Group Theory

Let A be a non-empty set. A binary operation '$*$' on A is a mapping from $A \times A \to A$.

i.e., $a * b \in A$ whenever $a, b \in A$

Eg: on N, define $a * b = a + b$, $a, b \in N$
'$+$' is a binary operation.

Eg: On N, define $a * b = a - b$, $a, b \in N$
'$-$' is <u>not</u> a binary operation

Eg: On Q, $a * b = a/b$, $a, b \in Q$
'$/$' is <u>not</u> a binary operation

Eg: But if $a * b = a/b$, $a, b \in Q \setminus \{0\}$
'$/$' is a binary operation.

Let A be a non-empty set. If '$*$' is a binary operation on A, then we can say that,

(i) '$*$' is closure if $a * b \in A$, $\forall\, a, b \in A$

ii) '$*$' is associative if $a * (b * c) = (a * b) * c$, $\forall a, b, c \in A$

iii) an element <u>$e \in A$</u> is called an <u>identity element</u> w.r.to $*$ if $a * e = e * a = a$, $\forall a \in A$

iv) For given $a \in A$, an element $b \in A$ is said to be inverse of 'a' w.r.to '$*$' if
$a * b = b * a = e$, 'e' identity element.

v) '$*$' is Commutative if $a * b = b * a$, $\forall a, b \in A$

Semigroup: Let A be a nonempty set with binary operation '$*$'.

$(A, *)$ is said to be a Semigroup if it satisfy the following properties:

(i) closure
ii) Associative

Eg: $(N, +)$, $(N, \cdot)$, $(Q, \cdot)$

Monoid: $(A, *)$ is said to be monoid if it satisfy the following properties;

(i) closure
ii) Associative
iii) identity

Eg: $(N, \cdot)$

Group: $(A, *)$ is said to be a group, if it satisfy the following properties;

(i) closure
ii) Associative
iii) identity
iv) inverse

Eg: $(Z, +)$ is a group

$(Z, \cdot)$ is not a group, because inverse does'not exist.

Eg: Show that cube root of unity form a group under multiplication.

$\cdot$	1	w	w^2
1	1	w	w^2
w	w	w^2	1
w^2	w^2	1	w

— closure & associative axioms satisfy
— identity element is '1'
— w is inverse of w^2

Hence it forms a group.

Abelian group: $(A, *)$ is said to be an abelian group, if the following axioms are satisfied;

i) Closure
ii) Associative
iii) identity
iv) inverse
v) Commutative.

Eg: $(\mathbb{Z}, +)$, $(\mathbb{Q}\setminus\{0\}, \cdot)$

Properties of a group:

Theorem: In a group $(G, *)$ identity element is unique.

Proof: Let e_1 and e_2 be the two identity elements of G

Suppose e_1 is an identity element and $e_2 \in G$

$$e_1 * e_2 = e_2 * e_1 = e_2$$

a, b, e
$a * e = e * a = a$
$(\mathbb{Z}, +)$
$3 \in \mathbb{Z}$
$3 + (0) = 3$
ide

111^{ly} e_2 is an ~~et~~ identity elt, and $e_1 \in G$

$$e_1 * e_2 = e_2 * e_1 = e_1$$

$\Rightarrow e_1 = e_2$, identity elt in a group is unique.

Theorem: In a group $(G, *)$, inverse element is unique.

Pf: Let there are two inverses b and c of $a \in G$

a^{-1}
$b = c$

$$a * b = b * a = e \quad \text{--- (1)}$$
$$a * c = c * a = e \quad \text{--- (2)}$$

$b = e * b$ (identity property)
$= (a * c) * b$ by (2)
$= (c * a) * b$ by (2)
$= c * (a * b)$ (associative)
$= c * e = c$ (by 1)

$\Rightarrow b = c$, inverse elt is unique.

Thm: In a group $(G,*)$, $(a^{-1})^{-1} = a$, $\forall a \in G$

Pf: Let $x = a^{-1}$

By definition, $a * x = x * a = e$

$$\Rightarrow x^{-1} = a$$

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

$(a*b)^{-1}$

$(x)*(y) = e$

$y * x = e$

Theorem: In a group $(G,*)$,

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

Pf: Let $x = a*b$, $y = b^{-1}*a^{-1}$

$$\begin{aligned} x*y &= (a*b)*(b^{-1}*a^{-1}) \\ &= a*(b*b^{-1}*a^{-1}) \quad \text{(associative)} \\ &= a*(e*a^{-1}) \\ &= a*a^{-1} = e \end{aligned}$$

$$\begin{aligned} y*x &= (b^{-1}*a^{-1})*(a*b) \\ &= (b^{-1}*a^{-1}*a)*b \quad \text{(associative)} \\ &= (b^{-1}*e)*b \\ &= b^{-1}*b \\ &= e \end{aligned}$$

$$\Rightarrow x*y = y*x = e$$

$$\Rightarrow x^{-1} = y$$

$$\Rightarrow (a*b)^{-1} = b^{-1}*a^{-1}$$

<u>Note:</u> $(a*b*c)^{-1} = c^{-1}*b^{-1}*a^{-1}$

$(a^{-1}*b*c^{-1})^{-1} = c*b^{-1}*a$

<u>Thm:</u> In a group $(G,*)$

(i) $a*b = a*c \Rightarrow b=c$ (left cancellation law)

ii) $a*b = c*b \Rightarrow a=c$ (Right cancellation law)

<u>Pf:</u> (i) $a*b = a*c$

operating a^{-1} on left

$a^{-1}*(a*b) = a^{-1}*(a*c)$

$(a^{-1}*a)*b = (a^{-1}*a)*c$

$e*b = e*c$

$\underline{\underline{b=c}}$

(ii) $a*b = c*b$

Operating b^{-1} on right

$(a*b)*b^{-1} = (c*b)*b^{-1}$

$a*(b*b^{-1}) = c*(b*b^{-1})$ (associative)

$a*e = c*e$

$\Rightarrow \underline{\underline{a=c}}$

<u>Theorem:</u> In a group $(G,*)$, the equations

$a*x = b$ and $y*a = b$, $a,b \in G$ have

unique solutions in G.

Proof: Consider the eqn $a * x = b \quad \text{--- (1)}$

$$\bar{a}^{1} * (a * x) = \bar{a}^{1} * b$$

$$e * x = \bar{a}^{1} * b$$

$$x = \bar{a}^{1} * b$$

$$\Rightarrow x \in G \quad (\text{by closure law})$$

$$\left(\because \bar{a}^{1} \in G, \; b \in G \quad a^{-1} * b \in G\right)$$

To prove the uniqueness,

Let x_1 and x_2 be the two solutions of (1)

i.e., $a * x_1 = b$

$a * x_2 = b$

$$\Rightarrow a * x_1 = a * x_2$$

$$\Rightarrow x_1 = x_2 \quad (\text{by left cancellation law})$$

Now consider, $y * a = b \quad \text{--- (2)}$

$$(y * a) * \bar{a}^{1} = b * \bar{a}^{1}$$

$$y * e = b * \bar{a}^{1}$$

$$y = b * \bar{a}^{1} \in G \quad (\text{by closure law})$$

To prove uniqueness,

Let y_1 and y_2 be two solns of eqn (2)

$y_1 * a = b$

$y_2 * a = b$

$$\Rightarrow y_1 * a = y_2 * a$$

$$\Rightarrow y_1 = y_2 \quad (\text{by right cancellation law})$$

Problems: 1

Let $(\{a,b\}, *)$ be a Semigroup.

If $a*a=b$, then prove that

(i) $a*b = b*a$

ii) $b*b = b$

Proof: (i) $LHS = a*b$

$= a*(a*a)$ (Given $a*a=b$)

$RHS = b*a$

$=(a*a)*a$

$\Rightarrow LHS = RHS$

i.e $a*b = b*a$

(ii) Case 1 Let $a*b=a$ (closure)

consider, $b*b = (a*a)*b$ (given $a*a=b$)

$= a*(a*b)$ (associative)

$= a*a$

$= b$ (given $a*a=b$)

Case 2 Let $a*b=b$ (closure)

$b*b = (a*a)*b$

$= a*(a*b)$ (associative)

$= a*b$

$= b$

$\Rightarrow b*b=b$