 elements a, b

$a, b \in R$

then $f(a) = f(b)$

$\Rightarrow e^a = e^b$: [substituting x as a & b in $f(x)$]

[$f(a) = e^a$, $f(b) = e^b$]

Apply log on both sides

$\log e^a = \log e^b$

$a \log e = b \log e$ [$\because \log e = 1$]

$a = b$. [$\because f(a), f(b) \in R^+$].

$\therefore f$ is one to one.

(2) f is onto :-

For any element c, $c \in R^+$, then there exist an element $\log c$, $\log c \in R$

Then $f(\log c) = e^{\log c} = c$

For every element in R^+, there exist an element in R, $\therefore f$ is onto.

(3) f is homomorphism:-

For any 2 elements a, b, $a, b \in R$ then,

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

$$= e^a * e^b \qquad \left[\because f(a) = e^a,\ f(b) = e^b\right]$$

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

$$f(a+b) = f(a) * f(b)$$

$\therefore f$ is homomorphism.

$f : R \to R^+$ satisfies the 3 conditions, hence

$f : R \to R^+$ is Isomorphism.

$\therefore R \cong R^+$.

Sub Group:-

A subset H of a group G is called a subgroup of G if H forms a group with respect to the binary operation in G.

→ Let $\langle G, * \rangle$ be a group, if H be a finite subset of group G, then H is a subgroup of G iff it satisfies the group property (closure, associative, identity, and inverse) with respect to the operation '*'.

(1) closure property :- $a * b \in H$. ; $a, b \in H$.

(2) Associative property :- $(a * b) * c = a * (b * c)$
$\forall a, b, c \in H$.

(3) Identity property :- $a * e = e * a = a$. $[e = 1]$
$a * 1 = 1 * a = a$.

(4) Inverse property :- $a * a^{-1} = a^{-1} * a = e$.

the subset H of group G, should satisfy all the 4 property to become H as a subgroup of G.

Eg; set of integers — set of rational numbers

(1) $\langle \mathbb{Z}, + \rangle$ is a subgroup of $\langle \mathbb{Q}, + \rangle$

set of real numbers

(2) $\langle \mathbb{Q}, + \rangle$ is a subgroup of $\langle \mathbb{R}, + \rangle$

$\therefore$ (Set of natural numbers $\overset{N}{}$) is subgroup of (set of Integers $\overset{Z}{}$)

(set of integer $\overset{Z}{}$) $\leq$ subgroup of (set of rational numbers $\overset{Q}{}$)

(set of rational numbers $\overset{Q}{}$) $\leq$ subgroup of (set of real numbers $\overset{R}{}$)

(set of real numbers $\overset{R}{}$) $\leq$ subgroup of (set of complex numbers $\overset{C}{}$)

$$N \leq Z \leq Q \leq R \leq C.$$

Q) Let $\langle G, * \rangle$ is a group, $G = \{1, -1, i, -i\}$ and $\langle H, * \rangle$ is a subgroup of $\langle G, * \rangle$. Check whether $\{1, -1\}$ is a subgroup of G (or) not.

Sol. $\langle G, * \rangle$ is a group.

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

Hnu parayuna subset, ā property anu satisfy cheytha, then H is a subgroup of 'G'

$\langle H, * \rangle$ is a subgroup of $\langle G, * \rangle$

Here, $H = \{1, -1\}$ is a subgroup if satisfies the following properties;

(1) Closure property :-

composition table

*	1	-1
1	1	-1
-1	-1	1

Let us take any two elements a and b, $a, b \in H$ then

$a * b \in H$, $\forall a, b \in H$.

Eg; $a = 1$, $b = -1$ $\Rightarrow H = \{1, -1\}$ (a, b)

$a * b \in H$

$1 * -1 \in H$

$-1 \in H$.

∴ closure property is satisfied.

(2) Associative property :-

Take any three elements a, b, c here $a, b, c \in H$

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

Eg; $a = 1$, $b = -1$, $c = 1$ $H = \{1, -1\}$ (a, b, c)

$1 * (-1 * 1) = (1 * -1) * 1$

$1 * -1 = -1 * 1$

$-1 = -1$ ∴ $-1 \in H$.

∴ Associative property is satisfied.

(3) Identity property :-

Take any element "a", here $a \in H$ then,

$$a * e = e * a = a.$$

where 'e' is identity element = 1.

Eg; $a = -1$, $a \in H$.

$$-1 * 1 = 1 * -1 = -1 \in H.$$

$\therefore$ Identity property is satisfied.

(4) Inverse property :-

Take any one element 'a', here $a \in H$. There exist an element a^{-1} in H, i.e, $a^{-1} \in H$ then

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

where, e is the identity element its value is equal to '1'.

a inverse is a^{-1}

a^{-1} inverse is a.

Eg; Let us take $a = 1$, where $a \in H$

Now, its inverse is $a^{-1} = 1$

$$\therefore a * a^{-1} = a^{-1} * a = e.$$

$1 * 1 = 1 * 1 = 1$

$= e.$

$\therefore$ 1 inverse is 1

-1 inverse is -1

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

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

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

$a^{-1} = \frac{1}{1} = 1$ //

Suppose $a = -1$, where $a \in H$.

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

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

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

a inverse is $a^{-1} = -1 \in H$

$\therefore a * a^{-1} = a^{-1} * a = e$

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

$\Rightarrow 1 = e$

$\therefore$ Inverse property is also satisfied.

$\therefore H = \{1, -1\}$ satisfies 4 properties. Hence $\langle H, * \rangle$ is a subgroup of $\langle G, * \rangle$ where $H = \{1, -1\}$ //.

COSETS:-

Let $\langle H, * \rangle$ be a subgroup of a group $\langle G, * \rangle$ and 'a' is an element of 'G' i.e, $a \in G$, then the set

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

is called the "Left Coset" of H in G and

$$H * a = \{h * a / h \in H\}$$

is called the "Right Coset" of H in G

Eg; Let $\langle G, * \rangle$ is a group. $a \in G$.

$\langle H, * \rangle$ is a sub group of $\langle G, * \rangle$, $H = \{P, Q, R, S\}$

coset

$aH = \{aP, aQ, aR, aS\}$ ⇒ Left coset.

$Ha = \{Pa, Qa, Ra, Sa\}$ ⇒ Right coset.

Left coset : $a * H = \{a * h \mid h \in H\}$ replacing H to h

Right coset : $H * a = \{h * a \mid h \in H\}$

~~a * H~~ $\boxed{a * H \neq H * a}$.

satisfies closure, associative, identity, inverse, competative property

If G is abelian group with respect to $*$, then

$\boxed{a * H = H * a}$

Note: $\langle H, + \rangle$ be a subgroups of $\langle G, + \rangle$ and $a \in G$, then the ~~closet~~ coset of H in G are,

1) Left ~~closet~~ coset $= a + H = \{a + h \mid h \in H\}$

2) Right coset $= H + a = \{h + a \mid h \in H\}$

If G is an abelian group then $aH = Ha$.

Eg; Let $\langle G, + \rangle$ is a group, $a \in G$;

$\langle H, + \rangle$ is a subgroup of $\langle G, + \rangle$ $H = \{P, Q, R, S\}$

$a+H = \{a+P, a+Q, a+R, a+S\}$ ⇒ Left coset

$H+a = \{P+a, Q+a, R+a, S+a\}$ ⇒ Right coset.

$a+H \neq H+a$.

If G is a abelian group with respect to $+$, then

$a+H = H+a$.

Properties:-

1) If G is a abelian group then, $a+H = H+a$;

2) The left and right coset of H, corresponding to the identity element e is H,

$\boxed{eH = H = He}$ $\quad e=1$ in $*$; $e=0$ in $+$

Eg; $\langle G, * \rangle$ is a group.

$\langle H, * \rangle$ is a subgroup of $\langle G, * \rangle$, $H = \{P, Q, R, S\}$.

$e * H = \{eP, eQ, eR, eS\}$

$e = 1$

$= \{P, Q, R, S\} = H$.

$H * e = \{Pe, Qe, Re, Se\}$

$e = 1$

$= \{P, Q, R, S\} = H$.

$\therefore e * H = H * e = H$.

3) Order of a subgroup ($O(H)$) is equal to order of ($O(aH)$) left coset (or) right coset ($O(Ha)$) i.e,

$$O(H) = O(aH) \text{ (or) } O(Ha).$$

Eg; $\langle G, * \rangle$ is a group $e \in G$

$\langle H, * \rangle$ is a subgroup of $\langle G, * \rangle$ $H = \{P, Q, R, S\}$

subgroup
no. of elements = order

$aH = \{eP, eQ, eR, eS\}$

$Ha = \{Pe, Qe, Re, Se\}$.

$O(H) = O(aH / Ha)$

$4 = 4$.

4) Order of subgroup is not equal to the order of G

i.e, $O(H) \neq O(G)$. ($4 \neq 1$)

5) A subgroup H itself is a left as well as (or) right coset of H in G.

Q) Find all the left cosets of subgroup $H = \{0, 2\}$ in group $\langle Z, +_4 \rangle$ $+_4 \Rightarrow$ Addition modulus

Sol Given group is $\langle Z, +_4 \rangle$

H is a subgroup of Z, $H = \{0, 2\}$.

Elements of Z are,

Take 0 to 3 elements

i.e, $\{0,1,2,3\}$. do mod 4 for each elements,

$0 \bmod 4 = 0$; $1 \bmod 4 = 1$; $2 \bmod 4 = 2$; $3 \bmod 4 = 3$

so, elements of Z are $\{0,1,2,3\}$

*) Now we have to find out all the distinct left cosets of H in Z as follows,

$0 \in Z$ $Z = \{0,1,2,3\}$ $(+_4)$ $H = \{0,2\}$

$0 +_4 H = \{0 +_4 0 , 0 +_4 2\}$ (addition Modulus (mod))

$= \{0 \bmod 4 , 2 \bmod 4\}$

$= \{0,2\} = H.$

$1 \in Z$

$1 +_4 H = \{1 +_4 0 , 1 +_4 2\}$

$= \{1 \bmod 4 , 3 \bmod 4\}$

$= \{1,3\}$

$2 \in Z$;

$2 +_4 H = \{2 +_4 0 , 2 +_4 2\}$

$= \{2 \bmod 4 , 4 \bmod 4\} = \{2,0\} = \{0,2\}$

$= H$

$3 \in Z$

$$3 +_4 H = \{ 3 +_4 0 , 3 +_4 2 \}$$

$$= \{ 3 \text{ Mod } 4 , 5 \text{ Mod } 4 \}.$$

$$= \{ 3, 1 \} = \{ 1, 3 \}.$$

Now, the distinct left cosets of H in Z are,

$\{ 0 +_4 H , 1 +_4 H \}$.

we avoided $2 +_4 H$ & $4 +_4 H$ because we got these answers in $0 +_4 H$ & $1 +_4 H$ so duplication is not needed.

LAGRANGE'S THEOREM:-

~~COROLLARY:-~~

Lagrange theorem was given by Joseph-Louis Lagrange. Lagrange theorem states that in group theory, for any finite group say G, the order of subgroup H (of group G) is the divisor of the order of G i.e,

$$\frac{o(G)}{o(H)}$$

Statement :-

Lagrange theorem states that the order of the subgroup 'H' is the divisor of the order of the group G.

This can be represented as;

$$|G| = |H| \cdot$$

If G is a finite group and H is a subgroup of G, then

a) $|H|$ devides $|G|$.

b) the no. of distinct left (right) coset of H in G is

$$|G| / |H|$$

COSET :-

When G is a finite group, and H is a sub group of G, given that 'g' is an element of G then;

$gH = \{ gh : h$ an element of $H \} \Rightarrow$ left coset of H in G

$Hg = \{ hg : h$ an element of $H \} \Rightarrow$ Right coset of H in G.

*) Three lemmas to prove the Lagrange theorem.

Lemma 1 :- If G is a finite ~~grough~~ grup and H is its subgroup, then there is a one one one correspondence blw 'H' and any coset of H.

Lemma 2: If G is a finite group and H is its subgroup, then the left coset relation, $g1 \sim g2$ iff $g1 * H = g2 * H$ is an equivalence relation.

Lemma 3:- Let 'S' be a set and $\sim$ be an equivalence relation on S. If A and B are 2 equivalence classes with $A \cap B = \phi$, then $A = B$.

Proof:-

Let H be any subgroup with an order 'n' of a finite group G of order m.

Let us consider the coset breakdown of G with respect to H.

Now considering that each coset of aH comprises 'n' different elements.

Let $H = \{h1, h2, \ldots hn\}$, then $ah1, ah2, \ldots ahn$ are the 'n' number of distinct members of aH.

Suppose $ahi = ahj \Rightarrow hi = hj$ be the cancellation law of G. Now G is a finite group, so the no. of. disjoint left cosets will also be finite, say P. So, the total no. of. elements of all cosets is 'np' which is equal to

the total number of element of G. Hence $m = np$.

$p = m/n$.

This shows that n, the order of H, divides m i.e, is a divisor of m, the order of the finite group G. We also see that the index 'p' is also a divisor of the order of the group.

Hence proved, $|G| = |H|$.

Corollary:-

Corollary 1:-

If G is a group of finite order m, then the order of any $a \in G$ divides the order of G and in particular

$a^m = e$.

Proof:- Let the order of 'a' be p, which is the least +ve integer, so,

$a^p = e$

then we can say,

$a; a^2; a^3, \ldots a^{p-1}, a^p = e$, the elements of group G are all different and they form 'a' Sub group. Since the subgroup has order p, thus 'p' the order of 'a' is the divisor of group G.

So, we can write, $m = np$, where $m = np$, where 'n' is a +ve integer.

So, $a^m = a^{np} = (a^p)^n = e$.

Hence, proved.

Corollary 2: If the order of finite group 'G' is a prime order, then it does not have proper subgroups.

proof: Let us suppose, the prime order of group G is m. Now, 'm' will have only 2 divisors 1 and m. Thus, the subgroups of G will be $\{e\}$ and G itself. So, there are no proper subgroups. Hence proved.

corollary 3:- A group of prime order (the order has only 2 divisors) is a cyclic group.

proof:- Suppose, G is the group of prime order of 'm' and $a \neq e \in G$.

As the order of 'a' divides 'm', it will be either 1 or m, But the order of a, $o(a) \neq 1$, since $a \neq e$. Therefore, the order of $o(a) = p$, and the cyclic subgroup of G generated by 'a' are also of order 'm'.

This proves that 'G' is nothing but the same cyclic subgroup formed by 'a', ie, G is cyclic.

RINGS:-

An algebraic system $\langle S, +, * \rangle$ is called a ring, if the binary operations '+' and '*' on S satisfies the following three properties,

1) $\langle S, + \rangle$ is an abelian group.
2) $\langle S, * \rangle$ is a semigroup.
3) The operation '*' is distributive over '+'.

Distributive property:-

For any 3 elements $a, b, c \in S$

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

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

Eg: 1) $\langle I, +, * \rangle$ is a ring

where I is the set of integers

$$I = \{-\infty, \ldots 0, \ldots +\infty\}.$$

2) $\langle Q, +, * \rangle$ is a ring

3) $\langle R, +, * \rangle$ is a ring

4) $\langle C, +, * \rangle$ is a ring.

Q) S.T $\langle C, +, * \rangle$ is a ring. C => Complex numbers.

Sol. Let $\alpha = a+ib$ and $\beta = c+id$ be any 2 elements of C.

Then $\alpha+\beta = (a+ib)+(c+id)$

$= (a+c)+i(b+d) \in C \quad \forall \alpha, \beta \in C.$

1) $\alpha+\beta = (a+ib)+(c+id)$

$= (a+c)+i(b+d)$

$= (c+a)+i(d+b)$

$= \beta+\alpha \quad \forall \alpha, \beta \in C.$

So, complex number satisfies commutative property.

2) Associative law holds good for addition of complex numbers.

3) The element $0 = 0+i0 \in C$ is the identity of C for addition, since $\alpha+0 = 0+\alpha = \alpha \quad \forall \alpha \in C.$

4) The element $-\alpha = -a-ib \in C$ is the inverse element, such that $-\alpha+\alpha = 0+i0 = 0$, the identity element of C.

Hence $\langle C, + \rangle$ is an abelian group.

5) $\forall \alpha, \beta, \gamma \in C \Rightarrow (\alpha\beta)\gamma = \alpha(\beta\gamma)$

Thus multiplication is associative.

6) $\alpha(\beta+\gamma) = (a+ib)\left[(c+id)+(e+if)\right]$

$= (a+ib)\left[(c+e)+i(d+f)\right]$

$= a(c+e)+ia(d+f)+ib(c+e)-b(d+f)$

$= \{ac+ae-bd-bf\}+i\{ad+af+bc+be\}$.

$= (ac-bd)+i(ad+bc)+(ae+bf)+i(af+be)$

$= (a+ib)(c+id)+(a+ib)(e+if)$

$= \alpha\beta+\alpha\gamma \quad \forall\ \alpha,\beta,\gamma \in C$.

Similarly $(\beta+\gamma)\alpha = \beta\alpha+\gamma\alpha \quad \forall\ \alpha,\beta,\gamma \in C$

Hence, $\langle C,+,*\rangle$ is a ring.

Types:- Ring with unity:- A ring 'R' is said to be a ring with unity, if the multiplicative identity $1 \in R$ such that $1.a = a.1 = a$, $\forall\ a \in R$.

commutative ring:- A ring 'R' is said to be a commutative ring, if $a.b = b.a$ $\forall\ a,b \in R$

FIELD:-

Let F be a non-empty set. An algebraic structure $\langle F,+,*\rangle$ together with 2 binary operations addition & multiplication for all $a,b \in F$ is called a field, if this structure satisfies following properties,

1) $\langle F,+\rangle$ is an abelian group.

2) $\langle F-\{0\},*\rangle$ is an abelian group. $F-\{0\}$ => the set F without 0.

3) Distributive laws:

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

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

An algebraic structure $(F, +, *)$ is said to be a field, if it satisfies following properties:-

1) closed under addition.
2) Associative under addition
3) Existence of additive identity.
4) Existence of additive inverse
5) Commutative under addition.

} abelian group w.r.t to addition

6) closed under multiplication.
7) Associative under multiplication.
8) Existence of multiplicative identity
9) Existence of multiplicative inverse.
10) Commutative under multiplication.

} Abelian group w.r.t to multiplication

11) Distributive laws (Distribution of '*' over '+').

Eg: 1) The set $C = \{a + ib ; a, b \in R\}$ of complex number is field under usual addition and multiplication of complex number.

2) $(Q, +, *)$ is a field, Q => Rational numbers.

3) $(R, +, *)$ is a field, R => Real numbers.

4) For any prime p, $Zp = \{0, 1, 2, \ldots p-1\}$ is a field with respect to addition & multiplication modulo P.

INTEGRAL DOMAINS:-

ZERO DIVISOR:-

*) If R is a commutative ring, then $a \neq 0 \in R$ is said to be zero-divisor if there exists $a, b \in R$, $b \neq 0$, such that $ab = 0$.

*) A ring 'R' is said to be ring with zero divisor, if there exists elements a, b in R, such that $ab = 0 \Rightarrow a \neq 0$, $b \neq 0$. R epozha ring with zero divisor aava vechal, a*b cheyyumbo 0 kittanam. but, $a \neq 0$ aayirkanam & $b \neq 0$ aayirkanam.

Ring without zero divisor:-

A ring 'R' is said to be ring without zero divisor, if $ab = 0 \Rightarrow$ either $a = 0$ or $b = 0$. 'R' epozha ring without 0 divisor aava vechal, a*b cheyyumbo '0' kittanam, but eathengilum oru element (a or b) zero aayirkanam.

Integral Domain:-

A commutative ring 'R' with unit element having no zero divisors is called an integral domain.

Eg:

For zero divisor.

Integer mod 6

Q). In a ring $R = Z_6 = \{(0,1,2,3,4,5), +_6, \times_6\}$. List the elements which are zero divisor.

Sol. Let us take 2 non zero elements 1 & 2.

$1 \times 2 = 2 \Rightarrow 2 \text{ Mod } 6 = \underline{2}$.

So, it didn't satisfy zero divisor.

Take another 2 non zero elements 2 & 3,

$2 \times 3 = 6 \Rightarrow 6 \text{ Mod } 6 = \underline{0}$.

So, it satisfies zero divisor. So, 2 & 3 is zero divisor.

Take, another 2 non zero elements, 3 & 4.

$3 \times 4 = 12 \Rightarrow 12 \text{ Mod } 6 = \underline{0}$

So, it satisfies zero divisor. 3 & 4 is zero divisor.

Take, another 2 non zero elements, 4 & 5.

$4 \times 5 = 20$, $20 \text{ Mod } 6 = 2$.

So, it didn't satisfy zero divisor.

Take, another 2 non zero elements, 5 & 1.

$5 \times 1 = 5$, $5 \text{ Mod } 6 = 5$.

So, it didn't satisfy zero divisor.

$\therefore$ 2, 3, 4 are zero divisors of R.

Integer modulo 5

Q) Find integral domain for $\mathbb{Z}_5 := \{0, 1, 2, 3, 4\}$

non zero

Ans → Take 2 elements : 1 & 2.

$1 \times 2 = 2$; $2 \text{ Mod } 5 = 2$.

2 & 1

So, it is integral domain.

→ Take another 2 elements which is of non zero ; 2 & 3.

$2 * 3 = 6$; $6 \text{ Mod } 5 = 1$.

2, 3

So, it is integral domain

→ Take another 2 elements which is of non zero : 3 & 4.

$3 * 4 = 12$, $12 \text{ Mod } 5 = 2$.

So, 3 & 4 is integral domain.

→ Take another non zero elements 4 & 1,

$4 * 1 = 4$; $4 \text{ Mod } 5 = 4$.

So, 4 & 1 is integral domain.

∴ $\mathbb{Z}_5$ is an integral domain.