GROUP

Jitendra Kumar
Department of Mathematics
Govt. Degree College Bhojpur
Moradabad

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.

$$f : G \times G \longrightarrow G$$

Remark : o is a binary operation on G iff aob Є G.

Algebraic Structure

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

Examples :

1. $(R,+,\cdot)$ is an algebraic structure.
2. $(N, +)$, $(Z, +)$, $(Q, +)$ 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,

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

- Existence of identity,

$\exists$ an element $e \in G$, called identity $aoe = eoa = a\ \forall\ a \in G$.

- Existence of inverse,

$a \in G$, $\exists\ a^{-1} \in G\ s.t\ a^{-1}\ oa = aoa^{-1} = e$ This a^{-1} is called inverse of a.

Abelian Group

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

Examples :

1. $(\mathbb{Z}, +)$,$(\mathbb{Q}, +)$,$(\mathbb{R}, +)$ all are commutative group.
2. $(Q_0, \cdot)$, $(\mathbb{R}_0, \cdot)$ are commutative group.

The set of all $m \times n$ matrics (real and complex) with matrix addition as a binary operation is commutative group. The zero matric is the identity element and the inverse of matric of A is –A.

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

$\Rightarrow ee' = e'e = e'$ $ae = ea = a$

e' is an identity element

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

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

$$ab = ac \Rightarrow b = c \text{ (left cancellation)}$$

$$ba = ca \Rightarrow b = c \text{ (right cancellation)}$$

Proof :

Let e be the identity element in a group G.

Let $a,b,c \in G$ be arbitrary

$$ab = ac$$

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

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

$$\Rightarrow eb = ec$$

$$\Rightarrow b = c$$

Again $\quad ba = ca$

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

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

$$\Rightarrow \quad be = ce$$

$$\Rightarrow \quad b = c$$

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 and A ≠ 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

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

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

This implies $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 0 & 2 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 0 & 3 \\ 0 & 0 \end{pmatrix}$

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

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

$$ba = ab = e \qquad \text{...(1)}$$

$$ca = ac = e \qquad \text{...(2)}$$

e be an identity in G.

$$ba = e = ca$$

or $ba = ca$

$b = c$ [by right cancellation law.]

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

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

Then 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

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

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

THANKS