

Q.1 Define group with ~~an~~ ^{group.} ~~example~~ examples?

Soln: Group: $\rightarrow$

Let $\circ$ be a binary operation defined over a non-empty set G . Then the set G together with the operation $\circ$ satisfying the following postulates is called a 'group'.

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

I $a \circ b \in G$, (Closure axiom)

II The operation is associative,

that is $a \circ (b \circ c) = (a \circ b) \circ c$ (Associative axiom)

III There exists an element $e \in G$ such that

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

The element e is called an identity element in G . (Identity axiom)

IV For every $a \in G$, there exists an element $a^{-1} \in G$ such that

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

(Inverse axiom)

a^{-1} is called the inverse of a in G .

For examples. I The set of integers including zero forms a group with respect to addition.

II The set of real numbers with addition as operation forms a group.

Q.2. Define sub-group with an example.

Soln: Sub group: $\rightarrow$

Let $(G, \circ)$ be any group and H any sub-set of G . If the set H together with the operation $\circ$ forms a group $(H, \circ)$, then $(H, \circ)$ is a sub-group of $(G, \circ)$.

For example.

The additive group of even integers H is a sub-group of the additive group of integers G .

Thm 3.1 Let $(G, \circ)$ be a group, then

17-07-2020

(i) The identity element e is unique

(ii) Every element $a \in G$ has unique inverse in G .

Proof: (i) Let e_1 and e_2 be two distinct identities of the group G . Then, by definition of identity, we have

$$e_1 \circ e_2 = e_1 \quad (\text{since } e_2 \text{ is identity})$$

And

$$e_1 \circ e_2 = e_2 \quad (\because e_1 \text{ is identity})$$

Hence, it follows that

$$e_1 = e_2$$

$\Rightarrow$ the identity is unique

(ii) Let any element $a \in G$ have two inverses b and c , then we have

$$a \circ b = e = a \circ c$$

$$\text{And } a \circ c = e = c \circ a$$

$$\therefore b = b \circ e = b \circ (a \circ c) = (b \circ a) \circ c \quad (\text{By associativity})$$

$$= e \circ c = c$$

$$\Rightarrow b = c$$

Hence, $a \in G$ has unique inverse.

Q.4. If $(G, \circ)$ is a group, then

(i) $(a^{-1})^{-1} = a \quad \forall a \in G$ (ii) $(a \circ b)^{-1} = b^{-1} \circ a^{-1} \quad \forall a, b \in G$.

Proof: I. Let $a \in G$, there exists an element $b \in G$ such that

$$a \circ b = b \circ a = e$$

From the symmetry of this result, we have

$$a^{-1} = b \quad \text{--- I}$$

$$\text{and } b^{-1} = a \quad \text{--- II}$$

Putting the value of b in eqn (ii) we get

$$(a^{-1})^{-1} = a, \quad \forall a \in G$$

II For all $a, b \in G$, we have

$$\begin{aligned} (a \circ b) \circ (b^{-1} \circ a^{-1}) &= a \circ (b \circ b^{-1}) \circ a^{-1} \quad (\text{By associativity}) \\ &= a \circ (e) \circ a^{-1} = (a \circ e) \circ a^{-1} \quad (\text{By associativity}) \\ &= a \circ a^{-1} = e \end{aligned}$$

Similarly, we can easily show that

$$(b^{-1} \circ a^{-1}) \circ (a \circ b) = e$$

$$\text{Thus, } (a \circ b) \circ (b^{-1} \circ a^{-1}) = e = (b^{-1} \circ a^{-1}) \circ (a \circ b)$$

Hence, it follows that $(a \circ b)^{-1} = b^{-1} \circ a^{-1}$

Proved