B.sc(H) part2 paper3
Topic:Different ways of defining group
Subject:mathematics
Dr. Hari Kant singh
RRS college mokama(patna)

Different ways of defining group

I. Definition of a group based upon left axioms.

Let G be a non-empty set and let a binary operation be defined on it. Then (G, *) is a group if the binary operation * satisfies the following postulates.*

1. *Closure property i.e.* $ab \in G$ *for all* $a, b \in G$
2. *Associativity i.e.* $(ab)c = a(bc)$ *for all* $a, b, c \in G$
3. *Existence of left identity. There exists an element* $e \in G$ *such that* $ea = a$ *for all* $a \in G$

   The element e is called the left identity.
4. *Existence of left inverse. There exists an element* $a^{-1} \in G$ *such that* $a^{-1}a = e$, *i.e. each element of G possesses left identity.*

Proof : In order to show the equivalence of this definition with the original definition of a group, we need to show that
(i) the left identity is also the right identity and
(ii) the left inverse of an inverse is also the right inverse.

For this, we shall first prove the existence of left cancellation law and then we shall prove other two results.

Left Cancellation Law : If a, b, c are in G, then
$ab = ac \Rightarrow b = c$

Proof : Since $a \in G$, there exists $a^{-1} \in G$ such that $a^{-1}a = e$ (existence of left inverse)

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

$\Rightarrow (a^{-1}a)b = (a^{-1}a)c$; by associativity

$\Rightarrow eb = ec$; $\because$ a^{-1} is left inverse of a

$\Rightarrow b = c$; $\because$ e is left identity

Now we shall prove the above two results.

Theorem 1. The left identity is also the right identity i.e. if e is the left identity, then also $ae = a$ for all $a \in G$.

Proof : Let $a \in G$ and e be the left identity i.e. $ea = a$.

Since a possesses left inverse, therefore there exists $a^{-1} \in G$ such that $a^{-1}a = e$.

We have, $a^{-1}(ae) = (a^{-1}a)e$; by associativity

$= ee$; $\because$ $a^{-1}a = e$

$= e$; $\because$ e is left identity

$= a^{-1}a$; $\because$ $a^{-1}a = e$

$\Rightarrow ae = a$; by left cancellation law.

$\therefore$ e is also the right identity.

Hence, $ea = a = ae$ for all $a \in G$.

Theorem 2 : *The left inverse of an element is also its right inverse i.e. if a^{-1} is the left inverse of a, then also $aa^{-1} = e$.*

Proof : Let $a \in G$ and e be the identity element.

Let a^{-1} be the left inverse of a i.e. $a^{-1}a = e$.

We need to prove that $aa^{-1} = e$.

We have, $a^{-1}(aa^{-1}) = (a^{-1}a)a^{-1}$; by associativity

$= ea^{-1}$; $\because$ $a^{-1}a = e$

$= a^{-1}$; $\because$ e is left identity

$= a^{-1}e$; $\because$ e is also right identity.

$\Rightarrow aa^{-1} = e$; by left cancellation law.

$\therefore$ a^{-1} is also the right inverse of a.

Hence a^{-1} is the inverse of a i.e. $a^{-1}a = aa^{-1}$.

Thus we prove that the non-empty set $(G, *)$ satisfying the given postulates, also satisfies the postulates of a group defined earlier.

Hence G is a group.

II. ***Let G is a non-empty set with a binary operation * defined on it. Let a, b, c ∈ G be arbitrary, then (G, *) is a group if the following postulates are satisfied.***

(i) $ab \in G$ ***(closure law)***

(ii) $a(bc) = (ab)c$ ***(Associative law)***

(iii) The equations $ax = b$ ***and*** $ya = b$ ***have solutions in G.***

Proof : In order to prove that a set equipped with a binary operation satisfying conditions (i), (ii) and (iii) is a group, we should show that the left identity exists and each element of G possesses left inverse.

It is given that for every pair of elements $a, b \in G$, the equation $ya = b$ has a solution in G. That is, if $a \in G$, then taking $b = a$, we see that there exists an element e $(= y)$ such that

$$ea = a \qquad \text{...(i)}$$

Suppose now that b is any arbitrary element of G. Since $a \in G$, therefore from (iii) there exists $x \in G$ such that

$$ax = b$$

Now $\quad eb = e(ax); \because \quad b = ax$

$= (ea)x;$ by associativity

$= (ax); \quad \because \; ea = a$ from (1)

$= b.$

Thus there exists $e \in G$ such that $eb = b$ for all $b \in G$. Hence e is the left identity.

Suppose now that a is any arbitrary element of G. Since $e \in G$, therefore taking $b = e$ in the given condition viz. $ya = b$, we see that the equation $ya = e$ has a solution in G. Let $c \in G$ such that $ca = e$. Then c is the left inverse of a. Therefore each element of G possesses left inverse.

Since left identity exists and each element possesses left inverse, therefore from (I), the left identity will also be the right identity and the left inverse of any element will also be its right inverse.

Thus, we see that if the given postulates are satisfied, then all the postulates G_1, G_2, G_3, G_4 of a group are satisfied. Hence G is a group.

III. Every finite semi group in which both cancellation laws hold is a group.

i.e. A non-empty set G equipped with a binary operation is a group if

(i) $ab \in G$ **(closure law)**

(ii) $a(bc) = (ab)c$ **(Associative law)**

(iii) $ax = bx \Rightarrow a = b$, $xa = xb \Rightarrow a = b$ **(cancellation law)**

Proof : Let G be a semi-group and $a, b, c \in G$

Since G is a semi-group, axioms G_1 and G_2 are satisfied viz.

G_1 : $ab \in G$ (G is closed)

G_2 : $(ab)c = a(bc)$.(G is associative)

In order to prove that G is a group under the given conditions, namely (i) $ab = ac \Rightarrow b = c$ and (ii) $ba = ca \Rightarrow b = c$, we need to show that

G_3 : G has an identity element and also

G_4 : G has an inverse element.

Suppose the set G has n distinct elements

$$a_1, a_2, a_3, \ldots a_n$$

Let a be any one of these elements.

Then the n products

$$aa_1, aa_2, aa_3 \ldots aa_n$$

are all elements of G. This follows from the fact that $a, b \in G \Rightarrow ab \in G$ (G is closed)

Also, all these n elements are distinct; for

$aa_i = aa_j$ where $a_i, a_j \in G \Rightarrow a_i = a_j$ (left cancellation law)

Therefore if $a_i \neq a_j$ then $aa_i \neq aa_j$.

Thus the elements $aa_1, aa_2, aa_3 \ldots aa_n$ are simply the rearrangement of the n elements of G. Hence if b is any element of G, then any one of these elements will be equal to b. Let $b = aa_k$.

Thus if a, b are any two elements of G, there exists an element, say $a_k \in G$ such that $aa_k = b$.

In other words, the equation $ax = b$ has a solution in G for every pair of elements $a, b \in G$.

Similarly by forming the product

$$a_1a, a_2a, \ldots a_na$$

and by using the right cancellation law, we can show that the equation $xa = b$ has a solution in G for every pair of elements $a, b \in G$.

Hence using the previous theorem, G is a finite group of order n.