UNIT-3 GROUP THEORY

GROUP

Let G be a non-empty set and $*$ be the binary operation

The $(G,*)$ is called a group under the binary operation $*$ if the following conditions are satisfied

(i) Closure property

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

(ii) Associativity

For any $a, b, c \in G$, $a * (b * c) = (a * b) * c$

(iii) Existence of Identity

Let $a \in G$

Then there exist an element $e \in G$ such that $a * e = e * a =$ [illegible]

for all $a \in G$

Here e is called the identity element

(iv) Existence of inverse

Let $a \in G$

Then there exists $a^{-1} \in G$ such that $a * a^{-1} = a^{-1} * a = e$

Here a^{-1} is the inverse of a

Q. Let $G = \{0, \pm 1, \pm 2, \dots \infty\}$. Prove that $(G, +)$ is a group.

Let $a, b \in G$

(i) Closure

Let $a, b \in G$

$a+b \in G$ for all $a, b \in G$

G is closed

(ii) Associativity

Let $a, b, c \in G$

$a+(b+c) = (a+b)+c \quad \forall\ a, b, c \in G$

(iii) Existance of identity

Let $a \in G$

Now $0 \in G$

$a+0 = 0+a = a \quad \forall\ a \in G$

"0" is the identity element

Existance of inverse

Let $a \in G$

$-a \in G \qquad a+(-a) = (-a)+a = 0$

$-a$ is the inverse of a

$(G, +)$ is a group under addition

Let $G = \{1, -1, i, -i\}$. Prove that G is group under multiplication

$\times$	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

Let $a, b \in G$

$a \cdot b \in G$ (from table)

(ii) Associativity

Let $a, b, c \in G$

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

(iii) Existance of identity

Let $a \in G$

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

1 is the identity element

(iv) Existence of Inverse

The inverse of 1 is 1

The inverse of -1 is -1

The inverse of i is $-i$

The inverse of $-i$ is i

$(G, \cdot)$ is a group.

ABELIAN GROUP [commutative group)

A group $(G, *)$ is said to be an abelian group if $a*b = b*a \;\forall\; a, b \in G$

Q. P.T the set of all +ve rational Q^+ is an abelian group under the binary operation $*$ defined by $a*b = a.b/2 \;\forall\; a, b \in Q^+$

Ans: (i) Closure property

Let $a, b \in Q^+$

$$a*b = \frac{a \cdot b}{2} \in Q^+$$

$(Q^+, *)$ is cloud

(ii) Associativity

Let $a, b, c \in Q^+$

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

$$= \frac{a \cdot \frac{(b \cdot c)}{2}}{2}$$

$$= \frac{a \cdot b \cdot c}{4}$$

$$= \frac{\left(\frac{ab}{2}\right) \cdot c}{2}$$

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

(iii) Existence of Identity

Let e be the identity

Let $a \in G$

$a * e = a$

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

$e = 2 \in Q^+$

"2" is the identity element in Q^+

(iv) Existence of inverse

Let $a \in Q^+$

Let a^{-1} be the inverse of a

$a * a^{-1} = 2$

$\frac{a \cdot a^{-1}}{2} = 2$

$a^{-1} = \frac{4}{a} \in Q^+$

(v) Commutative Property

Let $a, b \in Q^+$

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

$(Q^+, *)$ is an abelian group

NOTE : ADDITION MODULO m $(+_m)$

Let $a, b \in R$

If $a+b > m$

$a+b = qm + r$

where $0 < r < m$

$\boxed{a +_m b = r}$

Scanned by CamScanner

Q. Let $M_2 = \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} \Big/ ad - bc \neq 0 \right\}$

Q P.T M_2 under usual matrix multiplication is a group

Ans (i) closure property

$$A = \begin{bmatrix} a_1 & b_1 \\ c_1 & d_1 \end{bmatrix}, \quad B = \begin{bmatrix} a_2 & b_2 \\ c_2 & d_2 \end{bmatrix}$$

$$A \cdot B = \begin{pmatrix} a_1 a_2 + b_1 c_2 & a_1 b_2 + b_1 d_2 \\ c_1 a_2 + d_1 c_2 & c_1 b_2 + d_1 d_2 \end{pmatrix}_{2\times 2} \in M_2$$

$\left[\because |A \cdot B| = |A| \cdot |B| \neq 0 \quad \text{as } |A| \neq 0, \ |B| \neq 0 \right]$

(ii) Associativity

Let $A, B, C \in M_2$

$A \cdot (B \cdot C) = (A \cdot B) \cdot C$

(iii) Existence of identity

Let $A = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in M_2$

Now $I = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \in M_2$

$AI = IA = A$

$I = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$ is the identity.

(iii) Existance of Inverse

Let $A = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in M_2$

$A^{-1} = \frac{1}{|A|} \begin{bmatrix} d & -b \\ -c & a \end{bmatrix} \in M_2$

$A \cdot A^{-1} = A^{-1} \cdot A = I$

M_2 is a group under usual multiplication

Q If $(G, *)$ is a abelian group, Show that $(a*b)^n = a^n * b^n$ by mathematical induction.

Ans: For $n=1$, $a*b = a*b$

Assume that the result is true for $n=k$

$(a*b)^k = a^k * b^k$ —(i)

$(a*b)^{k+1} = (a*b)^k * (a*b)$

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

$= a^k * (b^k * a) * b$ (Associativity)

$= a^k * (a * b^k) * b$ (by comm prop)

$= (a^k * a) * b * b^k$ (by associativity)

$= a^{k+1} * b^{k+1}$

$= (a*b)^{k+1}$

The result is true for $n = k+1$

∴ By Induction, the Result is True for any n.

NOTE: ADDITION MODULO M $(+m)$

Let $a, b \in R$

If $a+b > m$

$a+b = qm + r$

where $0 < r < m$

$\boxed{a +_m b = r}$

Scanned by CamScanner

Q Show that the set of all integers addition modulo m is an abelian group.

Ans $Z_m = \{0, 1, 2, \ldots, m-1\}$

Let $a, b \in Z_m$

$a+b = qm+r$, where $0 < r < m$

$a +_m b = r$, if $a+b > m$

(i) Closure problem

For $a, b \in Z_m$

$a +_m b = r < m$

$a +_m b \in Z_m$

(ii) Associativity

Let $a, b, c \in Z_m$

$a+b = q_1 m + r_1$, $0 < r_1 < m$

$b+c = q_2 m + r_2$, $0 < r_2 < m$

$r_1 + c = q_3 m + r_3$, $0 < r_3 < m$

$a +_m b = r_1$, $b +_m c = r_2$

$a +_m (b +_m c) = a +_m r_2$

$a +_m (b +_m c) = r_3$ — (1)

$a + r_2$

$= a + b + c - q_2 m$

$= q_1 m + r_1 + c - q_2 m$

$= q_1 m + q_3 m + r_3 - q_2 m$

$= (q_1 + q_3 - q_2) m + r_3$

$(a +_m b) +_m c = r_1 +_m c$

$(a +_m b) +_m c = r_3$ — (2)

From (1) & (2)

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

(iii) Existance of Identity

Let $a \in Z_m$

$0 +_m a = a +_m 0 = a$ (for all $a \in Z_m$)

0 is the identity element.

(iv) Existance of Inverse

Let $a \in Z_m$

then $m-a < m$

$m-a \in Z_m$

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

$m-a$ is the inverse of a

(v) Commutative property

$a +_m b = b +_m a$ for all $a, b \in Z_m$

$\therefore (Z_m, +_m)$ is an abelian group

SEMI GROUP

Let G be a non-empty set and $*$ be the binary operation. Then $(G, *)$ is said to be semi-group if only closure and associative property are satisfied.

Eg: $N = \{1, 2, 3 \ldots\}$

$(N, +)$ is a semi-group

MONOID

Let G be a non-empty set and $*$ be the binary operation. The $(G, *)$ is said to be a monoid if

(i) $(G, *)$ satisfies closure

(ii) $(G, *)$ Satisfies associative property.

(iii) Identify element exists in G

Eg: Let $N = \{1, 2, 3, \ldots\}$

$(N, \times)$ is a monoid

SUBGROUP

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

Eg: Let $G = \{1, -1, i, -i\}$

$(G, *)$ is a group.

$H = \{1, -1\}$

Now H is a subset of G, Also $(H, \times)$ is a group under $\times$

$(H, \times)$ is a subgroup of G.

THEOREM

The neccessary and sufficient condition for a non-empty subset H of a group $(G, *)$ to be a subgroup is for $a, b \in H$, $a * b^{-1} \in H$

Soln: Let $(G, *)$ be a group

Part I Let $(H, *)$ be a subgroup of $(G, *)$

Then $(H, *)$ is a group

Let $a, b \in H$ $a * b^{-1} \in H$

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

PART II Let H be a non-empty subset of $(G, *)$ such that for $a, b \in H$

$\Rightarrow b^{-1} \in H$ — (1)

~~Part III~~ To prove $(H, *)$ is a group

For $b = a$ (1) becomes

$a * a^{-1} \in H$

$e \in H$

Identity exist

Let $a = e$, $b \in H$

$e * b^{-1} \in H$

$b^{-} \in H$

For $b \in H$, $b^{-1} \in H$

Inverse exist

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

(1) becomes

$a * (b^{-1})^{-1} \in H$

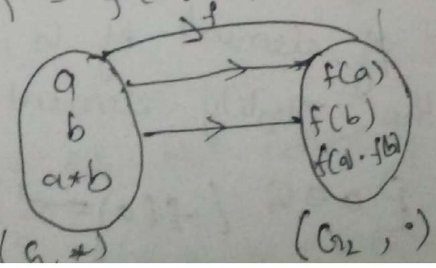
$a * b \in H$ closure property satisfied

$(H, *)$ is a group and hence is a subgroup.

GROUP HOMOMORPHISM

Let $(G_1, *)$ and $(G_2, \cdot)$ be two groups, then the mapping of $f : (G_1, *) \rightarrow (G_2, \cdot)$ is called a group homomorphism.

If $f(a * b) = f(a) \cdot f(b)$ for $a, b, \in G_1$



→ THEOREM

$f : (G, *) \to (G_1, \cdot)$ be a group homomorphism

(i) $f(e) = e'$, where e is the identity in G
e' is the identity in G'

(ii) $f(a^{-1}) = [f(a)]^{-1}$, for any $a \in G$

Solve (i) $f(e) = f(e * e) = f(e) \cdot f(e)$ by defn by homomorphism

∴ $f(e)$ is an idempotent element but only idempotent element in G_1 is the identity element.

$$\boxed{f(e) = e'}$$

(ii)
$$e = a * a^{-1}$$
$$f(e) = f(a * a^{-1})$$
$$f(e) = f(a) \cdot f(a^{-1})$$
$$e^{-1} = f(a) \cdot f(a^{-1})$$

Multiplying both sides by $[f(a)]^{-1}$
$$[f(a)]^{-1} \cdot e' = [f(a)]^{-1} \cdot f(a) \cdot f(a^{-1})$$
$$[f(a)]^{-1} = e' \cdot f(a^{-1})$$
$$[f(a)]^{-1} = f(a^{-1})$$

Kernel of a homomorphism (Ker f)

Let $f : (G, *) \to (G', \cdot)$ be a group homomorphism.

Then the set of elements of G, which are mapped into e', the identity element of G'.

ie, $\ker f = \{ a \in G \mid f(a) = e' \}$

Theorem

The Kernel of a homomorphism f from a group $(G, *)$ to another group $(G', \cdot)$ is a subgroup of $(G, *)$

Proof

Let $\ker f = \{ a \in G \mid f(a) = e' \}$

Let $a, b \in \ker f$

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

$$= f(a) \cdot (f(b))^{-1}$$

$a * b^{-1} \in \ker f$

$f(a) = e'$

$f(b) = e'$

$$= e' \cdot (e')^{-1}$$

$$= e' \cdot e'$$

$$= e'$$

Now

$\ker f$ is a subset of G

Moreover, for $a, b \in \ker f$,

$a * b^{-1} \in \ker f$

$\therefore \ker f$ is a subgroup.

Theorem:

In a group $(G, *)$, Identity element is unique.

Soln:

Let $(G, *)$ be a group.

Let if possible, e and e' be two identity element in G.

Treating e as the identity and e' as an element in G.

$$e * e' = e' * e = e' \quad \text{--- (1)}$$

Treating e' as the identity and e as an element in G.

$$e' * e = e * e' = e \quad \text{--- (2)}$$

Left cosets

Let $(H, *)$ be a subgroup of $(G, *)$. Then set of all elements of $a * h$ is called the left coset. It is denoted by aH.

$$aH = \{a * h / a \in G, h \in H\}$$

Right Coset

$$Ha = \{h * a / a \in G, h \in H\}$$

Lagrange's Theorem

The order of a subgroup divides the order of a group

Proof:

Order of a group = no of elements present in a a group. (only for finite group)

Lemma:

Any two left cosets (right cosets) are either disjoints or identical.

Let aH and bH be two left cosets

Let $c \in aH \cap bH$

Then $c \in aH$ and $c \in bH$

$\Rightarrow c = a * h_1$, $c = b * h_2$

$a * h_1 = b * h_2$ — (1)

Let $x \in aH$

Then $x = a * h_3$

$x = (b * h_2 * h_1^{-1}) * h_3$ (from 1 $a = b * h_2 * h_1^{-1}$)

$x = b * (h_2 * h_1^{-1} * h_3)$

$\in bH$

$x \in aH \Rightarrow x \in bH$

$aH \subset bH$

IIIly we can prove that $bH \subset aH$ — ②

From ① & ②

$aH = bH$

Now G can be written as the finite union of left cosets

$G = a_1 H \cup a_2 H \cup \; a_p H$ — (A)

Now $o(H) = o(aH)$

from (A)

$o(G) = o(a_1 H \cup a_2 H \cup \dots \cup a_p H)$

Assume $o(G) = m$

$o(H) = n$

$o(G) = o(a_1 H) + o(a_2 H) + \dots + o(a_p H)$

$= \underbrace{o(H) + o(H) + \dots}\; + o(H)$

$m = n + n + \dots + n$

$m = pp$

$\Rightarrow$ n divides m

$o(H)$ divides $o(G)$

Cyclic Group

Let (G, o) be a group. Then it is said to be cyclic if every element of G can be written as integral power of same $a \in G$.

ie fo $x \in G$, $x = a^n$ for some $a \in G$]

[there a is called the generator of G

Ex: Let $G = \{1, i, -i, -1\}$ be a under multiplication, then i is called the generator of G.

Order of an element

Let $(G, \cdot)$ be a cyclic group then the order of an element $a \in G$, the least Positive integer "n" such that $a^n = e$, where e is the identity.

Ex: $G = \{1, -1, i, -i\}$ is a cyclic group. Here "1" is the identity element. Then the order of

order of $1 = 1$
" $-1 = 2$
" $i = 4$
" $-i = 4$.

Theorem: Every subgroup of a cyclic group is cyclic.

Proof: Let $(G, \cdot)$ be a cyclic group.
Let $(H, \cdot)$ be a subgroup of $(G, \cdot)$.
Let m be the least +ve integer such that $a^m \in H$ — ①
~~Here a is called the generator of G.~~

Let, If possible, $a^n \in H$ where $n > m$

$\boxed{n = m \cdot q + r}$, $r < m$ — ②

$a^n = a^{m \cdot q + r}$

$a^n = (a^m)^q \cdot a^r \quad [a^r = a^n (a^m)^{-q}$

$r = y \cdot z$
$x \in H$
$y \in H$
$z \in H$

As $a^n, (a^m)^q \in H$, $a^r \in H$

$a^r \in H$. when $r < m$ which is contradiction to ①

$r = 0$

② becomes

$n = m \cdot q$

$a^n = a^{m \cdot q} = (a^m)^q$

$\Rightarrow$ H is cyclic and the generator is a^n

$\therefore$ Hence the theorem.

Combinations

Among n objects, r objects can be arranged in ^nC_r ways $(r<n)$

Solve:

$$a_{n+2} - 3a_{n+1} + 2a_n = 2^n$$

$$r^2 - 3r + 2 = 0$$

$$(r-1)(r-2) = 0$$

$$r = 1, 2.$$

$$a_n^{(C.F)} = k_1(1)^n + k_2 2^n$$

$$\boxed{a_n^{(P)} = A n \cdot 2^n}$$

$$a_{n+1}^{(P)} = A(n+1)2^{n+1}$$

$$a_{n+2}^{(P)} = A(n+2)2^{n+2}$$

$$A(n+2)2^{n+2} - 3A(n+1)2^{n+1} + An2^n = 2^n$$

$$2^n A\left((n+2)4 - 6(n+1) + n\right] = 2^n$$

$$A\left(-n+2\right] = 1$$

$$A = \frac{1}{2-n}$$

$$a_n^{(P)} = n(a_0 + a_1 n)2^n$$

$$a_n = a_n^{(C.F)} + a_n^{P}$$

$$a_{n+2} = a_n + a_{n+1}$$

$$a_{n+2} - a_{n+1} - a_n = 0$$

$$a_{n+2} - a_{n+1} - a_n = 0$$

$$a_{n+2}\, x^n - a_{n+1}\, x^n - a_n x^n = 0$$

$$\sum_{n=0}^{\infty} a_{n+2}\, x^n - \sum_{n=0}^{\infty} a_{n+1}\, x^n - \sum_{n=0}^{\infty} a_n x^n = 0$$

$$\frac{1}{x^2} \sum_{n=0}^{\infty} a_{n+2}\, x^{n+2} - \frac{1}{x} \sum a_{n+1}\, x^{n+1} - G(x) = 0$$

$$\frac{1}{x^2}\left[G(x) - a_0 - a_1 x\right] - \frac{1}{x}\left(G(x) - a_0\right) - G(x) = 0$$

$$\left\{ \left(\frac{1}{x^2} - \frac{1}{x} - 1\right) G(x) - \frac{1}{x^2}\left(a_0 + a_1 x\right) + \frac{a_0}{x} \right\} = 0$$

$$= \frac{1}{x^2}\left(a_0 + a_1 x\right) - \frac{a_0}{x}$$

$$\frac{(1 - x - x^2)\, G(x)}{x^2} = \frac{a_0 + a_1 x - a_0 x}{x^2}$$

$$G(x) = \left(\frac{a_0 + a_1 x - a_0 x}{1 - x - x^2}\right) = \frac{x}{1 - x - x^2}$$

$$= \frac{-x}{x^2 + x - 1} = \frac{-x}{\left(x - \left(\frac{-1+\sqrt{5}}{2}\right)\right)\left(x - \left(\frac{-1-\sqrt{5}}{2}\right)\right)}$$

$$G(x) = \frac{-x}{(x-a)(x-b)}$$

Let $$\frac{-x}{(x-a)(x-b)} = \frac{A}{(x-a)} + \frac{B}{(x-b)}$$

$$-x = A(x-b) + B(x-a)$$

when $x = a$, $-a = A(a-b)$

$$A = -\frac{a}{a-b} \qquad B = \frac{b}{a-b}$$

Scanned by CamScanner

$$G(x) = \frac{-a}{(a-b)}\left[\frac{1}{x-a}\right] + \frac{b}{(a-b)}\left[\frac{1}{x-b}\right]$$

$$= \frac{1}{(a-b)}\left[\frac{1}{1-x/a}\right] - \frac{1}{(a-b)}\left[\frac{1}{1-x/b}\right]$$

$$G(x) = \frac{1}{(a-b)}\left[1 + \frac{x}{a} + \cdots + \left(\frac{x}{a}\right)^n + \cdots\right] - \left(1 + x/b + \cdots + \left(\frac{x}{b}\right)^n + \cdots\right]$$

$a_0 = 0$
$a_1 = 1$

a_n = Coefficient of x^n

$$= \frac{1}{(a-b)}\left[\frac{1}{a^n} - \frac{1}{b^n}\right]x^2$$

$$a_n = \frac{1}{\sqrt{5}}\left[\frac{2^n}{(-1+\sqrt{5})^n} - \frac{2^n}{(-1-\sqrt{5})^n}\right]$$