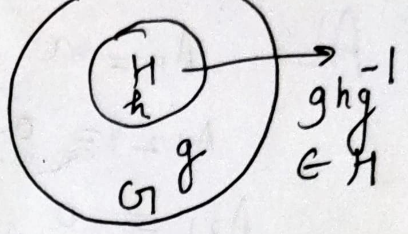
Normal Subgroup

→ A subgroup H of a group G is called a normal subgroup of G if for every $g \in G$, $h \in H$, $\Rightarrow$ $\boxed{ghg^{-1} \in H}$



Q- Let G be the group of 2×2 invertible real matrices $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$; $ad - bc \neq 0$. Let $H = \left[\begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix} : a \neq 0 \right]$.

Then show that H is a normal subgroup of G.

Ans:→ We first show that H is a subgroup of G.

Let $h_1, h_2 \in H$ such that

$$h_1 = \begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix} \quad h_2 = \begin{pmatrix} a_1 & 0 \\ 0 & a_1 \end{pmatrix};$$

$a \neq 0 \quad a_1 \neq 0$

Now $h_1 h_2 = \begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix} \begin{pmatrix} a_1 & 0 \\ 0 & a_1 \end{pmatrix} = \begin{pmatrix} aa_1 & 0 \\ 0 & aa_1 \end{pmatrix}$

$\in H \mid aa_1 \neq 0$

ie. H is closed under matrix multip

Further, For $A \in H$, we have

$$A = \begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix} \quad |A| = \begin{vmatrix} a & 0 \\ 0 & a \end{vmatrix}$$

(Determinant of matrix)

$$\boxed{|A| = a^2}$$

$|A| = (a \times a) - (0 \times 0)$
$= a^2$

Also $A_{11} = a$

$A_{12} = 0$

$A_{21} = 0$

$A_{22} = a$

$\therefore \text{adj } A = \begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix}^T = \begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix}$

(adjoint A)

Transpose

Hence $A^{-1} = \frac{\text{adj } A}{|A|} = \frac{1}{a^2} \begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix} = \begin{pmatrix} \frac{1}{a} & 0 \\ 0 & \frac{1}{a} \end{pmatrix}$

$\in H$, $a \neq 0$

As $|A| = a^2$

Thus each element belonging to H has multiplicative inverse. Hence H is a subgroup of G.

is the matrix that gives you the identity matrix when multiplied by its original matrix

$$g = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in G$$

$$h = \begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix} \in H \quad \text{Consider}$$

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

$$= \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix} \left(\frac{1}{ad-bc} \begin{pmatrix} d & -b \\ -c & a \end{pmatrix} \right)$$

Swap the positions and put −ve sign.

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

$$= \begin{pmatrix} a^2 & ba \\ ca & da \end{pmatrix} \begin{pmatrix} \frac{d}{ad-bc} & \frac{-b}{ab-bc} \\ \frac{-c}{ad-bc} & \frac{a}{ad-bc} \end{pmatrix}$$

$$= \begin{pmatrix} \dfrac{a^2 d - bac}{ad - bc} & \dfrac{-a^2 b + ba^2}{ad - bc} \\[2ex] \dfrac{cad - dac}{ad - bc} & \dfrac{-cab + da^2}{ad - bc} \end{pmatrix}$$

$\cancel{-b(a^2}$

$-b(a^2 - a^2)$

$ca(d-d)$

$$= \begin{pmatrix} \dfrac{a(ad - bc)}{ad - bc} & 0 \\[2ex] 0 & \dfrac{a(ad - bc)}{ad - bc} \end{pmatrix}$$

$$= \begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix} \in H$$

Hence H is a normal subgroup of G under matrix multiplication.

$$= \begin{pmatrix} \dfrac{a^2d - bac}{ad - bc} & \dfrac{-a^2b + ba^2}{ad - bc} \\[2ex] \dfrac{cad - dac}{ad - bc} & \dfrac{-cab + da^2}{ad - bc} \end{pmatrix} \quad \begin{matrix} \cancel{-b}\,(a^2 \\ -b(a^2 - a^2) \end{matrix}$$

$$c a(d - d) \qquad = \begin{pmatrix} \dfrac{a(ad - bc)}{ad - bc} & 0 \\[2ex] 0 & \dfrac{a(ad - bc)}{ad - bc} \end{pmatrix}$$

$$= \begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix} \in H$$

Hence H is a normal subgroup of G under matrix multiplication.

Homomorphism of Groups

* Let $(G, \circ)$ and $(G', *)$ be 2 groups.
* $f : \underset{\circ}{G} \to \underset{*}{G'}$ a mapping. $(a, b \in G)$

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

$a \quad f(a)$

$b \quad f(b)$

if this is satisfied, then $f(a \circ b) \quad f(a) * f(b)$ we call it as homomorphism.

Ex.1 Show that $f : G \to G'$ defined by $f(x) = 2^x$ is a homomorphism, where $G = (R, +)$, $G' = (R^+, \cdot)$

Ans:→ To show $f(a+b) = f(a) \cdot f(b) \quad \forall a, b \in G$

$$f(a) = 2^a, \quad f(b) = 2^b$$

$$f(a+b) = 2^{a+b} = 2^a \cdot 2^b = f(a) \cdot f(b)$$

$$f(a+b) = f(a) \cdot f(b) \Rightarrow f \text{ is homomorphism.}$$

Ex-2 Show that $f : (Z, +) \to (Z, +)$ defined by $f(x) = x \quad \forall x \in Z$ is a homomorphism.

Soln:→ To show $f(a+b) = f(a) + f(b) \quad \forall a, b \in Z$

$f(a) = a \quad f(b) = b \quad f(a+b) = a+b$

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

$\Rightarrow f$ is a homomorphism.

→ if f is one - one $\Rightarrow f$ is called monomorphism

→ if f is onto $\Rightarrow f$ is called epimorphism

→ if f is one - one and onto $\Rightarrow f$ is called isomorphism.
bijection

→ If $f: G \to G$ is a homomorphism $\Rightarrow f$ is called endomorphism.

→ If $f: G \to G$ is an isomorphism $\Rightarrow f$ is called automorphism

→ An isomorphism is also called automorphism if both domain and range are equal.

Cyclic group

① If every element of group G is of the form a^n for some $a \in G$ and some integer n, then G is called cyclic group.

* a is called generator of G.

* If G is the cyclic group generated by a. It is denoted by $\langle a \rangle$.

Show that the multiplicative group ②

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

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

$i^2 = (-1) \cdot i$

$(i)^4 = 1$

$\Rightarrow$ i is a generator of G

$\Rightarrow$ G is cyclic.

→ ~~Similarly, ⇒ i is also a generator of G~~

~~⇒ G is cyclic.~~

Similarly, $-i$ is also a generator of G.

Q2. Find the generators of the multiplicative group $\{1, \omega, \omega^2\}$

$(\omega)^1 = \omega$, $(\omega^2) = \omega^2$, $(\omega^3) = 1$

$\Rightarrow$ ω is a generator

$(\omega^2)^1 = \omega^2$ $(\omega^2)^2 = \omega^4 = \omega^3 \cdot \omega = \omega$

$(\omega^2)^3 = \omega^6 = 1$

$\Rightarrow$ ω^2 is also a generator

$\Rightarrow$ 1 is not a generator

$\Rightarrow$ ω and ω^2 are generators.

Q: Show that $A = (\{0,1,2,3,4,5\}, +_6)$ is cyclic. find all generators.

$(1)^1 = 1$ $\quad (1)^2 = 1 +_6 1 = 2$

$(1)^3 = 3$ $\quad (1)^4 = 4$ $\quad (1)^5 = 5$

$(1)^6 = 0$

$\Rightarrow$ 1 is a generator of A

$\Rightarrow$ A is cyclic

$(2)^1 = 2$ $\quad (2)^2 = 2 +_6 2 = 4$ $\quad (2)^3 = 0$

$(2)^4 = 2$ $\quad$ 2 is not a generator

Similarly, 3 and 4 are not generators.

$(5)^1 = 5$ $\quad (5)^2 = 5 +_6 5 = 4$

$(5)^3 = 5 +_6 5^2 = 5 +_6 4 = 3$

$(5)^4 = 5 +_6 (5)^3 = 2$

$(5)^5 = 5 +_6 (5^4 = 1$

$(5)^6 = 5 +_6 5^5 = 5 +_6 1 = 0$

$\Rightarrow$ 5 is also a generator

$\therefore$ 1 and 5 are generators of A

Show that $(Z, +)$ is a cyclic group. (3)

Ans: $1^0 = 0$, $1^1 = 1$, $1^2 = 1+1 = 2$, $1^3 = 3$

$1^4 = 4$ and so on

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

$1^{-3} = (1^3)^{-1} = 3^{-1} = -3$ $(\because a \Rightarrow -a)$ is the inverse

$\Rightarrow$ 1 is a generator $\Rightarrow$ $(Z, +)$ is a cyclic group.

Similarly, -1 is also a generator.

- Every cyclic group is abelian.
- If a is a generator G, then a^{-1} is also a generator.

Order of Group

- **Finite Group** :- A group consisting of finite no. of elements is called as finite group.
- **Infinite Group** :- A group having infinite no. of elements is called infinite group.

Ex.1 :- $Z = \{ \ldots\ldots -3, -2, -1, 0, 1, 2, 3, \ldots \}$

$\rightarrow$ Infinite Group with operation $+$

Ex.2 :- $G = \{1, -1, i, -i\}$ $(G, \times)$ $\rightarrow$ finite Group.

Order of a group :→ The no. of elements in a finite group is called the order of the group.

* An infinite group is said to be infinite order.

ex :- $G = \{1, -1, i, -i\}$ $(G, \times)$ is a group of order 4.

$G = \{1, \omega, \omega^2\}$, $G(\times)$ is a group of order 3.

Note :→ The order of a group is denoted by $o(G)$.