

GROUP

BY

Durgesh Chahar (M.Phil Scholar)

I.B.S Khandari agra

History

- ▶ The term group was coined by **Galois** around 1830 to describe sets of functions on finite sets that could be grouped together to form a closed set. The modern definition of the group given by both **Heinrich Weber** and **Walter Von Dyck** in 1882, it did not gain universal acceptance until the twentieth century.

Binary Operation :-

- ▶ Let G be a set. A binary operation on G is a function that assigns each order pair of elements of G an element of G .

$$f : G \times G \rightarrow G$$

- ▶ Remark :
 - is a binary operation on G iff $aob \in G$.

Algebraic Structure :-

- ▶ A non empty set together with one or more than one binary operation is called algebraic structure.

Examples :-

1. $(\mathbb{R}, +, \cdot)$ is an algebraic structure.
2. $(\mathbb{N}, +)$, $(\mathbb{Z}, +)$, $(\mathbb{Q}, +)$ are algebraic structures.

Group :-

A non empty set G together with an operation o is called a group if the following conditions are satisfied :

- Closure axiom,

$$\forall a, b \in G \Rightarrow aob \in G.$$

- Associative axiom,

$$(aob)oc = ao(boc) \quad \forall a, b, c \in G$$

- Existence of identity,

\exists an element $e \in G$, called identity

$$aoe = eoa = a \quad \forall a \in G.$$

- Existence of inverse,

$$a \in G, \exists a^{-1} \in G \text{ s.t}$$

$$a^{-1}oa = aoa^{-1} = e$$

This a^{-1} is called inverse of a .

Abelian Group :-

A group (G, o) is called abelian group or commutative group if $aob = boa \quad \forall a, b \in G$.

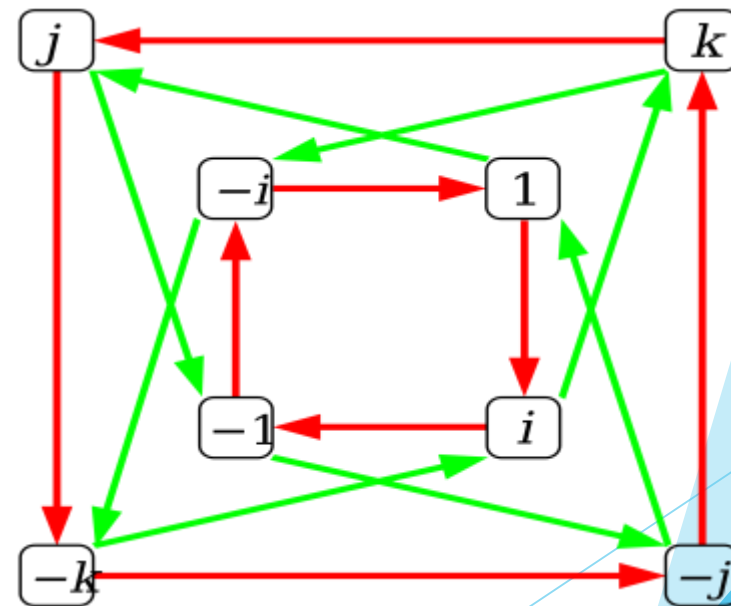
Examples :-

1. $(\mathbb{Z}, +)$, $(\mathbb{Q}, +)$, $(\mathbb{R}, +)$ all are commutative group.
2. (\mathbb{Q}_0, \cdot) , (\mathbb{R}_0, \cdot) are commutative group. 1 is an identity, $\frac{1}{a}$ is the inverse of a in each case.
3. The set of all $m \times n$ matrices (real and complex) with matrix addition as a binary operation is commutative group. The zero matrix is the identity element and the inverse of matrix of A is $-A$.

Quaternion Group :-

$G = \{ \pm 1, \pm i, \pm j, \pm k \}$ define a binary operation of multiplication as
 $i^2 = j^2 = k^2 = -1$, $ij = -jk = k$, $ki = -ik = j$, $jk = -kj = i$.

The red arrows represent multiplication on the right by i , and the green arrows represent multiplication on the right by j .



This is non abelian group for this operation.
This is called Quaternion group.

Klein's four group

- ▶ Let $G = (e, a, b, c)$ with operation o defined by the following table :

o	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

Theorem :-

Uniqueness of identity

- ▶ The identity e in a group always unique.

Proof-

If possible, suppose that e and e' are two identity elements in a group G .

e is an identity element

$$\Rightarrow ee' = e'e = e' \quad [ae = ea = a]$$

e' is an identity element

$$\Rightarrow ee' = e'e = e \quad [ae' = e'a = a]$$

these statements prove that $e = ee' = e'e = e'$

from which, we get $e = e'$.

Theorem :-

The cancellation laws

► Suppose, a, b, c are arbitrary elements of a group G . Then

1. $ab = ac \Rightarrow b = c$ (left cancellation)

2. $ba = ca \Rightarrow b = c$ (right cancellation)

Proof :-

Let e be the identity element in a group G . Let $a, b, c \in G$ be arbitrary

$$ab = ac$$

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

$$\Rightarrow (a^{-1}a)b = (a^{-1}a)c \quad [\text{by associative law}]$$

$$\Rightarrow eb = ec$$

$$\Rightarrow b = c$$

Again

$$ba = ca$$

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

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

$$\Rightarrow be = ce$$

$$\Rightarrow b = c$$

Example :-

1. The positive integer form a cancellative semigroup under addition.
2. The non-negative integers form a cancellative monoid under addition.
3. The cross product of two vectors does not obey the cancellation law.

if $a \times b = a \times c$, then it does not follow that $b = c$ even if $a \neq 0$.

4. Matrix multiplication also does not necessary obey the cancellation law.

$$AB = BC \text{ and } A \neq 0$$

Consider the set of all 2×2 matrices with integer coefficients. The matrix multiplication is defined by

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix} = \begin{pmatrix} aa' + bc' & ab' + bd' \\ ca' + dc' & cb' + dd' \end{pmatrix}$$

It is associative, and $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ is identity but the cancellation law does not follow

$$\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} 0 & 2 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} \text{ and}$$

$$\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} 3 & 0 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$$

This implies

$$\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} 0 & 2 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} 3 & 0 \\ 0 & 0 \end{pmatrix} \text{ but } \begin{pmatrix} 0 & 2 \\ 0 & 0 \end{pmatrix} \neq \begin{pmatrix} 3 & 0 \\ 0 & 0 \end{pmatrix}$$

Theorem :-

Uniqueness of inverse

- ▶ The inverse of each element of a group is unique.

Proof :-

If possible, let a and b be two elements of a group G , so that

$$ba = ab = e \quad \dots(1)$$

$$ca = ac = e \quad \dots(2)$$

e be an identity in G .

$$ba = e = ca$$

or $ba = ca$

$$b = c \quad \text{[by right cancellation law.]}$$

Theorem :-

- ▶ The left identity is also the right identity.

Proof:-

Let e be the left identity of a group G and let $a \in G$ be arbitrary. Then

$$ea = a \quad \text{..... (1)}$$

To prove that e is also that right identity. It suffices to show that

$$ae = a$$

suppose a^{-1} is the left inverse of a , then

a^{-1} is the left inverse of a , then

$$a^{-1}a = e \quad \text{..... (2)}$$

by associative law in G .

$$a^{-1}(ae) = (a^{-1}a)e = e \quad [\text{by (2)}]$$

$$= e = a^{-1}a \quad [\text{again by (2)}]$$

$$a^{-1}(ae) = a^{-1}a \Rightarrow ae = a \quad [\text{by left cancellation law}]$$

Theorem :-

Reverse rule

- ▶ Let a and b be the elements of a group G . Then
then $(ab)^{-1} = b^{-1}a^{-1}$.

Proof:-

consider arbitrary elements a and b of a group G .

Since b^{-1} and a^{-1} are inverse of a and b respectively.

$$b^{-1}b = bb^{-1} = e, \text{ and } a^{-1}a = aa^{-1} = e \quad \text{.....(1)}$$

Hence, by associativity law,

$$(ab)(b^{-1}a^{-1}) = a[(bb^{-1})a^{-1}] = a[ea^{-1}] = aa^{-1} = e \quad \text{.....(2)}$$

$$\text{This } \Rightarrow (ab)^{-1} = b^{-1}a^{-1}.$$

Generalizing this result, we obtain

$$(abc \dots)^{-1} = \dots c^{-1}b^{-1}a^{-1}$$

Theorem:-

► If let G be a group and $a \in G$ then $(a^{-1})^{-1} = a$.

Proof:-

let a^{-1} be the inverse of an element a of a group G , then

$$a^{-1}a = e \quad \text{.....(1)}$$

to prove that the inverse of a^{-1} is a ,

premultiplying (1) by $(a^{-1})^{-1}$,

$[(a^{-1})^{-1} a^{-1}] a = (a^{-1})^{-1} e$, by associative law

$$ea = (a^{-1})^{-1}$$

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

Remark - $e^{-1} = e$.

THANK YOU



A large, bold, black question mark is centered on a white background. The question mark is composed of a thick, curved line forming the hook and a solid black dot at the bottom.