Group Theory

Recap

Groupoid(Magma), Semi-group, Monoid

[Set with Single Binary(Closed) Operation]

A *semigroup* is a nonempty set G with an associative binary operation. A *monoid* is a semigroup with an identity. A *group* is a monoid such that each $a \in G$ has an inverse $a^{-1} \in G$. In a semigroup, we define the property:

(*iv*) Semigroup G is *abelian* or *commutative* if $ab = ba$ for all $a, b \in G$.

The *order* of a semigroup/monoid/group is the cardinality of set G, denoted $|G|$. If $|G| < \infty$, then the semigroup/monoid/group is said to be *finite*.

Semigroup, Monoid, Group :

Let G be a non-empty set and * be a binary operation defined on G.

A semigroup is a nonempty set G with an associative binary operation.
A monoid is a semigroup with an identity.
A group is a monoid such that each $a \in G$ has an inverse $a^{-1} \in G$.

Abelian Group :

Group G is abelian or commutative if $a*b = b*a$ for all $a, b \in G$.
An Abelian group is a group satisfying the commutative law.

Cardinality/Order :

The order of a semigroup/monoid/group is the cardinality of set G, denoted $|G|$.
If $|G| < \infty$, then the semigroup/monoid/group is said to be finite.

Relation between different algebraic structures :

If we define a binary algebraic structure as a set with a binary operation on it, then we have the following schematic:

(Binary Algebraic Structures) $\supseteq$ (Semigroups) $\supseteq$ (Monoids) $\supseteq$ (Groups) $\supseteq$ (Abelian Group) .

Questions related to monoid:

Semigroup with Identity

1. Is Identity element unique? — Yes
2. Do we have Left Cancellation Property in Monoid? — No
3. Do we have Right Cancellation Property in Monoid? — No

(1) In any structure, there is at most one identity element.

(2) In a monoid, we don't have left, Right Cancellation property.

Ex: $(N, *)$ $\quad a * b = \max(a, b)$

↳ Monoid ; $e = 1$

Q: If $a * b = a * c$ then $b = c$? (left Cancellation Property)

No.

$3 * 1 = 3 * 2$ But $1 \neq 2$.

3 3

So left Cancellation Not there.

$1 * 3 = 2 * 3$ But $1 \neq 2$.

3 3

So, In monoid, we dont have left Cancellation, Right Cancellation Property.

Q: $(Z, \times)$ — monoid; $e = 1$

Associative

Closes

Q: In $(Z, \times)$, If $a \times b = a \times c$ then $b = c$?

Q: $(Z, \times)$ — monoid; $e = 1$

Associative

Closed

Q: In $(Z, \times)$, If $a \times b = a \times c$ then $b = c$? ⇒ No

$5 \times 6 = 5 \times b \implies b = 6$ ✓

But

$5 \times 0 = 6 \times 0$ But $5 \neq 6$

So No Right Cancellation.

$0 \times 10 = 0 \times 5$ But $10 \neq 5$

So No left Cancellation.

Note: Meme on Internet:

$$6 \times 9 = 7 \times 9$$

$$\Rightarrow 6 = 7$$

Comment: $(\mathbb{Z}, \times)$ is a monoid,

In monoid, Right Cancellation is Not Guarranteed.

HW Q 25 : True/False ?

Closed operation

a. If $*$ is any binary operation on any set S, then $a * a = a$ for all $a \in S$. — false

b. If $*$ is any commutative binary operation on any set S, then $a * (b * c) = (b * c) * a$ for all $a, b, c \in S$. — True

c. If $*$ is any associative binary operation on any set S, then $a * (b * c) = (b * c) * a$ for all $a, b, c \in S$. false

d. The only binary operations of any importance are those defined on sets of numbers. — false

e. A binary operation $*$ on a set S is commutative if there exist $a, b \in S$ such that $a * b = b * a$. false

f. Every binary operation defined on a set having exactly one element is both commutative and associative. — True

(a) · false: $(N, +)$

$a = 5$

$5 + 5 \neq 5$

$a \# a = a$ — Idempotent element

a: Every Structure has Idempotent Property. — false

Idempotent Property: ⇒ all Elements are Idempotent.

$\forall a, \quad a \# a = a$

Ex: $(R - \{0\}, \times)$

No Idempotent Property:

$2 \times 2 \neq 2$

Ex: $(N, *)$, $a * b = \max(a, b)$

Idempotent property

$a * a = a$

$(\{T, F\}, \wedge)$ — Idempotent property

$T \wedge T = T$
$F \wedge F = F$

$(\{T, F\}, \rightarrow)$ — No Idempotent property.

$F \rightarrow F \neq F$

Idempotent element

$R^{\circ} = R - \{0\}$ = non-zero Reals

$(R^{\circ}, \times)$ — No Idempotent property

→ Idempotent elements = 1 $|X| = 1$

→ NoT Idempotent elements = $-1, 2, 9 \neq 1$

Ex: $(R, \times)$ —— $e = 1$

→ Inverse property!

3^{-1} = Inverse of $3 = \frac{1}{3}$ ✓

No

5^{-1} = " " $5 = \frac{1}{5}$

0^{-1} = " " 0 = DNE

(b) $*$ — Commutative binary op^n

then

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

$$\downarrow$$

$$d$$

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

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

Q: $*$ — Commutative binary opⁿ.

then $a * (b * c) = c * (b * a)$? X

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

$= (c * b) * a$

Commutative :

$\forall_{a,b}$ $\quad a * b = b * a$

Not Commutative :

At least one Counter Example.

$\exists_{a,b}$ $\quad a * b \neq b * a$

Q: If G is a Group But not Abelian then

① $\forall_{a,b}$ $a * b \neq b * a$

② $\exists_{a,b}$ $a * b \neq b * a$

Q: If G is a Group But not Abelian then Is it Possible!

that $\forall_{a,b}$ $a * b \neq b * a$

Ans: No

$a = e,\ b = e$

$e * e = e * e$

$a = x$, $b = x$ then $a * b = b * a$

$x * x$ $x * x$

$a = x$ $b = e$

Group

$x * e = e * x = x$

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

In Every Group :

- $a * e = e * a = a$ — Identity
- $a * a^{-1} = a^{-1} * a = e$

Ex: (Set of Invertible matrices, X)

$n \times n$

matrix multiplication

① Closed $M_{n\times n} \; P_{n\times n} = Q_{n\times n}$

② Associative $(MP)N = (M)(PN)$

③ Identity — Identity matrix $= I$

(4) Inverse

(5) Matrix mul is NOT Commutative.

$AB \neq BA$

$IA = AI = A$

$A\bar{A}^{-1} = \bar{A}^{-1}A = I$

Set of $n \times n$ invertible matrices

Under matrix mul $\Rightarrow$ Group

But not Abelian Group

not Commutative

f : $(S = \{a, b\}, *)$ ⇒ only one binary Op^n

$a * a = a$ ⇒ only one Alg. Structure

$a * a = a * a = a$ Comm

$a * (a * a) = a * (a * a) = a$ Also

Some Important monoids:

Example 2. The following are examples of (commutative) monoids: $(\mathbb{N}, \cdot, 1)$, $(\mathbb{N}, +, 0)$, $(\mathbb{Z}, \cdot, 1)$, $(\mathbb{Z}, +, 0)$, $(\mathbb{Q}, \cdot, 1)$, $(\mathbb{Q}, +, 0)$, $(\mathbb{R}, \cdot, 1)$, $(\mathbb{R}, +, 0)$, $(\mathcal{P}(A), \cap, A)$, $(\mathcal{P}(A), \cup, \emptyset)$, for A a given set, as well as $(\{T, F\}, \vee, F)$ and $(\{T, F\}, \wedge, T)$.

Any Non-empty set A

$(P(A), \cup)$ — monoid $e = \phi$

$(P(A), \cap)$ — monoid $e = A$

$(P(A), -)$ — Set Diff not Asso — Not Semigroup $\Rightarrow$ Not monoid

$A = \{a, b\}$

$P(A) = \{\phi, \{a\}, \{b\}, \{a, b\}\}$

Base set

A

Elements of Base set

Union $\Rightarrow e = \phi$; Intersection $\Rightarrow e = A$

Group Theory

Next Topic

Groups

Closed, Associative, Identity, Inverse

Website : https://www.goclasses.in/

Fundamental Definition. *A **group** is a set G, together with a binary operation $*$, such that the following hold:*

1. *(Associativity):* $(a * b) * c = a * (b * c)\ \forall a, b, c \in G$.
2. *(Existence of identity):* $\exists e \in G$ *such that* $a * e = e * a = a\ \forall a \in G$.
3. *(Existence of inverses): Given* $a \in G, \exists b \in G$ *such that* $a * b = b * a = e$.

Closure

Group

- **Group:** An algebraic system (G, *) is said to be a **group** if the following conditions are satisfied.

  1) * is a closed operation.

  2) * is an associative operation.

  3) There is an identity in G.

  4) Every element in G has inverse in G.

- **Abelian group (Commutative group):** A group (G, *) is said to be ***abelian*** (or ***commutative)*** if

  $a * b = b * a$.

Ex. Show that set of all non zero real numbers is a group with respect to multiplication .

- Solution: Let R^* = set of all non zero real numbers.

Let a, b, c are any three elements of R^* .

1. Closure property : We know that, product of two nonzero real numbers is again a nonzero real number .

   i.e., $a \cdot b \in R^*$ for all $a,b \in R^*$.

2. Associativity: We know that multiplication of real numbers is associative.

   i.e., $(a.b).c = a.(b.c)$ for all $a,b,c \in R^*$.

3. Identity : We have $1 \in R^*$ and $a \cdot 1 = a$ for all $a \in R^*$.

   $\therefore$ Identity element exists, and '1' is the identity element.

4. Inverse: To each $a \in R^*$, we have $1/a \in R^*$ such that

   $a \cdot (1/a) = 1$ i.e., Each element in R^* has an inverse.

$\bar{a}^1 = 1/a$

Contd.,

- 5.Commutativity: We know that multiplication of real numbers is commutative.

  i.e., $a \cdot b = b \cdot a$ for all $a,b \in R^*$.

  Hence, $(R^*, .)$ is an abelian group.

- Ex: Show that set of all real numbers 'R' is not a group with respect to multiplication.
- Solution: We have $0 \in R$.

  The multiplicative inverse of 0 does not exist.

  Hence. R is not a group.

Example

- Ex. Let (Z, *) be an algebraic structure, where Z is the set of integers and the operation * is defined by $n * m$ = maximum of (n, m).
  Show that (Z, *) is a semi group.
  Is (Z, *) a monoid ?. Justify your answer.
- Solution: Let a , b and c are any three integers.

Closure property: Now, $a * b$ = maximum of $(a, b) \in Z$ for all $a,b \in Z$

Associativity : $(a * b) * c$ = maximum of $\{a,b,c\}$ = $a * (b * c)$

$\therefore$ (Z, *) is a semi group.

Identity : There is no integer x such that

$a * x$ = maximum of $(a, x) = a$ for all $a \in Z$

$\therefore$ Identity element does not exist. Hence, (Z, *) is not a monoid.

Ex. Show that the set of all positive rational numbers forms an abelian group under the composition * defined by $a * b = (ab)/2$.

- Solution: Let A = set of all positive rational numbers.

Let a,b,c be any three elements of A.

1. Closure property: We know that, Product of two positive rational numbers is again a rational number.

   i.e., $a * b \in A$ for all $a,b \in A$.

2. Associativity: $(a*b)*c = (ab/2) * c = (abc) / 4$

   $a*(b*c) = a * (bc/2) = (abc) / 4$

3. Identity : Let e be the identity element.

   We have $a*e = (a\ e)/2$ ...(1) , By the definition of *

   again, $a*e = a$ .....(2) , Since e is the identity.

From (1)and (2), $(a\ e)/2 = a \Rightarrow e = 2$ and $2 \in A$.

$\therefore$ Identity element exists, and '2' is the identity element in A.

Contd.,

- 4. Inverse: Let $a \in A$

  let us suppose b is inverse of a.

  Now, $a * b = (a\ b)/2$ ....(1) (By definition of inverse.)

  Again, $a * b = e = 2$ .....(2) (By definition of inverse)

  From (1) and (2), it follows that

  $(a\ b)/2 = 2$

  $\Rightarrow \quad b = (4 / a) \in A$

$\therefore$ (A ,*) is a group.

- Commutativity: $a * b = (ab/2) = (ba/2) = b * a$
- Hence, (A,*) is an abelian group.

Some Common Groups :

$(\mathbb{Z}, +)$

$(\mathbb{R}, +)$

$(\mathbb{Q}, +)$

$(\mathbb{C}, +)$ — Set of Complex numbers

$(\mathbb{N}, +)$ — Not Group

$e = DNE$

$(W, +)$ — Not Group

$3^{-1} = DNE$

Some Common Groups :

$(R^0, \times)$ ⟵ $R^0 = R - \{0\}$

$(C^0, \times)$ ⟵ $C^0 = C - \{0\}$

$(Q^0, \times)$ ⟵ $Q^0 = Q - \{0\}$

$(R, \times)$
$(Q, \times)$
$(Z, \times)$
} Not Groups

$\bar{0}^1 = DNE$

(Z°, X) — No Inverse property

$3^{-1} = ?$, $3 \times ? = 1$

DNE

Examples :

Z, Q, R, and C form infinite abelian groups under addition. Each is an monoid under multiplication, but not a group (since 0 has no multiplicative inverse).
The set of all 2 × 2 matrices with real entries form a monoid under matrix multiplication but not a group (since this set includes many singular matrices).
The nonzero elements of Q, R, and C form infinite abelian groups under multiplication.
The even integers under multiplication form an semigroup that is not a monoid (since it contains no multiplicative identity).

Which of the following are groups?

(a) $(\mathbb{Z}, -)$, where $\mathbb{Z}$ is the set of integers, and $-$ is subtraction.

(b) $(\mathbb{R}, *)$, where $\mathbb{R}$ is the set of real numbers and $*$ is the binary operation defined by $x * y := x + y - 1$.

Abelian group

(a) $(Z, -)$ — not Asso, not Comm, e = DNE

Magma / Groupoid

No Inverse property

(b) $(R, *)$ $\quad a * b = a + b - 1$

(1) Closed ✓

(2) Asso ✓

(3) Is $e = 1$ ✓

(4) Comm ✓

(5) $\bar{a}^1$? $\quad a * \bar{a}^1 = 1$

$a + \bar{a}^1 - 1 = 1$

$e * a = a$

$e + a - 1 = a$

$e = 1$ ✓

$\bar{a}^1 = 2 - a$

Group Theory

Next Topic

Some Important Groups

Addition Modulo n, Roots of Unity

Website : https://www.goclasses.in/

1. Set of nth Roots of Unity, under multiplication
2. Z_n — Addition modulo n

Group Theory

Important Groups:

Roots of Unity(Roots of 1)

Iota, Omega (under multiplication)

Website : https://www.goclasses.in/

General definition [edit]

An *nth root of unity*, where n is a positive integer, is a number z satisfying the equation[1][2]

$$z^n = 1.$$

Given a positive integer n, a complex number z is called an **nth root of unity** if $z^n = 1$. In other words, z is a root of the polynomial $X^n - 1$.

$x = 1 \Rightarrow x = \{1\}$

$(\{1\}, \times)$ Group, order $= 1$, $e = 1$

$x^2 = 1 \Rightarrow x = \{1, -1\}$ — Roots of unity

$(\{1, -1\}, \times)$ — Group $e = 1$

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

$x^2 = 1$

$x = \{1, -1\}$

$(\{1, -1\}, \times)$ — $e = 1$

Group

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

$e^{-1} = e$

$(-1)(-1) = 1$

Order = 2

$x^3 = 1$

$x = \{1\}$

$x^3 = 1$

$x^3 - 1 = 0$ — 3-Deg Polynomial

$x = 1$ will satisfy.

$x^2(x-1) + x(x-1) + 1(x-1)$

$x^3 - x^2 + x^2 - x + x - 1$

$$x^3 - 1 = (x-1)(x^2+x+1) = 0$$

$x = 1$ ✓

$x^2 + x + 1 = 0$

$x = \frac{-b \pm \sqrt{b^2-4ac}}{2a}$

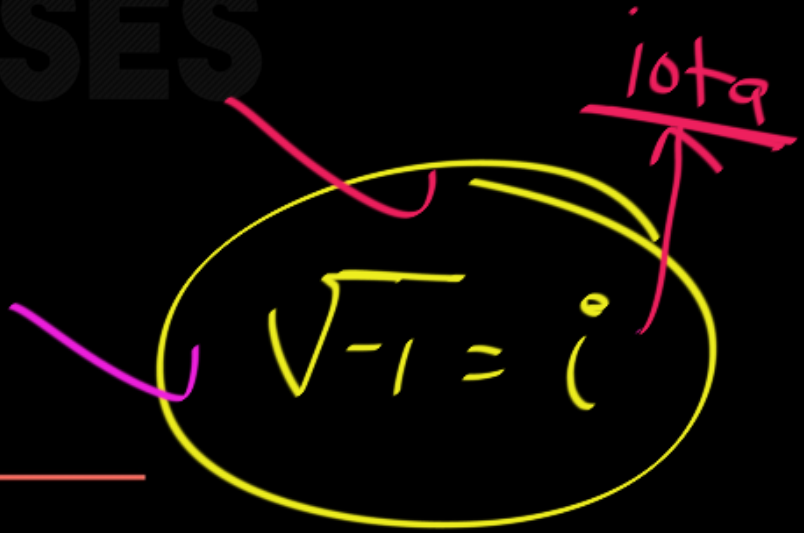
$$x = \frac{-1 \pm \sqrt{1-4}}{2} = \frac{-1 \pm \sqrt{-3}}{2}$$

$$x = \frac{-1 \pm \sqrt{-3}}{2}$$

$$\sqrt{-3} = \sqrt{3}\sqrt{-1}$$

$$\sqrt{-3} = \sqrt{3}\, i$$

$$\boxed{x = \frac{-1 \pm i\sqrt{3}}{2}}$$



$x^3 = 1 \Rightarrow x = \left\{1, \frac{-1+i\sqrt{3}}{2}, \frac{-1-i\sqrt{3}}{2}\right\}$

$1 \quad \omega \quad \omega^2$

$x = \{1, \omega, \omega^2\}$

$x^3 = 1 \Rightarrow x = \{1, \omega, \omega^2\}$

omega

$1 + \omega + \omega^2 = 0$

$\omega^3 = 1$

Cube roots of unity $= 1$

$x^3 = 1 \Rightarrow x = \{1, \omega, \omega^2\}$

$1 + \omega + \omega^2 = 0$

$\omega^3 = 1$

$1 \cdot \omega^2 = \omega^2$

$1 \cdot \omega = \omega$

$\omega \cdot \omega = \omega^2$

$\omega \cdot \omega^2 = \omega^3 = 1$

Also Closed

$(\{1, \omega, \omega^2\}, \times)$ — Group

$e = 1$

$\omega^2 \cdot \omega^2 = \omega^4$

$= \omega^3 \cdot \omega$

$= \omega$

$\omega^4 = \omega^3 \cdot \omega = 1 \cdot \omega = \omega$

$\omega^{10} = \omega^9 \cdot \omega = 1 \cdot \omega = \omega$

$\omega^{50} = \omega^{48} \cdot \omega^2 = \omega^2$

$((1, \omega, \omega^2), \times)$

$1^{-1} = 1$ ✓

$e^{-1} = e$ ✓

$(\omega^2)^{-1} \Rightarrow \omega^2 \bigcirc_{\omega} = 1$

$\omega^{-1} \Rightarrow \omega \cdot \bigcirc_{\omega^2} = 1$

$(\{1, \omega, \omega^2\}, \times)$ — Abelian Group

$e = 1$

Cube-roots of 1

$x^3 = 1 \Rightarrow x = (1)^{\frac{1}{3}} \Rightarrow$ Cube Root of 1

$x^4 = 1 \Rightarrow x = \{1, -1, i, -i\}$

$x^4 = 1 \Rightarrow x^4 - 1 = 0$

4th Root of unity

$a^2 - b^2 = (a+b)(a-b)$

$(x^2+1)(x^2-1) = 0$

$x^2 = -1 \Rightarrow x = i, -i$

$x^2 = 1 \Rightarrow x = \pm 1$

$(\{1, -1, i, -i\}, \times)$ — Closed — $-i \times -i = -1$

Assoc ; Comm

↳ Abelian Group

$e = 1$

$1^{-1} = 1$

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

$e^{-1} = e$

$(-1)(\quad) = 1$

-1

$i^{-1} = ?$

$i \cdot (\quad) = 1$

$-i$

$i^{-1} = -i$; $(-i)^{-1} = i$

Properties of i:

$$i = \sqrt{-1}$$

$$i^2 = -1$$

$$i^3 = i^2 \cdot i = -i$$

$$i^4 = i^2 \cdot i^2 = 1$$

$$i^{18} = (i^{16})(i^2) = -1$$

$i^{16} \rightarrow 1$, $i^2 \rightarrow -1$

Conclusion:

(1) $x = 1 \Rightarrow x = (\{1\}, \times)$ — Abelian Group

(2) $x^2 = 1 \Rightarrow x = (\{1, -1\}, \times)$ — Abelian Group

2^{nd} - Roots of unity

(3) $x^3 = 1$ $\Rightarrow$ $x = (\{1, \omega, \omega^2\}, \times)$ — Abelian Group

$x = 1^{1/3}$ → 3^{rd} Roots of unity

(4) $x^4 = 1$ $\Rightarrow$ $x = (\{1, -1, i, -i\}, \times)$ — Abelian Group

$x = 1^{1/4}$ → 4^{th} Roots of unity

Note:

for all $n \geq 1$;

n^{th} Roots of unity is Abelian Group under multiplication.

$x^n = 1 \Rightarrow x = \{1, \alpha, \alpha^2, \cdots, \alpha^{n-1}\}$

n solutions

Abelian Group under multiplication

n^{th} Roots of unity

Group Theory

Important Groups:

Addition Modulo n

$Z_n = \{0,1,2,\ldots,n-1\}$ under Addition Modulo Operation

Website : https://www.goclasses.in/

The group $\mathbb{Z}_n$ consists of the elements $\{0, 1, 2, \ldots, n-1\}$ with *addition* mod n as the operation. You can also *multiply* elements of $\mathbb{Z}_n$, but you do not obtain a group: The element 0 does not have a multiplicative inverse, for instance.

$n \in N$

$Z_n = \{0, 1, 2, \ldots, n-1\}$

Remainders when divided by n.

$Z_3 = \{0, 1, 2\}$ $Z_4 = \{0, 1, 2, 3\}$

$Z_2 = \{0, 1\}$ $Z_6 = \{0, 1, 2, 3, 4, 5\}$

Operation: Addition modulo n

$(Z_n, \oplus_n)$ $a \oplus_n b = (a+b) \bmod n$

$(Z_4, \oplus_4) = (\{0,1,2,3\}, \oplus_4)$

(1) Understand the opⁿ:

$1 \oplus_4 3 = (1+3) \bmod 4 = 4 \bmod 4 = 0$

$3 \oplus_4 2 = 1$; $0 \oplus_4 3 = 3$

$(\{0,1,2,3\}, \oplus_4)$ — Addition modulo 4

① Closed! Yes

② Asso — Just like Addition

③ e=1! $\boxed{e=0}$

④ Commutative

$1 \oplus_4 3 = 0$

$0 \oplus_4 2 = 2$

$0 \oplus_4 1 = 1$

$(\{0,1,2,3\}, \oplus_4)$ $\quad e = 0$

$0^{-1} = 0$

$\boxed{e^{-1} = e}$

$1^{-1} = ?$ $\quad 1 \oplus_4 \bigcirc = 0$ $\quad 1^{-1} = 3$; $\quad 3^{-1} = 1$

3

$2^{-1} = ? = 2 \oplus_4 \bigcirc = 0$ $\quad 2^{-1} = 2$

2

In General : $(Z_n, \oplus_n)$ $n \in N$

$Z_n = \{0, 1, 2, 3, \ldots, n-1\}, \oplus_n)$

(1) Closed
(2) Assoc
(3) $e = 0$
(4) Comm
(5) $\bar{a}^{-1} = n - a$; $\forall a \neq 0$

$\bar{0}^{-1} = 0$

$\bar{0}^{-1} = 0 \; ; \; \forall a \neq 0 \quad \bar{a}^{-1} = ?$

$a \oplus_n 0 = 0 \Rightarrow e$

$= (a + 0) \bmod n = 0$

$n \bmod n = 0$

$n - a$

Group Theory

Next Topic

Properties of Groups

Unique Identity, Unique Inverse, Left(Right) Cancellation

Website : https://www.goclasses.in/

For Groups,

Proofs are VERY Important (as you will see while solving GATE PYQs) and VERY EASY(for GATE level).

Almost All the proofs need two things-

1. **Apply the definitions**.(Eg. Definition of Identity element, Inverse element, Associativity etc)
2. **Multiply both sides by Inverse** of some element to get desired result.

Proposition. *Let $(G, *)$ be a group. The identity element is unique.*

Proof. Assume $e, e' \in G$ both behave like the identity. Then $e = e * e' = e'$.

e, e' ⇒ Identity

e = Id

e * e' = e'

e' = Id

e * e' = e

So, e * e' = e' = e

Q2: Prove that In a Group, every element has unique inverse!

Proof by Contradiction:

Assume a has two inverses b, c.

$\bar{a}^1 = b, c$

$\bar{a}^1 = b$

$\bar{a}^1 = c$

So, $\boxed{a * b = e}$; $\boxed{a * c = e}$

$\Rightarrow a * b = a * c$

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

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

Group is Asso. ✓

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

$$e * b = e * c \Rightarrow b = c$$

Proposition. *Let $(G, *)$ be a group. For $a \in G$ there is only one element which behaves like the inverse of a.*

Proof. Assume $a \in G$ has 2 inverses, $b, c \in G$. Then:

$$\begin{aligned} (a * b) &= e \\ c * (a * b) &= c * e \\ (c * a) * b &= c \quad \text{(associativity and identity)} \\ e * b &= c \\ b &= c \end{aligned}$$

(3) Prove that Group has left Cancellation property?

If $a * b = a * c$ then $b = c$

└ left Cancellation property

$a * b = a * c$

$\bar{a}^1 a = \bar{a}^1 a$

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

Group is Associative

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

$e * b = e * c$

$\Rightarrow b = c$

(4) Prove that Group has Right Cancellation property?

$$a * b = c * b$$

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

$$\Rightarrow a * e = c * e \Rightarrow \boxed{a = c}$$

In Group :

If $a * b = a * c \implies b = c$

If $a * b = c * b \implies a = c$

BUT $a * b = b * c \not\implies a = c$

In Abelian Group

If $a * b = a * c \Rightarrow b = c$ ✓

If $a * b = c * b \Rightarrow a = c$ ✓

And $a * b = \boxed{b * c} \Rightarrow a = c$

$a * b = c * b \Rightarrow a = c$

Cancellation Law for Groups. *Let $a, b, c \in G$ a group. Then*

$$a * c = a * b \Rightarrow c = b \text{ and } c * a = b * a \Rightarrow c = b$$

Proof. Compose on left or right by $a^{-1} \in G$, then apply the associativity and inverses and identity axioms. □

Theorem

- Ex. In a group (G, *) , Prove that the identity element is unique.
- Proof :

a) Let e_1 and e_2 are two identity elements in G.

Now, $e_1 * e_2 = e_1$ ...(1) (since e_2 is the identity)

Again, $e_1 * e_2 = e_2$ ...(2) (since e_1 is the identity)

From (1) and (2), we have $e_1 = e_2$

$\therefore$ Identity element in a group is unique.

Theorem 14.1

For any group G, the following properties hold:

(i) If $a, b, c, \in G$ and $ab = ac$ then $b = c$. (left cancellation law)
(ii) If $a, b, c, \in G$ and $ba = ca$ then $b = c$. (right cancellation law)
(iii) If $a \in G$ then $(a^{-1})^{-1} = a$. The inverse of the inverse of an element is the element itself.
(iv) If $a, b \in G$ then $(ab)^{-1} = b^{-1}a^{-1}$. That is the inverse of a product is the product of the inverses in reverse order.

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

$$a = b^{-1} \text{ iff } b = a^{-1}$$

Q: Group G then prove:

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

$ab = a * b$

let $(ab)^{-1} = y$ ⟶ find y.

means

$$aby = e$$

$$(\bar{a}^1 (a) by) = \bar{a}^1 e = \bar{a}^1$$

$$by = \bar{a}^1$$

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

Theorem

- In a Group (G, *) the following properties hold good

1. Identity element is unique.
2. Inverse of an element is unique.
3. Cancellation laws hold good

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

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

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

- In a group, the identity element is its own inverse.

- ***Order of a group*** : The number of elements in a group is called order of the group.

- Finite group: If the order of a group G is finite, then G is called a finite group.