

Group :- (Defn)

A group is a non empty set G of elements together with a binary operation " \circ " satisfying the following postulates is called a group

If $a, b, c \in G$, then

(i) $a \circ b \in G$ (closure law)

(ii) The operation is associative

$$a \circ (b \circ c) = (a \circ b) \circ c$$

(iii) There exists an element $e \in G$ such that

$$a \circ e = e \circ a = a.$$

The element e is known as an identity element in G

(iv) ~~For every $a \in G$, there exists an element $b \in G$ such that~~
Existence of inverse.

Each element of G possesses inverse, In other words $a \in G \Rightarrow$ there exists an element $b \in G$ such that $b \circ a = e = a \circ b$. The element

b is then called the inverse of a and

we write $b = a^{-1}$. Thus a^{-1} is an

element of G such that $a^{-1} \circ a = e = a \circ a^{-1}$

$$a^{-1} \circ a = a \circ a^{-1} = e$$

Commutative

Abelian Group :- A group (G, \circ)

is called an abelian or commutative if and only if ' \circ ' is commutative

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

Then the group G is called abelian group.

Finite Group: A group (G, \circ) is said to be finite if the underlying set G consists of only a finite no. of elements.

Infinite group: - A group (G, \circ)

If the group contains an infinite no. of elements then the group is called an infinite group.

The no. of elements in a group is called its order.

An infinite group has an infinite order.

Examples of Abelian group or Commutative group

- (i) The set of all even integers with zero forms an abelian group with respect to addition operation.
- (ii) The set of integers including zero forms a group with respect to addition.
- (iii) The set of real no. with addition as operation forms a group.

Qn:- If $a, b, c \in G$ then

$$ab = ac \Rightarrow b = c \quad \text{[Left Cancellation law]}$$

$$a^{-1}ba = a^{-1}ca \Rightarrow b = c \quad \text{[Right Cancellation law]}$$

Ans. \Rightarrow

Cancellation laws hold good in a group

Proof: $a \in G \Rightarrow \exists a^{-1} \in G$ such that,

$$a^{-1}a = e = aa^{-1} \quad \text{where, } e \text{ is the identity element}$$

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

(multiplying both sides on the left by a^{-1})

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

$$\Rightarrow eb = ec \quad [\because a^{-1}a = e]$$

$$\Rightarrow b = c \quad [\because e \text{ is identity}]$$

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

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

$$\Rightarrow be = ce$$

$$\Rightarrow b = c$$

Qn. \Rightarrow If a and b are elements of a group G , the equations

$$(i) ax = b$$

and (ii) $ya = b$

have unique solutions in G .

Ans. \rightarrow (i) Consider the eqn

$$ax = b \quad \text{--- (1)}$$

We are going to show that $a^{-1}b$ is the solution of the given equation.

It has to be observed that $a^{-1}b \in G$, for a^{-1} and $b \in G$ and therefore $a^{-1}b \in G$.

It $a^{-1}b$ is the solution of the eqn.

then, $x = a^{-1}b$ must satisfy the given eqn.

Now, putting $x = a^{-1}b$ in (1) we have the L.H.S.

$$\begin{aligned} \text{then, } a^{-1}a &= e = a^{-1}a^{-1}b \\ &= a^{-1}(a^{-1}b) = (aa^{-1})b \quad [\text{by associative}] \end{aligned}$$

$$= e^{-1}b \quad [\text{property of inverse } a^{-1}]$$

$$= b \quad [\text{property of the identity}]$$

Therefore the eqn has a

solution $x = (a^{-1}b)$

Now we are going to show that

$x = a^{-1}b$ is the unique solution. It not,

[Suppose $x = c$ is another solution in G .

Putting $x = c$ in (1), we have

$$ac = b$$

multiplying both sides by a^{-1} on the left, we have,

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

$$\text{or, } (a^{-1}a)c = a^{-1}b$$

$$\text{or, } ec = a^{-1}b$$

$$\therefore c = a^{-1}b$$

which means that whatever solution we assume for the given eqn, it will come out to be $a^{-1}b$.

Hence, the solution $x = a^{-1}b$ is unique.

(ii) Consider the eqn

$$ya = b \quad \text{--- (2)}$$

We are going to show that $a^{-1}b$ is the solution of the given equation.

It has to be observed that $a^{-1}b \in G$, for $a^{-1} \in G$ & $b \in G$ and therefore $a^{-1}b \in G$.

If $a^{-1}b$ is solution of the eqn, then, $y = a^{-1}b$ must satisfy the given eqn.

Now, putting $y = a^{-1}b$ in (2), we get the R.H.S.

$$\text{L.H.S.} = (a^{-1}b)a$$

$$= b(aa^{-1}) \quad \text{[by associative]}$$

$$= b \cdot e \quad \text{[by defn of inverse } a^{-1}]$$

$$= b \quad \text{[by defn of the identity]}$$

Therefore the eqn has a solution $y = a^{-1}b$

Now, we are going to show that $y = a^{-1}b$ is the unique solution. If not, suppose $x = c$ is another solution in G .

Putting $y = c$ in (2), we have

$ca = b$
Multiplying both sides by a^{-1} on the Right we have

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

$$\text{or } c(aa^{-1}) = ba^{-1}$$

$$\text{or } ce = ba^{-1}$$

$$\text{or } c = ba^{-1}$$

Which means that whatever solution we assume for the given eqn, it will come out to be ba^{-1} .

Hence, the solution $y = ba^{-1}$

is unique.

✓ QN → To state and prove uniqueness of Inverse.

The Inverse of an element in a group is unique.

Prove that in a group (G) each element a of G has a unique inverse a^{-1} in G .

Ans → Let G be a group. Let a be an element of G and let a^{-1} be its inverse.

We have to prove that a^{-1} is unique.

Let not. Suppose a' is another inverse of a . Since a^{-1} is the inverse of a , therefore,

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

Similarly, since a' is the inverse of a , therefore,

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

where e is the identity element of G . Multiplying (1) by a' on the left, we have

$$a'(aa^{-1}) = a'e = a' \quad \text{--- (3)}$$

Multiplying (2) by a^{-1} on the right, we have

$$(a'a)a^{-1} = ea^{-1} = a^{-1} \quad \text{--- (4)}$$

Since by associative law,

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

therefore we have from (3) & (4)

$$a' = a^{-1}$$

Hence the inverse of an element in a group is unique.

Ans → Let a be any element of a group G and let e be the identity element. Suppose b and c are two inverses of a .

i.e. $ba = e = ab$

& $ca = e = ac$

we have,

$b(ac) = be$ [∵ $ac = e$]

$b(ac) = b$ [∵ e is identity]

Also, $(ba)c = ec$ [∵ $ba = e$]

$(ba)c = c$ [∵ e is identity]

But in a group composition is associative. Therefore,

$b(ac) = (ba)c$

∴ $b = c$.

Q3