Abstract Algebra

Page No.
Date

* Introduction:-

* Notes:-

1) N denotes the set of all natural numbers
   i.e.
   $N = \{1, 2, 3, \ldots\}$

2) 'Z' is the set of all integers
   i.e.
   $Z = \{0, \pm 1, \pm 2, \pm 3, \ldots\}$

3) 'Q' is the set of all rational numbers
   i.e.
   $Q = \left\{\frac{p}{q} / q \neq 0\right\}$

4) 'R' is the set of all real numbers

5) 'C' is the set of all complex numbers
   i.e.
   $C = \{z = x + iy / x, y \in R\}$

* Union Intersection:-

Let A & B be subsets of a set 'U' then the union of A&B is written as $A \cup B$
i.e.
$A \cup B = \{x \in U / x \in A \text{ or } x \in B\}$

Page No.
Date

* Intersection :-

The intersection of A & B written as $A \cap B$

i.e. $A \cap B = \{ x \in U / x \in A \text{ and } x \in B \}$

* Difference :-

The difference of A & B written as $A - B$

i.e.

$A - B = \{ x \in U / x \in A \text{ but } x \notin B \}$

* Cartesian Product :-

Let 'A', 'B' be sets, the set of all order pairs (x, y) where

$x \in A$ & $y \in B$ is called cartesian product of A & B and it is denoted by $A \times B$

i.e.

$A \times B = \{ (x, y) / x \in A, y \in B \}$

eg :- 1) $A = \{1, 2, 3, 4\}$, $B = \{a, b, c\}$ write down $A \times B$

→ $A = \{1, 2, 3, 4\}$, $B = \{a, b, c\}$

$\therefore A \times B = \{ (1,a), (1,b), (1,c), (2,a), (2,b), (2,c),$
$(3,a), (3,b), (3,c), (4,a), (4,b), (4,c) \}$

* Cardinality of a set :-

Let A and B be the sets, then the cardinality of a set A & B. it is denoted by $|A|$ & $|B|$

Let A & B be sets if $\exists$ an injective

Page No.
Date

mapping

$f: A \to B$ then, cardinality of $|A|$ & $|B|$ is said to be less than equal to cardinality

$$|A| \leq |B|$$

(If cardinality of A is greater than cardinality of B ($|A| > |B|$) then no. of element A does not have preimage in B)

Let A & B be the sets and the mapping $f: A \to B$ then, cardinality of A ($|A|$) is greater than or equal to cardinality of B ($|B|$) if f is subjective i.e onto

$$|A| \geq |B|$$

(If $|A|$ is strictly less than of $|B|$ then does not exist a subjective mapping)

Let A & B be the sets and the mapping $f: A \to B$ $\exists$ a bijective ~~mapping~~ if $|A| = |B|$

* Note :-

Let n be a fixed passitive integer. let $x, y \in \mathbb{Z}$ suppose that $x \equiv y$ means

$$x \equiv y \pmod{n}$$

$$\Rightarrow n / x-y$$

then '$\equiv$' is an equivalence relation on '$\mathbb{Z}$'

The set of equivalence classes denoted by $\mathbb{Z}_n$ or $\mathbb{Z}/(n)$ is the set

$$\mathbb{Z}_n = \{ \bar{0}, \bar{1}, \bar{2}, \text{------}, \overline{n-1} \}$$

* **Algebric Structure:-**

A non empty set with one or more binary operation define over it and satisfying certain laws of binary operations is called Algebric structure

e.g :- (R,+), (R,·), (Q,+), (Q,·), (C,+), (C,·)

* **Binary operation:-**

Let 's' be non empty set the function $* : S \times S \longrightarrow S$ is called binary operation on 's', here image of $(x,y) \in S \times S$ under '*' it is denoted by "$x*y$".

* **Semi group:-**

Let 'G' be a non empty set and '*' be a binary operation on 'G' then the algebric structure (G,*) is said to be a semi group if $a,b \in G$

then, $a*b \in G$

and $a,b,c \in G$

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

e.g:- (N,+), (R,+), (R,-), (R,·), (Z,+), (Z,-), (Z,·)
(Q,+).

* **Group :-**

Let a non empty set G with a binary operation '*' on 'G' is called a group if the following properties are hold

1) Closure property :-

$\forall a, b \in G$
$\Rightarrow a*b \in G$

2) Associative property:-

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

3) Existance of identity :- (e is an identity element)

Their exist an element $e \in G$ such that
$a*e = a = e*a$ $\therefore$ e is said to be identity in G

4) Existance of inverse:-

$\forall$ element $a \in G$ then $\exists$ an element $b \in G$ such that,
$a*b = b*a = e$

* Examples:-

1) Show that $(R, +)$ is a group

→ R is a non empty set
$R = \{0, 1, 2, 3, 4, \ldots\}$

1) Closure

$\forall a, b \in R$
then $a+b \in R$

2) Associative

$\forall\ a, b, c \in R$

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

3) Existance of identity

$\exists\ 0 \in R$ such that

$a+0 = a = 0+a$

4) Existance of inverse

$\forall\ a \in R$ such that

$a+(-1) = 0$

$\therefore (R, +)$ is an group.

2) $(Q, +)$ ~~is~~

→ Q is a non empty set

$Q = \{ p/q \ / q \neq 0 \}$

1) Closure

$\forall\ a, b \in Q$

then, $a+b \in Q$

2) Associative

$\forall\ a, b, c \in R$

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

3) Existance of identity

$\exists\ e = 0 \in Q$ Such that $\frac{p}{q} + 0 = \frac{p}{q}$

$\therefore 0$ is identity in Q

4) Existance of inverse

$\forall \frac{p}{q} \in Q$ such that

$\frac{p}{q} + \left(\frac{-p}{q}\right) = 0 \quad \left(\because \frac{-p}{q} \in Q\right)$

3) $(Q, \cdot)$

→ Q is a non empty set

$Q = \{p/q \ / q \neq 0\}$

1) Closure

$\forall a, b \in Q$

then $a \cdot b \in Q$

2) Associative

$\forall a, b, c \in R$

then $a \cdot (b \cdot c) = (a \cdot b) \cdot c$

3) ~~Associative~~ Existance of identity

$\exists 1 \in Q$ such that $\frac{p}{q} \cdot 1 = \frac{p}{q}$

$\therefore 1$ is identity in Q

4) Existance of inverse :-

we have $\frac{p}{q} \times \frac{q}{p} = 1$

$\Rightarrow (p/q)$ have inverses q/p where $p \neq 0$

4) Show that 'z' with a set of all integers form a group with a binary operation '$*$' defined by

$a * b = a + b + 1 \quad \forall a, b \in z$

5) Show that the set $G = \{1, -1, i, -i\}$ is a group w.r.t multiplication operation (means $\cdot$)

4) $\longrightarrow$

$\rightarrow$ Here,

Z is a non empty set

1) Closure

let, $a, b \in Z$

$a * b = a + b + 1$

here,

$a, b \in Z \Rightarrow a + b$ also belongs to Z

$a * b = a + b + 1$ also belongs to Z

$\Rightarrow a * b \in Z$

2) Associative

$\forall a, b, c \in Z$

$\Rightarrow a * (b * c) = a * (b + c + 1)$

$= a + b + c + 1 + 1$

$= a + b + c + 2 \quad — (1)$

also,

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

$= a + b + 1 + c + 1$

$= a + b + c + 2 \quad — (2)$

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

3) Exeistance of identity

$\exists e \in Z$, such that

$a * e = a$

Scanned by CamScanner

now,

$$a * e = a + e + 1 = a$$
$$\Rightarrow e + 1 = a - a$$
$$\Rightarrow e + 1 = 0$$
$$\Rightarrow e = -1 \in \mathbb{Z}$$

4) Existance of inverse

$\exists$ b such that

$$a * b = e = -1$$
$$\Rightarrow a + b + 1 = -1$$
$$\Rightarrow b = -2 - a \in \mathbb{Z}$$

$\therefore$ set of integers with binary operation '$*$' defined by $a * b = a + b + 1$ is a group.

5) ——— ?

→ Here, G is a non empty set

1) closure

let, $a, b \in G$ & $a = 1, b = -1$

$\therefore a \cdot b = 1 \cdot (-1) = -1 \in G$

2) Associative

let, $a, b, c \in G$ & $a = 1, b = -1, c = i$

$\therefore a \cdot (b \cdot c) = 1 (1 \cdot i) = i$ — ①

& $(a \cdot b) \cdot c = (1 \cdot 1) \cdot i = i$ — ②

$\Rightarrow a \cdot (b \cdot c) = (a \cdot b) \cdot c$

Page No.
Date

3) Exeistance of identity
$\exists\ e \in G$ such that   let $= a = 1$
$a \cdot e = a$
$\Rightarrow 1 \cdot e = 1 \Rightarrow e = -1 \quad \in G$

4) Exeistance of inverse
$\exists\ b \in G$ such that $\&\ a = 1$
$a \cdot b = e$
$1 \cdot b = -1$
$b = -1/1 = -1 \quad \in G.$

$\therefore G$ is a group

6) Show that $\begin{bmatrix} a & b \\ c & d \end{bmatrix}$ the set of 2x2 matrices with real entress under componentwise addition
i.e. $\begin{bmatrix} a_1 & b_1 \\ c_1 & d_1 \end{bmatrix} + \begin{bmatrix} a_2 & b_2 \\ c_2 & d_2 \end{bmatrix} = \begin{bmatrix} a_1+a_2 & b_1+b_2 \\ c_1+c_2 & d_1+d_2 \end{bmatrix}$

to show that this is a group.

$\rightarrow$ Let,
$G = \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} \Big/ a, b, c, d \in R \right\}$

1) Closure property
$\forall\ A, B \in G$ such that
$A = \begin{bmatrix} a_1 & b_1 \\ c_1 & d_1 \end{bmatrix}, B = \begin{bmatrix} a_2 & b_2 \\ c_2 & d_2 \end{bmatrix}$

Page No.
Date

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

$$= \begin{bmatrix} a_1+a_2 & b_1+b_2 \\ c_1+c_2 & d_1+d_2 \end{bmatrix} \in G$$

$\forall\ a_1+a_2,\ b_1+b_2,\ c_1+c_2,\ d_1+d_2 \in R$

2) Associative property

let,

$A, B, C \in G$ such that.

$$A = \begin{bmatrix} a_1 & b_1 \\ c_1 & d_1 \end{bmatrix},\ B = \begin{bmatrix} a_2 & b_2 \\ c_2 & d_2 \end{bmatrix},\ C = \begin{bmatrix} a_3 & b_3 \\ c_3 & d_3 \end{bmatrix}$$

$$A+(B+C) = \left[\begin{bmatrix} a_1 & b_1 \\ c_1 & d_1 \end{bmatrix} + \left[\begin{bmatrix} a_2 & b_2 \\ c_2 & d_2 \end{bmatrix} + \begin{bmatrix} a_3 & b_3 \\ c_3 & d_3 \end{bmatrix}\right]\right]$$

$$= \begin{bmatrix} a_1 & b_1 \\ c_1 & d_1 \end{bmatrix} + \begin{bmatrix} a_2+a_3 & b_2+b_3 \\ c_2+c_3 & d_2+d_3 \end{bmatrix}$$

$$= \begin{bmatrix} a_1+a_2+a_3 & b_1+b_2+b_3 \\ c_1+c_2+c_3 & d_1+d_2+d_3 \end{bmatrix}$$

$$= \begin{bmatrix} a_1+a_2 & b_1+b_2 \\ c_1+c_2 & d_1+d_2 \end{bmatrix} + \begin{bmatrix} a_3 & b_3 \\ c_3 & d_3 \end{bmatrix}$$

$$= \left(\begin{bmatrix} a_1 & b_1 \\ c_1 & d_1 \end{bmatrix} + \begin{bmatrix} a_2 & b_2 \\ c_2 & d_2 \end{bmatrix}\right) + \begin{bmatrix} a_3 & b_3 \\ c_3 & d_3 \end{bmatrix}$$

$$= (A+B)+C$$

$\Rightarrow A+(B+C) = (A+B)+C$

$\forall\ a_1+a_2+a_3,\ b_1+b_2+b_3,\ c_1+c_2+c_3,\ d_1+d_2+d_3 \in R$

Page No.
Date

3) Existance of identity
$\exists\ e \in G$ such that
$A + e = A$
$e = A - A$
$e = 0$
$\Rightarrow e = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix} \in G \quad \forall\ 0 \in R$

4) Existance of inverse
$\exists\ B \in G$ such that.

$A + B = e$
$B = e - A$
$B = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix} - \begin{bmatrix} a_1 & b_1 \\ c_1 & d_1 \end{bmatrix}$

$B = \begin{bmatrix} -a_1 & -b_1 \\ -c_1 & -d_1 \end{bmatrix} \in G \quad \forall\ -a_1, -b_1, -c_1, -d_1 \in R$

hence,
set of 2x2 matrices with real integer under componentwise addition is group

7) The set of 2x2 matrices with integer entries under componentwise addition
i.e $\begin{bmatrix} a_1 & b_1 \\ c_1 & d_1 \end{bmatrix} + \begin{bmatrix} a_2 & b_2 \\ c_2 & d_2 \end{bmatrix} = \begin{bmatrix} a_1+a_2 & b_1+b_2 \\ c_1+c_2 & d_1+d_2 \end{bmatrix}$

to show that this is a group

8) The set of 2x2 matrices with Natural entries under componentwise addition i.e. $\begin{bmatrix} a_1 & b_1 \\ c_1 & d_1 \end{bmatrix} + \begin{bmatrix} a_2 & b_2 \\ c_2 & d_2 \end{bmatrix} = \begin{bmatrix} a_1+a_2 & b_1+b_2 \\ c_1+c_2 & d_1+d_2 \end{bmatrix}$

to cheak that this is a group or not.

7) $\longrightarrow$

→ let,

$$G = \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} \Big/ a, b, c, d \in \mathbb{Z} \right\}$$

with componantwise addition

1) Closure propeety.

$\forall$ $A, B \in G$ such that

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

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

$$A+B = \begin{bmatrix} a_1+a_2 & b_1+b_2 \\ c_1+c_2 & d_1+d_2 \end{bmatrix} \in G \quad \forall\ a_1 a_2, b_1, b_2, c_1, c_2, d_1, d_2 \in \mathbb{Z}$$

2) Associative propeety

let,

$A, B, C \in G$ such that,

$$A = \begin{bmatrix} a_1 & b_1 \\ c_1 & d_1 \end{bmatrix}, \quad B = \begin{bmatrix} a_2 & b_2 \\ c_2 & d_2 \end{bmatrix}, \quad C = \begin{bmatrix} a_3 & b_3 \\ c_3 & d_3 \end{bmatrix}$$

$$A + (B+C) = \begin{bmatrix} a_1 & b_1 \\ c_1 & d_1 \end{bmatrix} + \left(\begin{bmatrix} a_2 & b_2 \\ c_2 & d_2 \end{bmatrix} + \begin{bmatrix} a_3 & b_3 \\ c_3 & d_3 \end{bmatrix} \right)$$

$$= \begin{bmatrix} a_1 & b_1 \\ c_1 & d_1 \end{bmatrix} + \begin{bmatrix} a_2+a_3 & b_2+b_3 \\ c_2+c_3 & d_2+d_3 \end{bmatrix}$$

$$= \begin{bmatrix} a_1+a_2+a_3 & b_1+b_2+b_3 \\ c_1+c_2+c_3 & d_1+d_2+d_3 \end{bmatrix}$$

$$= \begin{bmatrix} a_1+a_2 & b_1+b_2 \\ c_1+c_2 & d_1+d_2 \end{bmatrix} + \begin{bmatrix} a_3 & b_3 \\ c_3 & d_3 \end{bmatrix}$$

$$= \left(\begin{bmatrix} a_1 & b_1 \\ c_1 & d_1 \end{bmatrix} + \begin{bmatrix} a_2 & b_2 \\ c_2 & d_2 \end{bmatrix} \right) + \begin{bmatrix} a_3 & b_3 \\ c_3 & d_3 \end{bmatrix}$$

$$= (A+B)+C$$

$\Rightarrow$ $A+(B+C) = (A+B)+C \quad \forall \; a_1, a_2, a_3, b_1, b_2, b_3, c_1, c_2, c_3, d_1, d_2, d_3 \in \mathbb{Z}$

3) Existance of identity

$\exists \; e \in G$ such that

$$A+e = A$$

$$e = A-A$$

$$e = 0$$

$$e = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix} \in G \qquad \forall \; 0 \in \mathbb{Z}$$

4) Existance of inverse

$\exists \; B \in G$ such that

$$A+B = e$$

$$B = e-A$$

$$B = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix} - \begin{bmatrix} a_1 & b_1 \\ c_1 & d_1 \end{bmatrix}$$

Date

$$B = \begin{bmatrix} -a_1 & -b_1 \\ -c_1 & -d_1 \end{bmatrix} \in G \quad \forall -a_1, -b_1, -c_1, -d_1 \in Z$$

hence,
A set of 2x2 matrices with integer entries is a group

8) ⟶ ?

→ let,

$$G = \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} / \forall a, b, c, d \in N \right\}$$

1) Closure property

$\forall$ A, B $\in$ G such that.

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

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

$$A + B = \begin{bmatrix} a_1 + a_2 & b_1 + b_2 \\ c_1 + c_2 & d_1 + d_2 \end{bmatrix} \in G \quad \forall \begin{matrix} a_1, a_2, b_1, b_2 \\ c_1, c_2, d_1, d_2 \end{matrix} \in N$$

2) Associative property

let A, B, C $\in$ G such that

$$A = \begin{bmatrix} a_1 & b_1 \\ c_1 & d_1 \end{bmatrix}, \quad B = \begin{bmatrix} a_2 & b_2 \\ c_2 & d_2 \end{bmatrix}, \quad C = \begin{bmatrix} a_3 & b_3 \\ c_3 & d_3 \end{bmatrix}$$

$$A + (B + C) = \begin{bmatrix} a_1 & b_1 \\ c_1 & d_1 \end{bmatrix} + \left(\begin{bmatrix} a_2 & b_2 \\ c_2 & d_2 \end{bmatrix} + \begin{bmatrix} a_3 & b_3 \\ c_3 & d_3 \end{bmatrix} \right)$$

$$= \begin{bmatrix} a_1 & b_1 \\ c_1 & d_1 \end{bmatrix} + \begin{bmatrix} a_2+a_3 & b_2+b_3 \\ c_2+c_3 & d_2+d_3 \end{bmatrix}$$

$$= \begin{bmatrix} a_1+a_2+a_3 & b_1+b_2+b_3 \\ c_1+c_2+c_3 & d_1+d_2+d_3 \end{bmatrix}$$

$$= \begin{bmatrix} a_1+a_2 & b_1+b_2 \\ c_1+c_2 & d_1+d_2 \end{bmatrix} + \begin{bmatrix} a_3 & b_3 \\ c_3 & d_3 \end{bmatrix}$$

$$= \left(\begin{bmatrix} a_1 & b_1 \\ c_1 & d_1 \end{bmatrix} + \begin{bmatrix} a_2 & b_2 \\ c_2 & d_2 \end{bmatrix} \right) + \begin{bmatrix} a_3 & b_3 \\ c_3 & d_3 \end{bmatrix}$$

$$= (A+B)+C$$

$\Rightarrow \quad A+(B+C) = (A+B)+C \quad \forall \; a_1, a_2, a_3, b_1, b_2, b_3, c_1, c_2, c_3, d_1, d_2, d_3 \in N$

3) Existance of identity

$\exists \; e \in G$ such that

$A + e = A$

$e = A - A$

$e = 0$

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

but $e = 0 \notin N$

$\therefore$ The set of 2×2 matrices with Natural entries does not satisfies III^{rd} condition of properties of group

$\therefore$ This is not a group

9) Let A be a set of mapping from $R \to R$ show that $(A+)$ is a group under usual addition of mappings

→ Let, A is a set $A = \{f / f : R \to R\}$ with usual addition of mapping

$(f+g)(x) = f(x) + g(x)$

here,

A is non-empty

Now,

following conditions are hold

1) Closure property

let,

$f, g \in A$

i.e. $f : R \to R$

& $g : R \to R$

$\Rightarrow f+g : R \to R$

$(f+g)(x) = f(x) + g(x)$

$\therefore f+g \in A$

2) Associative property

let,

$f, g, h \in A$

i.e. $f : R \to R$

$g : R \to R$

$h : R \to R$

Page No.
Date

Now consider

$$(f+(g+h))(x) = f(x)+(g+h)(x)$$
$$= f(x)+g(x)+h(x)$$
$$= (f+g)(x)+h(x)$$
$$= ((f+g)+h)(x)$$

$$\implies (f+(g+h)) = (f+g+h)$$

3) Existance of identity

$\exists$ e such that

$$f(x)+e(x) = f(x)$$
$$e(x) = f(x)-f(x)$$
$$e(x) = 0(x)$$

$\therefore$ $e: R \to R$, $e=0$

$\therefore$ e is an identity of mapping

4) Existance of inverse

$\exists$ h such that

$$f(x)+h(x) = e(x)$$
$$h(x) = e(x)-f(x)$$
$$= 0(x)-f(x)$$
$$= (0-f)(x)$$
$$h(x) = -f(x)$$

since

$-f: R \to R$, which is inverse of 'f'

Page No.
Date

10) Let, H be the subset of 'C' consisting of the n^{th} root of unity prove that 'H' is a group under multiplication.

→ Let, H be a set such that

$$H = \{x / x^n = 1\}$$

here, H is non empty

Now,

following conditions are hold

1) Closure property

let,

$x, y \in H$ such that

$x^n = 1, y^n = 1$

$$(x \cdot y)^n = (n)^n$$

$$x^n \cdot y^n = 1 \cdot 1$$

$$x^n \cdot y^n = 1 \in H$$

2) Associative property

let,

$x, y, z \in H$ such that

$x^n = 1, y^n = 1$ & $z^n = 1$

$$(x(y \cdot z))^n = x^n (y \cdot z)^n$$

$$= x^n \cdot y^n \cdot z^n$$

$$= 1 \cdot 1 \cdot 1$$

$$= 1 \quad \text{—— (1)}$$

Page No.
Date

$$((x\cdot y)\cdot z)^n = (x\cdot y)^n\cdot z^n$$
$$= x^n\cdot y^n\cdot z^n$$
$$= 1\cdot 1\cdot 1$$
$$= 1 \longrightarrow ②$$

from eqn ① & ②

$$(x\cdot(y\cdot z))^n = ((x\cdot y)\cdot z)^n$$
$$\Rightarrow x\cdot(y\cdot z) = (x\cdot y)\cdot z \quad \in H$$

3) Existance of identity
$\exists e$ such that

$$(x\cdot e)^n = x^n$$
$$x^n\cdot e^n = x^n$$
$$\Rightarrow e^n = \frac{x^n}{x^n}$$
$$= 1$$
$$\Rightarrow e^n = 1 \quad \in H$$

4) Existance of invese
$\exists y$ such that

$$(x\cdot y)^n = e^n$$
$$x^n\cdot y^n = e^n$$
$$y^n = e^n/x^n \Rightarrow 1/x^n \Rightarrow -x^n$$
$$\therefore y^n = -x^n \quad \in H$$

$\therefore$ This is a group

* Examples of Group:-

1) Integer Modulo 'n' under addition operation:-

let, $x, y \in Z$ and let n be a (+)ve integer define $x \equiv y \pmod{n}$

If $\frac{n}{x-y}$

$\implies x-y = nK \qquad K \in Z$

clearly, '$\equiv$' is an equivalence relation denote by '$\bar{x}$', the equivalence class containing x.
let, $Z/(n)$ denote the set of equivalence classes

we define addition in $Z/(n)$ as follow

$$\bar{x} + \bar{y} = \overline{x+y}$$

this is define

thus, $Z/\text{mod } n$ is an additive abelian group of order 'n'.

$$Z/(n) \text{ or } Z_n = \{\bar{0}, \bar{1}, \bar{2}, \ldots\ldots, \overline{n-1}\}$$

by the cayley table we will prove for Z_6

Now,

$$Z_6 = \{0, 1, 2, 3, 4, 5\}$$

$Z_n^* = \{ k \in Z_n / k < n \text{ s.t. } \gcd(k,n) = 1 \}$

$+_6$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$
$\bar{0}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$
$\bar{1}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$	$\bar{0}$
$\bar{2}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$	$\bar{0}$	$\bar{1}$
$\bar{3}$	$\bar{3}$	$\bar{4}$	$\bar{5}$	$\bar{0}$	$\bar{1}$	$\bar{2}$
$\bar{4}$	$\bar{4}$	$\bar{5}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$
$\bar{5}$	$\bar{5}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$

In general, we can say Z_n is group under addition modulo n.

2) Integer modulo N under multiplication

Consider the set $Z/(n)$ as in above we define,

multiplication in $Z/(n)$

$$\bar{x} \cdot \bar{y} = \overline{x \cdot y}$$

as proved for addition in example above

We can prove the multiplication is well define then

$(Z_n, \cdot)$ is a semi group with identity and the set 'Z_n^*' consisting of the invertible elements in $Z/(\text{mod } n)$ form a multiplicative group of order $\phi(n)$

where ϕ is an Euler function.

eg:- To show that Z_7 is a group under addition operation

$+_7$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$	$\bar{6}$
$\bar{0}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$	$\bar{6}$
$\bar{1}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$	$\bar{6}$	$\bar{0}$
$\bar{2}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$	$\bar{6}$	$\bar{0}$	$\bar{1}$
$\bar{3}$	$\bar{3}$	$\bar{4}$	$\bar{5}$	$\bar{6}$	$\bar{0}$	$\bar{1}$	$\bar{2}$
$\bar{4}$	$\bar{4}$	$\bar{5}$	$\bar{6}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$
$\bar{5}$	$\bar{5}$	$\bar{6}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$
$\bar{6}$	$\bar{6}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$

we define $a +_7 b \in Z_7$
for all $a, b \in Z_7$

1) clearly closure property satisfied
2) Associative property also done
3) $\exists\ \bar{0} \in Z_7$ is an identity element w.r.t addition modulo 7 $(+_7)$.
4) Inverses :-

$\bar{0}$	$\bar{0}$
$\bar{1}$	$\bar{6}$
$\bar{2}$	$\bar{5}$
$\bar{3}$	$\bar{4}$
$\bar{4}$	$\bar{3}$
$\bar{5}$	$\bar{2}$
$\bar{6}$	$\bar{1}$

respectively

$\therefore$ all properties are satisfied
$\therefore (Z_7, +_7)$ is an group.

H.W To show that Z_{12}^*, Z_{10}^*, Z_5^* group under multiplication

3) Z_5^*

→ $Z_5^* = \phi(5)$
$= 5-1$
$= 4$

$\therefore Z_5^* = \{1, 2, 3, 4\}$

$\times_5$	1	2	3	4
1	1	2	3	4
2	2	4	1	3
3	3	1	4	2
4	4	3	2	1

* Note!-
1) Z_n is a group w.r.t addition modulo 'n'.
2) Z_n^* is a group w.r.t multiplication modulo 'n'. with $\phi(n)$ element

* Abelian Group!-
It the binary operation on a group $(G,*)$ is commutative i.e.
$a*b = b*a \quad \forall\, a, b \in G$

Scanned by CamScanner

then the group is called abelian group.

3/07/2019

* Permutation Group:-

Let 'X' be a non empty set and let 'G' be the set of bijective mapping on 'X' to 'X' i.e. permutation of 'X'. Then 'G' is a group under usual composition of mapping. The unit element of 'G' is the identity map of 'X' and the other group postulate are easily verified.

The group is called group of permutation of X (symmetric group on X). It is denoted by 'Sx'

If cardinality of 'X' ($|X|=n$) then

$|S_x| = n!$

Now,

To show that S_3 is a group under composition operation

Let,

$S_3 = \{ (1)(2)(3), (1\,2\,3), (1\,3\,2), (1)(2\,3), (1\,3)(2), (1\,2)(3) \}$

1) closure property

let, $(1\ 2\ 3), (1\ 3\ 2) \in S_3$

now,

$$\begin{bmatrix} 1 & 2 & 3 \\ \downarrow & \downarrow & \downarrow \\ 2 & 3 & 1 \end{bmatrix} \begin{bmatrix} 1 & 3 & 2 \\ \downarrow & \downarrow & \downarrow \\ 3 & 2 & 1 \end{bmatrix}$$

$$\Rightarrow \begin{bmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{bmatrix}$$

i.e. $(1)(2)(3) \in S_3$

$\therefore (1\,2\,3)(1\,3\,2) \in S_3$

2) Associative

let, (2 3), (1 3) & (1 2 3) $\in S_3$.

then.

$$(2\ 3)\left[(1\ 3)\ (1\ 2\ 3)\right]$$

$$\begin{bmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{bmatrix}\left(\begin{bmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{bmatrix}\begin{bmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{bmatrix}\right).$$

$$= \begin{bmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{bmatrix}\begin{bmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{bmatrix}$$

$$= \begin{bmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{bmatrix} \Longrightarrow (1\ 3\ 2)$$

Simillarly,

$$\left[(2\ 3)\ (1\ 3)\right](1\ 2\ 3)$$

$$\left(\begin{bmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{bmatrix}\begin{bmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{bmatrix}\right)\begin{bmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{bmatrix}$$

$$= \begin{bmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{bmatrix}\begin{bmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{bmatrix}$$

$$= \begin{bmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{bmatrix} \Longrightarrow (1\ 3\ 2)$$

$$\therefore \left[(2\ 3)\ (1\ 3)\right](1\ 2\ 3) = (2\ 3)\left[(1\ 3)(1\ 2\ 3)\right]$$

3) Exeistance of identity

$\exists$ e such that

$a \circ e = a$

we exeist a mapping which is identity (1)(2)(3)

4) Existance of inverse

$\exists$ b such that

$a \cdot b = e$

$(1\ 2\ 3) \cdot$ ~~b = (1) (2) (3)~~

$a = \begin{bmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{bmatrix} \cdot$ ~~$b = \begin{bmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{bmatrix}$~~

$b = (1 3 2)$

$\therefore ab = (123)(132) = (1)(2)(3)$

$\therefore$ a has inverse $b = (132)$.

$\therefore$ Find all inverses

* Symmetrices of a Geometric Figure:-

Consider permutation of the set 'X' of all points of some geometric fig called a permutation $\sigma : X \to X$ a symmetry of S when it preserve distances i.e when $d(a, b) = d(\sigma(a), \sigma(b))$

where,

$d(a, b)$ denotes the distance between points $a, b \in X$ if σ, τ are two symmetrices then,

$d((\sigma\tau)(a), (\sigma\tau)(b))$

$= d[\sigma(\tau(a)), \sigma(\tau(b))]$

$= d(\tau(a), \tau(b))$

$\Rightarrow d(a, b)$

Thus,

σ, τ is also a symmetric further if σ is symmetry then distance of
$d(\sigma^{-1}(a), \sigma^{-1}(b)) = d[\sigma(\sigma^{-1}(a), \sigma(\sigma^{-1}(b))]$
so, σ^{-1} is also symmetry
clearly, the identity permutation is symmetry
hence, the set of symmetrices of 'S' form a group under composition of mapping

e.g :- 1) let, G be a group such that $a^2 = e$ $\forall a \in G$ show that 'G' is abelian

→ Given, G be a group

$G = \{ a \in G / a^2 = e \}$

let, $a, b \in G$ such that $a^2 = e, b^2 = e$
also,
$a \cdot b \in G$ ---- $\because$ closure property
$\Rightarrow (ab)^2 = e$
$= e \cdot e$
$= b^2 a^2$
$= (ba)^2$
$\Rightarrow ab = ba$

2) Let, G be a group such that $(ab)^2 = a^2 b^2$ $\forall a, b \in G$ show that 'G' is abelian

→ Given, G be a group
& $a, b \in G$

Page No.
Date

$G = \{a, b \mid (ab)^2 = a^2 b^2\}$

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

$abab = aabb$

now,

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

$\therefore$ left multiply by a^{-1} & ~~write~~ right multiply by b^{-1}

$\therefore \underline{a^{-1}a}\, b\, a\underline{b\, b^{-1}} = \underline{a^{-1}a}\, a\, b\underline{b\, b^{-1}}$

$e\, b\, a\, e = e\, a\, b\, e$

$\Rightarrow ba = ab$

$\therefore$ G is a abelian group.

* Order of a group:-

The no. of elements of a group is called its order. we will it is denoted by '$|G|$'

* Order of an element:-

The order of an element $a \in$ in a group G is a smallest +ve integer such that

$a^n = e$

then, n is said to be order of an element

(In additive group this would be $n a = 0$)

If no such integer exist we say that group has infinite order.

Order of an element 'a' is denoted by $|a|$

Scanned by CamScanner

Example:-

1) Find order of each element in Z_5 group under addition modulo 5 $(+_5)$

→ $(Z_5, +_5)$

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

$\bar{0} + \bar{0} = 0 \qquad \therefore |\bar{0}| = 1$

$\bar{1} + \bar{1} = \bar{2}$

$\bar{1} + \bar{1} + \bar{1} = \bar{3}$

$\bar{1} + \bar{1} + \bar{1} + \bar{1} + \bar{1} = \bar{5} = 0 \qquad \therefore |\bar{1}| = 5$

$\bar{2} + \bar{2} = \bar{4}$

$\bar{2} + \bar{2} + \bar{2} = \bar{6} = 1$

$\bar{2} + \bar{2} + \bar{2} + \bar{2} = \bar{8} = 3$

$\bar{2} + \bar{2} + \bar{2} + \bar{2} + \bar{2} = \overline{10} = 0 \qquad \therefore |\bar{2}| = 5.$

$\bar{3} + \bar{3} = \bar{6}$

$\bar{3} + \bar{3} + \bar{3} = \bar{9} = 4$

$\bar{3} + \bar{3} + \bar{3} + \bar{3} = \overline{12} = 2$

$\bar{3} + \bar{3} + \bar{3} + \bar{3} + \bar{3} = 15 = 0 \qquad \therefore |\bar{3}| = 5$

$\bar{4} + \bar{4} + \bar{4} + \bar{4} + \bar{4} = \overline{20} = 0 \qquad \therefore |\bar{4}| = 5$

2) Find order of each element in Z_7^* group under multipli-cation modulo 7 $(\times_7)$

→ $(Z_7^*; \times_7)$

$\therefore Z_7^* = \{1, 2, 3, 4, 5, 6\}$

$|\bar{1}| = (\bar{1})^1 = 1 \qquad \therefore |\bar{1}| = 1$

* Linear Group :-

1) General Linear Group ($GL(n, F)$) :-

let, $GL(n, F)$ be the set of '$n \times n$' invertible matrices over a field. then, $GL(n, F)$ is a group under multiplication i.e

$$GL(n, F) = \{ A \in GL(n, F) / |A| \neq 0 \}$$

eg

To show that $GL(2,R)$ is a group under multiplication

→ Given,

$$GL(2,R) = \{A \in GL(2,R) \,/\, |A| \neq 0\}$$

& order $n = 2$

1) Closure property

i) Let A & $B \in GL(2,R)$ such that

$$A = \begin{bmatrix} a & b \\ c & d \end{bmatrix}, \quad B = \begin{bmatrix} k & l \\ m & n \end{bmatrix}$$

& $|A| = ad - bc \neq 0$ & $|B| = kn - ml \neq 0$

$$\therefore A \cdot B = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \cdot \begin{bmatrix} k & l \\ m & n \end{bmatrix}$$

$$= \begin{bmatrix} ak+bm & al+bn \\ ck+dm & cl+dn \end{bmatrix} \in GL(2,R)$$

$$|AB| = [(ak+bm)(cl+dn) - (al+bn)(ck+dm)]$$

2) Associative property

Let $A, B, C \in GL(2,R)$ such that

$$A = \begin{bmatrix} a & b \\ c & d \end{bmatrix}, \quad B = \begin{bmatrix} k & l \\ m & n \end{bmatrix}, \quad C = \begin{bmatrix} w & x \\ y & z \end{bmatrix}$$

$$\therefore A \cdot (B \cdot C) = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \cdot \left(\begin{bmatrix} k & l \\ m & n \end{bmatrix} \cdot \begin{bmatrix} w & x \\ y & z \end{bmatrix} \right)$$

$$= \begin{bmatrix} a & b \\ c & d \end{bmatrix} \begin{bmatrix} kw+ly & kx+lz \\ mw+ny & mx+nz \end{bmatrix}$$

$$= \begin{bmatrix} a(kw+ly)+b(mw+ny) & a(kx+lz)+b(mx+nz) \\ c(kw+ly)+d(mw+ny) & c(kx+lz)+d(mx+nz) \end{bmatrix}$$

e.g

To show that $GL(2,R)$ is a group under multiplication

→ Here, $GL(2,R)$ is non empty

1) closure property

Let A & $B \in GL(2,R)$

Such that,

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

$|A| = a_1d_1 - c_1b_1 \neq 0$; $|B| = a_2d_2 - b_2c_2 \neq 0$

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

$$= \begin{bmatrix} a_1a_2 + b_1c_2 & a_1b_2 + b_1d_2 \\ c_1a_2 + d_1c_2 & c_1b_2 + d_1d_2 \end{bmatrix}$$

$$\therefore |A| = [(a_1a_2 + b_1c_2)(c_1b_2 + d_1d_2) - (a_1b_2 + b_1d_2)(c_1a_2 + d_1c_2)]$$

$$= a_1a_2c_1b_2 + a_1a_2d_1d_2 + b_1c_2c_1b_2 + \cancel{b_1c_2d_1d_2} - (\cancel{a_1b_2c_1a_2}) - (a_1b_2d_1c_2) - (b_1d_2c_1a_2) - (\cancel{b_1d_2d_1c_2})$$

$$= a_1d_1(a_2d_2 - b_2c_2) - b_1c_1(-c_2b_2 + b_1d_2)$$

$$= (a_2d_2 - b_2c_2)(a_1d_1 - b_1c_1) \neq 0$$

$\therefore |AB| \neq 0$ $\quad \therefore AB \in GL(2,R)$

$\therefore$ closure property hold.

Date

2) Associative property

let,

$A, B, C \in GL(2,R)$

such that

$$A = \begin{bmatrix} a_1 & b_1 \\ c_1 & d_1 \end{bmatrix}, \quad B = \begin{bmatrix} a_2 & b_2 \\ c_2 & d_2 \end{bmatrix}, \quad C = \begin{bmatrix} a_3 & b_3 \\ c_3 & d_3 \end{bmatrix}$$

& $|A| \neq 0, \ |B| \neq 0, \ |C| \neq 0$

Now,

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

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

$\therefore$ Associative property hold

3) Existance & identity

let $A \in GL(2,R)$ $\exists$ E such that

$A \cdot E = A$ $\qquad |A| \neq 0$

$\therefore \ |AE| = |A|$

$|A| \, |E| = |A|$

$$|E| = \frac{|A|}{|A|} = 1$$

$\therefore \ |E| = 1$

Scanned by CamScanner

$\exists\ E = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \in GL(2,R)$

4) Existance of inverse

let $A, B \in GL(2,R)$ & & $|A| \neq 0$, $B \neq 0$

$A \cdot B = E$

$|A \cdot B| = |E|$ ~~or~~ $A^{-1} A\ B = A^{-1} E$

$|A|\ |B| = |E|$ $\quad$ $E B = A^{-1}$

$|B| = \dfrac{|E|}{|A|}$ $\quad \Rightarrow B = A^{-1}$

$|B| = |E| \cdot |A^{-1}|$

$|B| = |A^{-1}|$

$B = A^{-1}$

2) To show that $GL(3,R)$ is group under multiplication sub. is $GL(2,R)$ is abelian

→ Here, $GL(3,R)$ is non empty

$GL(3,R) = \{ A \in GL(3,R) / |A| \neq 0 \}$

1) closure property

let, $A, B \in GL(3,R)$

i.e $|A| \neq 0$ & $|B| \neq 0$

now.

$|A \cdot B| = |A| . |B| \neq 0$

$\Rightarrow AB \in GL(3,R)$

Date

② Associative property

let

$A, B, C \in GL(3,R)$

i.e

$|A| \neq 0, \quad |B| \neq 0, \quad |C| \neq 0$

Now,

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

$= |A|\cdot|B|\cdot|C|$

$= |AB||C|$

$= |(AB)\cdot C|$

$\Rightarrow |A\cdot(BC)| = |(AB)\cdot C| \quad \in GL(3,R)$

3) Existance of identity

let $E \in GL(3,R)$

such that

$A\cdot E = A$

$|AE| = |A|$

$|A|\cdot|E| = |A|$

$|E| = \frac{|A|}{|A|} = 1, \quad \exists\ E = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$

4) Existance of inverse:-

$\exists\ B \in GL(3,R)$ such that

$A\cdot B = E$

$\therefore |AB| = |E| \qquad$ or $\qquad A\cdot A^{-1}B = A^{-1}E$

$E\cdot B = A^{-1}$

$B = A^{-1}$

$\therefore$ It holds all the conditions of group

$\therefore GL(3,R)$ is a group under multiplication.

Scanned by CamScanner

(5) Let. $A, B \in GL(2, R)$ where $|A| \neq 0$ & $|B| \neq 0$ such that

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

now,

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

$$= \begin{bmatrix} a_1a_2 + b_1c_2 & a_1b_2 + b_1d_2 \\ c_1a_2 + d_1c_2 & c_1b_2 + d_1d_2 \end{bmatrix}$$

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

$$= \begin{bmatrix} a_2a_1 + b_2c_1 & a_2b_1 + b_2d_1 \\ c_2a_1 + d_2c_1 & c_2b_1 + d_2d_1 \end{bmatrix}$$

$\Rightarrow A \cdot B \neq B A$

$\therefore GL(2, R)$ is not an abelian group

* Special Linear Group:-

Let $SL(n, R)$ is the set of $n \times n$ matrices over a field 'F' whose determinant is 1 then, $SL(n, F)$ is a special linear group under multiplication

Ex:- show that $SL(2, R)$ is a group under multiplication.

→ Here $SL(2,R) = \{ A \in SL(2,R) / |A| = 1 \}$

i) closure property

let $A, B \in SL(2,R)$ such that

$|A| = 1, \quad |B| = 1$

now, $|AB| = |A| \cdot |B|$

$= 1 \cdot 1$

$= 1$

$\therefore |AB| = 1 \quad \in SL(2,R)$

$\Rightarrow AB \in SL(2,R)$

2) Associative property

let, $A, B, C \in SL(2,R)$ such that

$|A| = 1, |B| = 1, |C| = 1$

now,

$|A \cdot (BC)| = |A| \cdot |BC|$

$= |A| |B| |C|$

$= 1 \cdot 1 \cdot 1$

$= 1$

$= 1 \cdot 1 \cdot 1$

$= |A| |B| |C|$

$= |AB| |C|$

$= |(AB) \cdot C|$

$\Rightarrow |A \cdot (BC)| = |(AB) \cdot C| \quad \in SL(2,R)$

$\Rightarrow A \cdot (BC) = (AB) \cdot C \quad \in SL(2,R)$

3) Existance of ~~inverse~~ identity

let $E \in SL(2,R)$

Scanned by CamScanner

such that

$AE = A$

$|AE| = |A|$

$|A|\,|E| = |A|$

$|E| = \frac{|A|}{|A|} = \frac{1}{1} = 1$

$\therefore E = I \implies E = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$

4) Existance of inverse

let $B \in SL(2,R)$

such that

$A \cdot B = E$ or $A \cdot B = E$

$A^{-1} A B = A^{-1} E$ $|AB| = |E|$

$E B = A^{-1}$ $|A|\,|B| = 1$

$B = A^{-1}$ $1 \cdot |B| = 1 \implies |B| = 1$

$\therefore$ St holds all the properties of group

$\therefore$ $SL(2,R)$ is a group.

H.W

2) To show that $SL(3,R)$ is abelian group under multipli-
-cation.

* $U(n)$ Group :-

$U(n)$ to be the set of all passitive integers less than 'n' and relatively prime to 'n' (i.e $\gcd(k,n) = 1$) then $U(n)$ is a group under multiplication modulo n ($\times_n$)

i.e. $U(n) = \{ k \,/\, k < n \text{ \& } \gcd(k,n) = 1 \}$

Scanned by CamScanner

Ex:-

1) To show that $U(15)$ is group under multiplication modulo 15 ($\times_{15}$)

→ $U(15) = \{K / K < 15 \ \& \ \gcd(K, 15) = 1\}$

$U(15) = \{1, 2, 4, 7, 8, 11, 13, 14\}$

$\times_{15}$	1	2	4	7	8	11	13	14
1	1	2	4	7	8	11	13	14
2	2	4	8	14	1	7	11	13
4	4	8	1	13	2	14	7	11
7	7	14	13	4	11	2	1	8
8	8	1	2	11	4	13	14	7
11	11	7	14	2	13	1	8	4
13	13	11	7	1	14	8	4	2
14	14	13	11	8	7	4	2	1

2) To show that $U(10)$, $U(12)$ & $U(5)$ is abelian group

* Note:-

1) $|U(n)|$ is $\phi(n)$ where, ϕ is Euler function

$U(10)$

→ $U(10) = \{K / K < 10 \ \& \ \gcd(K, 10) = 1\}$

$U(10) = \{1, 3, 7, 9\}$

$\times_{10}$	1	3	7	9
1	1	3	7	9
3	3	9	1	7
7	7	1	9	3
9	9	7	3	1

Direct Product Group :-

Let $G_1, G_2, \ldots, G_n$ be a family of groups then the cartetian product $G_1 \times G_2 \times \cdots \times G_n$ is a group under the pointwise binary operation defined by the cartation product

$G_1 \times G_2 \times G_3 \times \cdots \times G_n = \{(g_1 . g_2, \ldots g_n) / g_1 \in G_1, g_2 \in G_2, \ldots, g_n \in G_n$

such that

$(g_1, g_2, \ldots g_n)(g_1', g_2' \ldots g_n') = (g_1 . g_1', g_2 . g_2', \ldots g_n g_n')$

where, $g_i . g_i' \in G_i$

Ex:-

To show that $G_1 \times G_2$ is a group under the pointwise binary operation defined by

$G_1 \times G_2 = \{(g_1 . g_2) / g_1 \in G_1, g_2 \in G_2\}$

$(g_1 g_2)(g_1', g_2') = (g_1 g_1', g_2 g_2')$

where $g_i . g_i' \in G_i \quad 1 \leq i \leq n$

$G_1 \times G_2 = \{(g_1 . g_2) / g_1 \in G_1 \;\&\; g_2 \in G_2\}$

① closure property

let $(g_1 . g_2), (g_1' . g_2') \in G_1 \times G_2$

$\therefore (g_1, g_2)(g_1', g_2') = (g_1 . g_1', g_2 . g_2') \in G_1 \times G_2$

$\Rightarrow g_1 . g_1' \in G_1 \;\&\; g_2 . g_2' \in G_2$

Date

② Associative property.

let,

$(g_1, g_2), (g_1', g_2')$ & $(g_1'', g_2'') \in G_1 \times G_2$

$\therefore [(g_1, g_2)((g_1', g_2').(g_1'', g_2''))] = (g_1, g_2)(g_1' . g_1'', g_2' . g_2'')$

$= (g_1 g_1' g_1'', g_2 . g_2' g_2'')$

$= (g_1 g_1', g_2 . g_2')(g_1'', g_2'')$

$= [(g_1, g_2)(g_1', g_2')](g_1'', g_2'')$

$\Rightarrow (g_1, g_2)((g_1', g_2')(g_1'', g_2'')) = ((g_1, g_2)(g_1', g_2')).(g_1'', g_2'')$

③ Existance of identity

Let $a \in G_1 \times G_2$

$\exists$ e such that

$a . e = a$, $a = (g_1, g_2)$ & $e (e_1, e_2)$

~~$a = g_1$~~ but we know that G_1 & G_2 are two groups, by the property of $\exists$ of identity in G_1 & G_2

such that $\exists$ $e_1 \in G_1$ & $e_2 \in G_2$ ie

$g_1 e_1 = g_1 \forall g_1 \in G$ & $g_2 . e_2 = g_2$

$\therefore (g_1, g_2)(e_1, e_2) = (g_1 e_1, g_2 e_2)$

$= (g_1, g_2)$

$\exists$ $e = (e_1, e_2) \in G_1 \times G_2$ where $e_1 \in G_1$ & $e_2 \in G_2$.

(4) Existance of inverse

Let $a \in G_1 \times G_2$, $\exists$ b such that

$a \cdot b = (e_1, e_2) \Rightarrow (g_1, g_2) \cdot b = (e_1 . e_2)$

here, $g_1 \in G_1$ & $g_2 \in G_2$

where

g_1^{-1} & g_2^{-1} exist

$\therefore g_1^{-1} \in G_1$ & $g_2^{-1} \in G_2$

$\Rightarrow b = (g_1^{-1}, g_2^{-1})$

$\therefore a \cdot b = (e_1, e_2)$

$(g_1, g_2) \cdot b = (e_1, e_2)$

$b = (g_1^{-1}, g_2^{-1}) \in G_1 \times G_2$

& $g_1^{-1} \in G_1$ & $g_2^{-1} \in G_2$

$(g_1, g_2)(g_1^{-1}, g_2^{-1}) = (g_1 \cdot g_1^{-1}, g_2 \cdot g_2^{-1})$

$= (e_1, e_2)$

$\exists$ $b = (g_1^{-1}, g_2^{-1})$ is inverse of $a = (g_1, g_2)$

$\therefore$ It is a group

* Kein Four Group:-

The set $K_4 = \{ e, a, b, ab \,/\, a^2 = e, b^2 = e$ & $ab = ba \}$

is said to be kein four group.

i.e. K_4 group is abelian

Scanned by CamScanner

Date

* Quaternian Group:-

It is denoted by 'Q_8' i.e.

$$Q_8 = \{ \pm 1, \pm i, \pm j, \pm k \;/\; i\cdot j = k,\ j\cdot k = i \ \&\ k\cdot i = j,\ j\cdot i = -k,\ k\cdot j = -i \ \&\ i\cdot k = -j,\ i\cdot j = j\cdot k = k\cdot i = 1,\ \&\ ji = kj = ik = -1 \}$$

is a group under multiplication, it exist all the properties of groups and Q_8 is non-abelian group. because $i\cdot j \neq j\cdot i$

Ex:-

1) Prove that the matrices $\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}, \begin{bmatrix} -1 & 0 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix}$ form a multiplicative group.

→ let,

$$G = \left\{ \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}, \begin{bmatrix} -1 & 0 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix} \right\}$$

① closure property

let $A, B \in G$ such that

$$A = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \quad B = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$$

$$A\cdot B = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \cdot \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} = \begin{bmatrix} 1+0 & 0+0 \\ 0+0 & 0-1 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} \in G$$

$\therefore A\cdot B \in G$

Page No.
Date

(2) Associative property

Let $A, B, C \in G$ such that

$A = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$, $B = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$, $C = \begin{bmatrix} -1 & 0 \\ 0 & 1 \end{bmatrix}$

now

$$A(B \cdot C) = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \cdot \left(\begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} \begin{bmatrix} -1 & 0 \\ 0 & 1 \end{bmatrix} \right)$$

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

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

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

&

$$(A \cdot B) \cdot C = \left(\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} \right) \begin{bmatrix} -1 & 0 \\ 0 & 1 \end{bmatrix}$$

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

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

$\Rightarrow A(B \cdot C) = (A \cdot B) \cdot C \quad \in G$

Scanned by CamScanner

Date

③ ∃ of identity
Let $E \in G$ such that

$$A \cdot E = A$$

$$E = \frac{A}{A}$$

$$\Rightarrow E = I = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \in G$$

④ ∃ of inverse :
Let $B \in G$ such that

$$A \cdot B = E$$

$$A^{-1} \cdot A B = A^{-1} E$$

$$E \cdot B = A^{-1}$$

$$B = A^{-1} \Rightarrow B = \begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix} \in G$$

Page No.
Date

* Dihydral Group:-

The dihydral group $D_{(n)}$ is a group of order $2n$ generated by '2' element σ & τ satisfying

$$D_n = \{ e, \sigma, \sigma^2, \ldots, \sigma^{n-1}, \tau, \tau\sigma, \tau\sigma^2, \ldots, \tau\sigma^{n-1} \}$$

and $\sigma^n = e = \tau^2$

and $\tau\sigma = \sigma^{n-1} \cdot \tau$

where, $\sigma = (1, 2, 3, \ldots, n)$

& $\tau = \begin{pmatrix} 1 & 2 & 3 & \ldots & n-1 & n \\ 1 & n & n-1 & \ldots & 3 & 2 \end{pmatrix}$

Ex:- ① Find ~~the order of~~ 1^{st} D_3 & D_4 & find the order of each element in D_3 & D_4.

Page-69, Q.6
H.W ② Prove that the following matrices form a non-abelian group of order '8' under multiplication of matrices.

$$G = \left\{ \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} \sqrt{-1} & 0 \\ 0 & \sqrt{-1} \end{bmatrix}, \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}, \begin{bmatrix} 0 & \sqrt{-1} \\ \sqrt{-1} & 0 \end{bmatrix}, \right.$$

$$\left. \begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix}, \begin{bmatrix} -\sqrt{-1} & 0 \\ 0 & \sqrt{-1} \end{bmatrix}, \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}, \begin{bmatrix} 0 & -\sqrt{-1} \\ -\sqrt{-1} & 0 \end{bmatrix} \right\}$$

Further show that if $e = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$, $a = \begin{bmatrix} \sqrt{-1} & 0 \\ 0 & -\sqrt{-1} \end{bmatrix}$

& $b = \begin{bmatrix} 0 & -\sqrt{-1} \\ \sqrt{-1} & 0 \end{bmatrix}$

then,

$a = e$, $b^2 = a^2$ & $b^{-1}ab = a^3$

& What is this group

Scanned by CamScanner

* Subgroup:-

Let, $(G, \cdot)$ be a group and 'H' be a subset of 'G'. 'H' is called a subgroup of 'G' if H-itself a group w.r.t operation on 'G', it is written as

$$H < G$$

* Examples of subgroups:-

1) Let, Group $G = R$ under addition and we know that $Z \subseteq R$ and $Q \subseteq R$

now we show that, Z is a group under addition, simillarly we show that Q is a group under addition

(1) $\forall\ a, b \in Z$

$\Rightarrow a+b \in Z$

(2) $\forall\ a, b, c \in Z$

$\Rightarrow a+b = Z$

$\Rightarrow a+(b+c) = (a+b)+c$

(3) $\exists\ e$ such that

$a+e = a \Rightarrow a+0 = a$

(4) $\exists\ b$ such that

$a+b = 0$

$b = -a$

Date

$\therefore Z^+$ is a group & simillarly (Q^+) is a group

$\therefore (Z,+)$ is a subgroup of $(Z,+)$ & $(Q,+)$ is a subgroup of $(R,+)$

2) $R \subseteq C$ and 'C' is a group under addition and now we know that $(R,+)$ is group

$\therefore (R,+)$ is a sub group of $(C,+)$

3) $(Q^*,\cdot) \subseteq (R^*,\cdot) \Rightarrow (Q^*,\cdot)$ is a sub group of $(R^*,\cdot)$.

4) $(R^*,\cdot) \subseteq (C^*,\cdot) \Rightarrow (R^*,\cdot)$ is a sub group of $(C^*,\cdot)$

5) We know that $GL(n,F)$ & $SL(n,F)$ are General Linear group & special linear group under matrix multiplication.

i.e. $GL(n,F) = \{A / |A| \neq 0\}$ & $SL(n,F) = \{A / |A| = 1\}$

therefore

All matrices ~~are~~ ~~contain~~ in $SL(n,F)$ are contain in $GL(n,F)$

$\therefore SL(n,F) \subseteq GL(n,F)$

But

we know that, $GL(n,F)$ & $SL(n,F)$ are groups under matrix multiplication

$\therefore$ By definition of subgroup

$SL(n,F) < GL(n,F)$

theo

Pro

* Note:-

1) Every Group is subgroup with itself.

2) Take only identity element in any group G under operation on 'G' is subgroup.

* Proper Subgroup:-

A subgroup is said to proper if $H \neq \{e\}$ & $H \neq G$ i.e H is a proper subgroup of G

e.g.:- $SL(n,F)$ is a proper subgroup of $GL(n,F)$

theorem:- A semigroup 'G' is a group iff for all $a,b \in G$ each of the equation

$ax=b$ & $ya=b$ has a solution.

Proof:- Consider G is a group then, a & $b \in G$ then $\exists$ inverses of a & b i.e. a^{-1} & b^{-1} now consider,

$ax=b$ & $ya=b$ we have

$$ax=b$$
$$a^{-1}ax=a^{-1}b$$
$$ex=a^{-1}b$$
$$x=a^{-1}b$$

&

$$ya=b.$$
$$yaa^{-1}=ba^{-1}$$
$$ye=ba^{-1}$$
$$y=ba^{-1}$$

$\Rightarrow x=a^{-1}b$ & $y=ba^{-1}$ respectively

$\therefore$ $ax = b$ & $ya = b$ has a solution

now,

conversely suppose that $ax = b$ & $ya = b$ has a solution.

let, G be a semi group

i.e.

G satisfies closure property

i.e.

$\forall a, b \in G \Rightarrow ab \in G$

& $\forall a, b, c \in G \Rightarrow [a \cdot (b \cdot c)] = [(a \cdot b) c]$

let.

$a \in G$ then, in a particular case $ya = a$ has a solution

$\Rightarrow y = e$

so that,

$\forall a \in G \Rightarrow e \cdot a = a$

now,

for any 'b' in G the equation

$ax = b$ has a solution say $x = x_0$

i.e

$ax_0 = b$

$\therefore$ $eb = e a x_0$

$= a x_0$

$= b$

hence,

'e' is left identity further for every $a \in G$ the equation $ya = e$ has a solution

hence,

$ya = e$

$y = e/a$

Date

$\Rightarrow y = ea^{-1}$

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

$\therefore$ a has inverse ie a^{-1}

$\therefore$ G is a group.

Theorem:- A finite semi group. G is a group iff the cancellation laws holds for all elements in G i.e $ab = ac \Rightarrow b = c$ & $ba = ca \Rightarrow b = c \ \forall \ a, b, c \in G$

Proof:- Consider G is a group and $a, b \in G$ then, show that,

$ab = ac \Rightarrow b = c$

& $ba = ca \Rightarrow b = c$

now, taking

$ab = ac \quad \forall \ a, b, c \in G$

$\Rightarrow a^{-1}ab = a^{-1}ac$ -- multiply a^{-1} on left side on both side

$\Rightarrow eb = ec$

$\Rightarrow b = c$

& $ba = ca$

$\Rightarrow baa^{-1} = caa^{-1}$ multiply a^{-1} on right side on both side

$\Rightarrow be = ce$

$\Rightarrow b = c$

conversely, suppose that

Let G be a finite semi group & suppose that the cancellation laws hold

Scanned by CamScanner

Page No.
Date

we can prove that
$\forall a, b \in G$ the eq^n
$ax = b$
& $ya = b$ has a solution
and,
$\therefore$ by ~~above grow the~~ a semi group G is group
iff $\forall a, b \in G$ then
$ax = b$ & $ya = b$ has solution

$\therefore$ G is a group

Eg:- 1) If G is a group such that
$(ab)^n = a^n b^n$ for 3 conjugative integees then show that
$ab = ba$

$\rightarrow$ let G be a group such that $(ab)^n = a^n b^n$
for 3 conjugative integer
we consider,
$n, n+1, n+2$ three conjugative integer such that

$(ab)^n = a^n \cdot b^n$ ——— ①
$(ab)^{n+1} = a^{n+1} \cdot b^{n+1}$ ——— ②
$(ab)^{n+2} = a^{n+2} \, b^{n+2}$ ——— ③

from eq^n ① & ② we get
$(a^n b^n)(ab) = (ab)^{n+1}$
$= a^{n+1} \cdot b^{n+1}$

$\Rightarrow$ by appropriate cancellation
$b^n a = a b^n$

similarly, from eq^n (2) & (3) we get

$b^{n+1} \cdot a = a\, b^{n+1}$

but, we give $b^{n+1} \cdot a = b(b^n \cdot a)$

$= b(a\, b^n)$

$= (ab)b^n$

so,

$a\, b^{n+1} = b\, a\, b^n$

this gives

$b(a\, b^n) = b\, a\, b^n$

$\Rightarrow ab\cancel{b^n} = ba\cancel{b^n}$

by cancellation law

$\Rightarrow ab = ba$

Theorem:- Let 'G' be a group a non-empty subset H of G is a subgroup of G. if and only if either of the following hold

its for all.

1) $\forall\ a, b \in H$

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

$\forall\ a, b \in H$

$\Longrightarrow a b^{-1} \in H$

Proof:- Let 'G' be a group & H is a non-empty subset of G.

Now, we suppose that H is a subgroup

'H' it self group.

$\therefore$ for all $a, b \in H$

$\Longrightarrow a, b \in H$ $\qquad \because$ H is group

& H satisfied closure

since,

we have,

(1) $a \in H$ then,

$\exists\ a^{-1} \in H$ -- $\because$ H is group

(2) ~~or~~ for $b \in H$ by the property of inverse

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

& we know that

$\therefore ab^{-1} \in H$ --- by closure property

conversely,

suppose that

(1) $\forall\ a, b \in H$ & $a^{-1} \in H$

(2) $\forall\ a, b \in H$ & $ab^{-1} \in H$

by the (I) property closure property hold &
associative property hold

Now,

for any $a \in H$. a^{-1} also $\in H$

then by ~~pr~~ second property

$$aa^{-1} \in H \qquad -- \ aa^{-1} = e$$

$$e \in H$$

$\Rightarrow$ existance of identity hold

& $\exists$ of inverse hold

$\therefore$ H itself group under operation of G

$\therefore$ H is a subgroup

Q:- Let H & K are subgroup of G then show that $H \cap K$ is subgroup of G.

→ We know that:

H & K are subgroup of G

that is H & K itself group

∴ by the existance of identity

$e \in H$ & $e \in K$

$\Rightarrow e \in H \cap K$

∴ $H \cap K$ is non empty

we know that.

$H \subseteq G$ & $K \subseteq G$

$\Rightarrow H \cap K \subseteq G$

$\forall$ $a, b \in H \cap K$

$\Rightarrow a, b \in H$ & $a, b \in K$

$\Rightarrow ab \in H$ & $ab \in K$

$\Rightarrow ab \in H \cap K$ ---- ∵ K & H are subgroups

Now, consider

$a \in H \cap K$

$\Rightarrow a \in H$ & $a \in K$

$\rightarrow a^{-1} \in H$ & $a^{-1} \in K$

$\Rightarrow a^{-1} \in H \cap K$

$\forall$ $a, b \in H \cap K$

$\rightarrow a, b \in H$ & $a, b \in K$

$\Rightarrow ab \in H$, $ab \in K$

hence $H \cap K$ is subgroup of G.

Scanned by CamScanner

Page No. | Date

* Note:-

let A & B be the subset of group G.

$\therefore$

$AB = \{ xy \,/\, x \in A,\ y \in B \}$

$A+B = \{ x+y \,/\, x \in A,\ y \in B \}$

Theorem:- Let H & K be a subgroup of G.
and $H \cup K$ is subgroup iff $H \subseteq K$ or $K \subseteq H$.

Proof:- let,

H & K be subgroup of G

now,

suppose that H containing K or K containing H

$\therefore H \cup K \subseteq K \cup K = K$

or $K \cup H \subseteq H \cup H = H$

but we know that

H & K are subgroup of G

$\therefore$ $H \cup K$ is also subgroup of G

Now,

conversely, suppose that

$H \cup K$ is subgroup

to show that H containing K or K containing H

contrary assume that

neither $H \subseteq K$ nor $K \subseteq H$ then

$\exists$ element $a \in H - K$

$\Rightarrow a \in H$ & $a \notin K$

and,

$b \in K - H$

$\Rightarrow b \in K$ & $b \notin H$ $\quad \Bigg\} - (1)$

Scanned by CamScanner

Now,

$a, b \in H \cup K$

$\Rightarrow ab \; H \cup K$

$\Rightarrow ab \in H$ or $ab \in K$

$\Rightarrow a, b \in H$ or $a, b \in K$ $\quad \because H \; \& \; K$ are subgroups

which is contradiction to $b \notin H$ & $a \notin K$

$\therefore$ our assumption is wrong

$\therefore$ either $H \subseteq K$ or $K \subseteq H$

ex:- Let G be a group and H is a subgroup ~~show~~ of G show that

$\forall x \in G$, $x^{-1} H x$ is a subgroup of G

$\rightarrow$ ~~Given~~, Let,

G is a group

& H is a subgroup of G $\quad (H < G)$

$\forall x \in G$ $\quad$, $x^{-1} \in G$

now consider a set $K = \{ x a x^{-1} / x \in G, a \in H \}$

now,

consider $a_1, b_1 \in K$ such that

$a_1 = x a x^{-1}$, $b_1 = x b x^{-1}$ $\quad \forall a, b \in H$

$\Rightarrow a_1 b_1 = x a x^{-1} x b x^{-1}$

$= x a b x^{-1}$ $\quad (\because x^{-1} x = e, \because x \in G \; \& \; G$ is group$)$

$\Rightarrow$ ~~ab~~ $= x ab x^{-1}$, $ab \in H$ $\quad -- (\because H < G)$

$\Rightarrow a_1 b_1 = x ab x^{-1} \in K$

$\Rightarrow a_1 b_1 \in K$

Now,

$$a_1^{-1} = (xax^{-1})^{-1}$$
$$= x^{-1}a(x^{-1})^{-1}$$
$$a_1^{-1} = x^{-1}ax \in K \quad \text{-- } (\because a^{-1} \in H, \because H \text{ is subgroup of } G)$$

Now, consider

$a_1, b_1 \in K$

$$a_1 b_1^{-1} = (xax^{-1})(xbx^{-1})^{-1}$$
$$= xax^{-1}(x^{-1})^{-1}b^{-1}x^{-1}$$
$$= xax^{-1}xb^{-1}x^{-1}$$
$$= xab^{-1}x^{-1} \quad \text{-- } (\because xx^{-1} = e)$$

$$a_1 b_1^{-1} = xab^{-1}x^{-1} \in K, \quad ab^{-1} \in H \ (\because H \subset G)$$

$\therefore K$ is a subgroup of G

i.e. xHx^{-1} is a subgroup of G

Theorem:- Let, H & K be subgroup of group G then. HK is subgroup of G iff $HK = KH$

Proof:- let H & K be a subgroup of group G

$\Rightarrow H < G, \ K < G$

suppose that,

$HK = KH$ to show that HK is subgroup of G.

We know that

H & K are subgroup of G i.e. itself group under operation of G

$\therefore e \in H$ & $e \in K$ — ($\because$ identity exist in group H & K)

$\therefore\ e = e \cdot e \in HK$

now,

define $HK = \{xy \mid x \in H,\ y \in K\}$

now consider,

$a_1, b_1 \in HK$

i.e. $a_1 = x_1 y_1$ $\quad b_1 = x_2 y_2 \in HK$

① $a_1 b_1 = x_1 y_1 x_2 y_2$ $\quad x_1 \in H,\ y_1 \in K$ & $x_2 \in H,\ y_2 \in K$

$= x_1 x_3 y_2$ $\quad x_3 = y_1 x_2 \in KH = HK$

$\Rightarrow x_1 x_3 y_2 \in HK$

$\therefore a_1 b_1 \in HK$

now,

$a_1^{-1} = (x_1 \cdot y_1)^{-1}$ $\quad x_1 \in H$ & $y_1 \in K$

$= y_1^{-1} \cdot x_1^{-1}$ $\quad$ ~~$x_1^{-1} \in H$ & $y_1^{-1} \in K$~~

$\therefore\ x_1^{-1} \in H$ & $y^{-1} \in K$

$\Rightarrow y^{-1} \cdot x^{-1} \in KH = HK$

$\therefore\ a_1^{-1} \in HK$

Now,

~~② $(a_1 \cdot b_1)^{-1} = a_1^{-1} \cdot b_1^{-1}$~~

~~$= (x_1 y_1)^{-1} \cdot (x_2 y_2)^{-1}$~~

~~$= x_1^{-1} \cdot y_1^{-1} \cdot x_2^{-1} \cdot y_2^{-1}$~~

② $a_1 b_1^{-1} = (x_1 y_2)(x_2 y_2)^{-1}$

$= x_1 y_1 x_2^{-1} y_2^{-1}$

$= x_1 y_1 y_2^{-1} x_2^{-1} \in HK$

$\therefore a_1 b^{-1} \in HK$

$\therefore$ HK is a subgroup of 'G'

Conversely, suppose that

HK is a subgroup of 'G'

to show that, $HK = KH$

Now consider.

$a_1 \in HK$

we know that,

$a_1^{-1} \in HK$ -- ($\because$ HK is a subgroup of G)

i.e.

$a_1^{-1} = x_1 y_1$, $x_1 \in H$ & $y_1 \in K$

$(a_1^{-1})^{-1} = (x_1 y_1)^{-1} = y^{-1} \cdot x^{-1} \in KH$

$\Rightarrow a_1 \in KH$

$\therefore HK \subseteq KH$ —— (1)

simillarly.

$b_1 \in KH$

we know that,

$b_1^{-1} \in KH$ -- ($\because$ KH is a subgroup of G)

i.e.

$b_1^{-1} = x_2 y_2$, $x_2 \in K$, $y_2 \in H$

$(b_1^{-1})^{-1} = (x_2 y_2)^{-1}$

$= y_2^{-1} \cdot x_2^{-1}$, $y_2^{-1} \in H$, $x_2^{-1} \in K$

$\Rightarrow y_2^{-1} \cdot x_2^{-1} \in HK$

$\Rightarrow b_1 \in HK$

$\therefore KH \subseteq HK$ —— (2)

by eqn (1) & (2)

$HK \subseteq KH$ & $KH \subseteq HK$

$\therefore HK = KH$

Date

Theorem:- let G be a group and $a \in G$

i) If $a^n = e$ for some $n \neq 0$ then $o(a)/n$

ii) If $o(a) = m$ then $\forall$ integer 'I', $a^i = a^{ei}$ where 'ei' is the remender of I modulo m

iii) $[a]$ is of order m iff $o(a) = m$

Proof:- Suppose.

let G be a group & $a \in G$

i) s/s $a^n = e$ then,

$$(a^n)^{-1} = e^{-1} = e$$

$$\Rightarrow a^{-n} = e$$

hence,

$$a^i = e \quad \text{for same } i > 0$$

$\therefore$ by the well ordering principal there is least possitive intege $m = o(a)$ such that

$$a^m = e$$

by the division algorithim

$$n = mq + r \qquad 0 \leq r \leq m \quad \text{--- (1)}$$

~~where~~ hence,

$$a^n = a^{mq+r}$$

$$\Rightarrow e = (a^m)^q \cdot a^r$$

$$\Rightarrow e = (e)^q \cdot a^r$$

$$\Rightarrow e = e \cdot a^r$$

$$\Rightarrow a^r = e$$

$$\therefore a^r = a^0$$

$$\Rightarrow r = 0$$

$\therefore$ eq^n (1) becomes

$$n = mq + 0$$

$$\therefore n = mq$$

$$\Rightarrow m / n$$

but $m = o(a)$

$$\Rightarrow \therefore o(a)/n$$

ii) Suppose $o(a) = m$

again by division althorithum for any $i \in Z$ such that

$$i = mq + r \quad , \; 0 \le r < m$$

$$\Rightarrow a^i = a^{mq+r}$$

$$= a^{mq} \cdot a^r$$

$$= (a^m)^q \cdot a^r$$

$$= e^q \cdot a^r$$

$$\Rightarrow a^i = e \cdot a^r$$

$$\Rightarrow a^i = a^r$$

$$\Rightarrow r = r(i)$$

where $r(i)$ is a remender i modulo m

$$\Rightarrow a^i = a^{r(i)}$$

iii) Let $o(a) = m$ then, i.e. $a^m = e$

hence,

$$\{ e, a, a^2, a^3, \ldots, a^{m-1} \}$$

are distinct

for otherwise $a^i = a^j$ for some i, j

where, $0 \leq i, j < m-1$

hence,

$$a^{i-j} = e \quad \Rightarrow o(a) = i-j$$

which is a contradiction to $o(a) = m$

let, now,

$H = [a]$ be a cyclic subgroup generated by 'a' for any $i \in Z$

$$\therefore \quad a^i = a^{r(i)}$$

$\Rightarrow$ H has exactly m elements which are $\{e, a, a^2, \dots a^{m-1}\}$

~~note~~,

$$\Rightarrow o([a]) = m$$

Conversely suppose that.

$o([a])$ is m then a^i's are not distinct for $i \in Z$

hence,

$$\Rightarrow a^i = a^j$$

for some $i, j \in Z$

when, $i < j$. then

$$\Rightarrow a^{j-i} = e$$

hence,

'a' is of a finite order say "$j-i = m$"

$$\therefore \quad a^m = e$$

$$\Rightarrow o(a) = m$$

* Let, H be a subgroup of G. given $a \in G$, the set

$aH = \{ah / h \in H\}$

is called the left coset of H determined by a,

and,

$Ha = \{ha / h \in H\}$

is called ~~ω~~ right coset of H determined by a.

* Note:-

1) A subset ~~(g)~~ $C(G)$ is called left coset of H in G if

$C = aH$ for some $a \in G$

and

The set of all left coset of H in G is written as

$\frac{G}{H} = \{ah / h \in H\}$

* Let 'H' be a subgroup 'G', the cardinal number of the set of left (right) cosets of H in 'G' is called the index of 'H' in 'G'

and it is denoted by

$[G : H] = \left|\frac{G}{H}\right|$

* Homomorphism :-

Let, G, H be groups a mapping some $\phi : G \to H$ is called homomorphism if $\forall\, x, y \in G$

such that,

$$\phi(x \cdot y) = \phi(x) \cdot \phi(y)$$

Ex:- 1) Let, G & H be groups and let, e' be the identity of H. the mapping $\theta : G \to H$ defined by $\theta(x) = e'$ $\forall$ $x \in G$

to show that it is a homomorphism

$\rightarrow$ Given,

G & H be groups & "e'" is a identity of H

if $\forall$ $x, y \in G$, i.e. $\theta(x) = e'$, $\theta(y) = e'$

$\Rightarrow xy \in G$

$\therefore \theta(xy) = e'$

$= e' \cdot e'$

$= \theta(x) \cdot \theta(y)$

$\Rightarrow \theta(xy) = \theta(x) \cdot \theta(y)$

2) For any group G the identity mapping ~~$\circledS$~~ $i : G \to G$ define by $i(x) = x$ to show that it is homomorphism

$\rightarrow$ Given, G is a group & $i : G \to G$

i.e. $i(x) = x$

by G is a group.

$\forall$ $x, y \in G$, $i(x) = x$, $i(y) = y$

$\Rightarrow$ ~~$\circledS$~~ $x \cdot y \in G$

$\therefore i(x \cdot y) = xy$

$= x \cdot y$

$\Rightarrow i(x \cdot y) = i(x) \cdot i(y)$ //

Date

3) Let G be a group $G(R^+, \cdot)$, o & a passitive real no. under multiplication and let 'H' be a additive group 'R'. the mapping $\phi : R^+ \longrightarrow R$ defined by

$$\phi(x) = \log x$$

to show that $\phi : R^+ \longrightarrow R$ is homomorphism.

→ Given, G is a group $(R^+, \cdot)$
& H is a additive group 'R'

the mapping $\phi : R^+ \longrightarrow R$ is defined by

$$\phi(x) = \log x$$

if G is a group.
$\forall$ $x, y \in G = R^+$ such that $\phi(x) = \log x$, $\phi(y) = \log y$

$xy \in G = R^+$

$\therefore \phi(xy) = \cancel{(\log x)}\ \cancel{(\log y)}\ \log(x \cdot y)$

$= \cancel{\log(x+y)} = \log x + \log(y)$

$= \quad = \phi(x) + \phi(y)$

$\Longrightarrow \phi(xy) = \phi(x) + \phi(y)$

$\therefore$ This mapping is homomorphism.

4) Let G be a group for a given $a \in G$ consider the mapping

$I_a : G \to G$ given by

$I_a(x) = axa^{-1} \quad \forall x \in G$

to show that ϕ is homomorphism under multiplication on G

→ Given,

G is a group

& $a \in G$ such that $I_a : G \to G$

$I_a(x) = axa^{-1} \quad \forall x \in G$

when G is a group

$\forall$ ~~a.b~~ $x, y \in G$ such that

$I_a(x) = axa^{-1}$, $I_a(y) = byb^{-1}$

~~⇒ a.b ∈ G~~

~~⇒ $I_{(ab)}(x) = abxa^{-1}b^{-1}$~~

~~= a~~

$\Rightarrow xy \in G$

$\Rightarrow I_{(a)}(xy) = \cancel{axa^{-1}aya^{-1}} = axya^{-1}$

$= \cancel{axeya^{-1}} = axeya^{-1}$

$= \cancel{axya^{-1}} = \underline{axa^{-1}}\,\underline{aya^{-1}}$

$= \quad = I_a(x) \cdot I_a(b)$

$\rightarrow I_a(xy) = I_a(x) \cdot I_a(y)$

Page No.
Date

5) Prove that a group Z under addition & Z_n under addition modulo n, then the function
$$\phi : Z \rightarrow Z_n$$
given by
$$\phi(x) = \overline{x} \quad \forall\ x \in Z$$

6) The mapping $f : G \rightarrow G$ given by $f(x) = x^2$ is homomorphism if $(xy)^2 = x^2y^2$.

5) $\longrightarrow$

$\rightarrow$ Z is a group under addition
& Z_n is a group under addition modulo n
& the function
$$\phi : Z \rightarrow Z_n$$
given by
$$\phi(x) = \overline{x} \quad \forall\ x \in Z$$

Z is a group
let $x, y \in Z$ $\qquad$ $\phi(x) = \overline{x}$ & $\phi(y) = \overline{y}$
$x+y \in Z$

$$\phi(x+y) = \overline{x+y}$$
$$= \overline{x} + \overline{y}$$
$$= \phi(x) + \phi(y)$$

$$\Longrightarrow \phi(x+y) = \phi(x) + \phi(y)$$

Scanned by CamScanner

Date

6) —— §

→ The mapping $f: G \to G$ given by $f(x) = x^2$

$\Rightarrow$ G is a group

$\forall\ x, y \in G$ such that

$$f(x) = x^2,\quad f(y) = y^2$$

$\therefore\ xy \in G$

$$\therefore f(xy) = (xy)^2$$
$$= x^2 y^2$$
$$= f(x) \cdot f(y)$$

$$\Rightarrow f(xy) = f(x) \cdot f(y)$$

Def[n] * If ϕ is bijective then ϕ is called an isomorphism of G onto H if ϕ is homomorphism
we written as $G \cong H$

Ex:- 1) Let $\phi: G \to G$ define by $\phi(x) = x$ $\forall\ x \in G$ to show that ϕ is isomorphic image.

→ Given $\phi: G \to G$ define by $\phi(x) = x$ $\forall\ x \in G$

① ϕ is one-one

let, $\phi(x) = \phi(y)$

$\Rightarrow x = y$

② ϕ is onto

let $y \in G$ in codomain

$y = \phi(x)$ $\forall\ x \in G$

(3) Given G is group

let $x, y \in G$ such that $\phi(x) = x$, $\phi(y) = y$

$\Rightarrow xy \in G$

$\phi(xy) = xy$

$= \phi(x) \cdot \phi(y)$

Def^n :- If ϕ is just one-one i.e. injective then we say that ϕ is an monomorphism if ϕ is homomorphism

Def^n Epimorphism :-

If ϕ is ~~subj~~ surjective & homomorphism then the mapping called as Epimorphism

Def^n Automorphism :-

A homomorphism of G into itself is isomorphism then the mapping is called an automorphism of G.

Def^n :- Let G & H be a groups and let $\phi : G \to H$ be a homomorphism, the kernel of ϕ is define to be the set

$$\ker \phi = \{ x \in G / \phi(x) = e' \}$$

Scanned by CamScanner

Page No.
Date

Theorem:- Let, G & H be groups with identities e & e' respectively and let $\phi: G \to H$ be a homomorphism. Then,

1. $\phi(e) = e'$
2. $\phi(x^{-1}) = [\phi(x)]^{-1}$ for each $x \in G$

Proof:- Let, G & H be groups and e & e' be the identity in G & H respectively

(1) Now,

$$\phi(e) \cdot \phi(e) = \phi(e \cdot e)$$
$$= \phi(e)$$
$$\cancel{\phi(e) \cdot \phi(e) = e'}$$
$$\phi(e) \cdot \phi(e) = e' \cdot \phi(e) \quad \text{---} \quad (e \cdot \phi(x) = \phi(x))$$

by right cancelation law

$$\phi(e) = e'$$

(2) let,

$$\phi(e) = e'$$
i.e. $e' = \phi(x \cdot x^{-1})$
$$= \phi(x) \cdot \phi(x^{-1}) \quad \text{--} \; (\because \phi \text{ is homomorphism})$$
$$e' = \phi(x) \cdot \phi(x^{-1})$$

multiplying $[\phi(x)]^{-1}$ in both sid-

$$\cancel{e' [\phi(x)]^{-1} = \phi(x^{-1})}$$
$$\cancel{\Rightarrow [\phi(x)]^{-1} = \phi(x^{-1})}$$

$$\Rightarrow [\phi(x)]^{-1} \cdot e' = [\phi(x)]^{-1} \cdot \phi(x) \cdot \phi(x^{-1})$$

$$\Rightarrow [\phi(x)]^{-1} = e' \cdot \phi(x^{-1})$$
$(\because \phi(x) \in H, [\phi(x)]^{-1}$ i.e. $\phi(x)[\phi(x)]^{-1} = e')$

$$\Rightarrow [\phi(x)]^{-1} = \phi(x^{-1})$$

Theorem:- A homomorphism $\phi: G \to H$ is injective iff Kernel of $\phi = \{e\}$

Proof:- Given,

Let, A homomorphism $\phi: G \to H$ is injective

suppose,

ϕ is injective and let, $x \in \ker.\phi$

i.e. $\phi(x) = e'$

where, e' is an identity in H

we know that,

$\phi(e) = e'$

so,

$\phi(x) = \phi(e)$

$\Rightarrow x = e$ $\quad \because \phi$ is one-one

i.e $e \in \ker.\phi$

$\therefore \ker.\phi = \{e\}$

Conversely suppose that

$\ker.\phi = \{e\}$ then show that ϕ is one-one or i.e. injective

Consider

$\phi(x) = \phi(y)$

multiplying $[\phi(y)]^{-1}$ on both side

$\therefore \phi(x).[\phi(y)]^{-1} = \phi(y)[\phi(y)]^{-1}$

$\phi(x).[\phi(y)]^{-1} = e'$

Page No.
Date

but we know that
$$\phi(x^{-1}) = [\phi(x)]^{-1}$$

$\therefore \phi(x) \cdot \phi(y^{-1}) = e'$

$\Rightarrow \phi(xy^{-1}) = e'$ -- ($\because \phi$ is homomorphism)

$\Rightarrow x \cdot y^{-1} \in \ker\phi = \{e\}$

$\Rightarrow x \cdot y^{-1} = e$

multiplying to right hand side by y

$\therefore x \cdot y^{-1} \cdot y = ey$

$\Rightarrow x \cdot e = y$

$\Rightarrow x = y$

theorem:- Let $\phi: G \to H$ be a homomorphism of a groups then, $\ker.\phi$ is a subgroup of G and image of ϕ ($Im.\phi$) is a subgroup of H

Proof:- Let, $\phi: G \to H$ be a homomorphism of groups

i.e. G is a group

& H is a group

and,

e & e' are identity in G & H respectively

Now,

To show that,

$\ker.\phi$ is non-empty.

let

$e \in G$ ... ($\because G$ is a group.)

$\Rightarrow \phi(e) = e'$

$\therefore e \in \ker.\phi$

Date

$\therefore$ Ker. ϕ is non empty.

To show that,

$a \cdot b \in Ker\, \phi$, $a^{-1} \in Ker.\, \phi$ & $a \cdot b^{-1} \in Ker.\, \phi$

let,

$a, b \in Ker.\, \phi$

i.e. we know that

$Ker.\phi = \{a \in G \mid \phi(a) = e'\}$

$\Rightarrow \phi(a) = e'$ & $\phi(b) = e'$ $\forall\ a, b \in G$

so,

$\phi(ab) = \phi(a) \cdot \phi(b)$ $\quad$ --- ($\because \phi$ is homomorphism)

$= e' \cdot e'$

$\phi(ab) = e'$ $\quad \forall\ ab \in G$

$\Rightarrow ab \in Ker.\, \phi$

consider,

$a \in Ker.\phi$

i.e $\phi(a) = e'$ $\quad \forall\ a \in G$

$\phi(a^{-1}) = [\phi(a)]^{-1}$ $\quad$ --- ($\because$ by previous theorem)

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

$= e'$ $\quad \forall\ a^{-1} \in G$

$\phi(a^{-1}) = e'$ $\quad \forall\ a^{-1} \in G$

$\Rightarrow a^{-1} \in Ker.\, \phi$

Page No | Date

Now,

let, $a\ b \in$ Ker. ϕ

i.e. $\phi(a) = e'$, $\phi(b) = e'$ $\forall\ a, b \in G$

so,

$\phi(ab^{-1}) = \phi(a) \cdot \phi(b^{-1})$ ... ($\because \phi$ is homomorphism)

$= \phi(a) \cdot [\phi(b)]^{-1}$

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

$= e' \cdot e'$

$\phi(ab^{-1}) = e'$ $\forall\ a, b^{-1} \in G$ ($\because G$ is group)

$\Rightarrow ab^{-1} \in$ Ker. ϕ.

$\therefore$ Ker. ϕ is subgroup of G

* Note:- We have Im. $\phi = \{x \in G / \phi(x)\}$

(2) Suppose that.

Im. $\phi = \{x \in G / \phi(x)\}$

Now,

To show that Im. ϕ is nonempty

let. $e \in G$ because G is a group

$\therefore \phi(e) = e'$

$\therefore$ Im. $\phi = \{e \in G / \phi(e) = e'\}$ i.e. $e' \in$ Im. ϕ

$\therefore$ Im. ϕ is non empty

(a) let, α & $\beta \in$ Im. ϕ

i.e. $\alpha = \phi(x)$, $\beta = \phi(y)$. $x, y \in G$

$\alpha \cdot \beta = \phi(x) \cdot \phi(y)$

$= \phi(xy)$ $xy \in G$ ($\because \phi$ is homomorphism)

$\Rightarrow \alpha\beta \in$ Im. ϕ.

Scanned by CamScanner

Date

so,

$\alpha \in Im.\phi$

$\alpha = \phi(a)$ $\qquad$ $x \in G$

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

$= \phi(x^{-1})$ $\qquad$. $x^{-1} \in G$

(b) $\alpha, \beta \in Im.\phi$.

$\alpha = \phi(x)$ $\quad$ $\beta = \phi(y)$ $\qquad$ $x, y \in G$

$\alpha \cdot \beta^{-1} = \phi(x) \cdot [\phi(y)]^{-1}$

$= \phi(x) \cdot \phi(y^{-1})$

$= \phi(x \cdot y^{-1})$ $\quad$. - ($\because$ ϕ is homomorphism)

$\Rightarrow \alpha \cdot \beta^{-1} = \phi(x \cdot y^{-1})$ $\qquad$ $\forall\ xy^{-1} \in G$

$\Rightarrow \alpha \cdot \beta^{-1} \in Im.\phi$.

$\therefore$ $Im.\phi$ is a subgroup H

Defn:- The centre of a group G written as $Z(G)$ is the set of those elements in G that commute with every element in G

i.e. $Z(G) = \{ a \in G \mid ax = xa \ \forall x \in G \}$

Scanned by CamScanner

Theorem:- The centre of group 'G' i.e. $Z(G)$ is subgroup of G.

Proof:- Let,

G be a group and centre of group 'G' denoted by

$$Z(G)$$

i.e.

$$Z(G) = \{ a \in G \mid ax = xa \quad \forall x \in G \}$$

since,

$e \in G$ i.e. $ex = x = xe \quad \forall x \in G$

i.e.

$e \in Z(G)$

$\therefore$ $Z(G)$ is nonempty set.

let,

$a, b \in Z(G)$

i.e. $ax = xa$ & $bx = xb \quad \forall x \in G,\ a, b \in G$

$\therefore ab \in G$ --- ($\because$ by closureness property)

so, consider

$(ab)x = a(bx)$ --- ($\because$ by associative property)

$= a(xb)$

$= (ax)b$ ($\because$ by associative property)

$= (xa)b$

$= x(ab)$ --- ($\because$ by associative property)

$\Rightarrow (ab)x = x(ab) \quad \forall x \in G$

$\therefore ab \in Z(G)$

Now,

$a \in Z(G)$

$\Rightarrow ax = xa \quad \forall x \in G$

multiplying a^{-1} by left side

$a^{-1}ax = a^{-1}xa$

$ex = a^{-1}xa$ $\quad$ -- ($\because aa^{-1} = e$)

$x = a^{-1}xa$

multiplying a^{-1} by ~~write~~ right side

$\Rightarrow xa^{-1} = a^{-1}xaa^{-1}$

$xa^{-1} = a^{-1}x.e$ $\quad$ -- ($\because a.a^{-1} = e$)

$xa^{-1} = a^{-1}x$ $\quad \forall x \in G$

$\Rightarrow a^{-1} \in Z(G)$

Now,

$a, b \in Z(G)$

$\Rightarrow$ ~~ab~~ $\Rightarrow ax = xa$ & $bx = xb$ $\quad \forall x \in G$ & $a, b \in G$

let,

$b \in Z(G)$

$\Rightarrow bx = xb$

$\Rightarrow b^{-1}bx = b^{-1}xb$

$\Rightarrow e.x = b^{-1}xb$

$\Rightarrow x = b^{-1}xb$

$\therefore xb^{-1} = b^{-1}xbb^{-1}$

$\Rightarrow xb^{-1} = b^{-1}xe$

$\Rightarrow xb^{-1} = b^{-1}x$ $\quad \forall x \in G$

$\therefore b^{-1} \in Z(G)$

Now,

$a, b^{-1} \in Z(G)$ $\quad$ -- ($\because$ by closure property)

$ax = xa$, $b^{-1}x = xb^{-1}$ $\quad \forall x \in G$

& $ab^{-1} \in G$ ($\because$ Closure property)

Scanned by CamScanner

Now

$(ab^{-1})x = a(b^{-1}x)$ -- ($\because$ by associative property)

$= a(xb^{-1})$

$= (ax)b^{-1}$ -- ($\because$ by associative property)

$= (xa)b^{-1}$

$= x(ab^{-1})$ -- ($\because$ by associative property)

$\Rightarrow (ab^{-1})x = x(ab^{-1})$

$\therefore ab^{-1} \in Z(G)$

$\therefore Z(G)$ is a subgroup of G