Friday, March 26, 2021 9:48 AM

Group Theory

$G \to$ Set ?

$A = \{a, b, c\}$

$B = \{1, 2, 3\}$

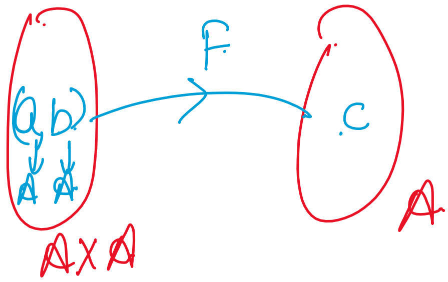
Binary operation / function

$\hookrightarrow F : A \times A \to A$ is Binary operation

Cartesian Product $A \times B$

$(a, 1)$ — $a \in A$, $1 \in B$

$F(a, b) = c$



$\Rightarrow$ A non-empty set 'G' together with binary operation '$*$' is called as algebraic structure & notation $\langle G, * \rangle$

Group: A non-empty set G with Binary operation '$*$' is called a group if it satisfies following properties:

① **Closure:** $\forall a, b \in G$ then $a * b \in G$

$\forall \to$ for all

then $a * b \in G$ | $\in \rightarrow$ belongs to

eg: $G = \{1, 2, 3, 4, \text{------}\}$

$* =$ Addition

for every a, b [Let $2, 6 \in G$

$2 + 6 = 8 \in G \Rightarrow$ closure satisfied

eg: $G = \{1, 2, 3, 4, \text{------}\}$

$* =$ Subtraction

$1 - 2 = -1 \notin G \Rightarrow$ closure not satisfied

② Associativity : $\forall\ a, b, c \in G$

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

eg: $G = \{1, 2, 3, 4, 5, \text{----}\}$

$* =$ Addition

$$(a + b) + c = a + (b + c)$$

$$(2 + 3) + 7 = 2 + (3 + 7) = 12$$

Associativity satisfied

eg: $* =$ multiplication $\rightarrow$ satisfied

$$(2 \times 3) \times 4 = 2 \times (3 \times 4)$$

eg: $* =$ subtraction $\rightarrow$ not satisfied

$$(2 - 3) - 1 \neq 2 - (3 - 1)$$

$-2 \neq 0$

3. Existence of Identity Element

$\forall\ a \in G$, $\exists$ an element $e \in G$ such that

$$a * e = a = e * a$$

Here, e is called as identity element

$\exists$ There exists

eg: $G = \{1, 2, 3, 4, 5, ---\}$.
$* =$ Multiplications

$$a \times 1 = a = 1 \times a$$

$\Rightarrow 1 \in G$, identity element exists

eg: $G = \{1, 2, 3, ---\}$
$* =$ Addition

$$a + 0 = a = 0 + a$$

$\Rightarrow 0 \notin G$, identity not exists

4. Existence of Inverse element

$\forall\ a \in G$, $\exists$ an element $b \in G$ such that

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

Here, e = identity element
$\Rightarrow$ b = Inverse element of a

eg: G = Set of Integers = $\{0, \pm 1, \pm 2, \pm 3 \ldots\}$
$*$ = Addition

$$a + \underline{0} = a = \underline{0} + a$$

$0 \in G$ i.e. Identity exists.

$$a + \underline{(-a)} = 0 = -a + a$$

If $a \in G$, Inverse of a $\in G \Rightarrow$ Inverse exist.

eg: $G = \{0, \pm 1, \pm 2, \pm 3, \text{---} \}$ ✓
$*$ = Multiplication

Identity $e = 1 \in G$

$$a \cdot \underline{1} = a = 1 \cdot a$$

Inverse

$$a \cdot \frac{1}{a} = 1 = \frac{1}{a} \cdot a$$

$\Rightarrow$ $\frac{1}{a} \notin G$ So Inverse not exists

Qu: Check $\langle G, + \rangle$ is a group or not where G is set of odd natural numbers

Sol: $G = \{1, 3, 5, 7, \text{------}\}$

$* = \text{Addition}$

① Closure : $1 + 3 = 4 \notin G$

$\Rightarrow$ Closure not satisfied

$\Rightarrow$ Hence, $\langle G, + \rangle$ is not a group

Que: $\langle \mathbb{R}, \cdot \rangle$ is group or not ?

$\mathbb{R} \to$ Real no.

$\mathbb{Q} \to$ Rational

Sol: $\mathbb{R}$ = Real ,

$*$ – Multiplication

① Cloure Property: $\forall\ a, b \in R$

$a \cdot b \in R$ True

$\therefore$ Closure property satisfied.

② Associative : Reals satisfy asso.

ie $(a \cdot b) \cdot c = a \cdot (b \cdot c) \ \forall\ a, b, c$

③ Existence of Identity

$a \cdot 1 = a = 1 \cdot a$

$\Rightarrow e = 1 \in R$, identity exists

④ Existence of Inverse:

$$a * b = e = b * a$$

But For $0 \in R$, no element exists such that $0 \times b = 1 = b \times 0$

$\therefore$ $(R, \cdot)$ is not a group.

$\langle G, * \rangle$ is a groupoid if closure satisfies

$\langle G, * \rangle$ is a semi-group if closure & associativity satisfies

$\langle G, * \rangle$ is a Monoid if closure, associativity & Existence of identity satisfies

Abelian Group: A group $\langle G, * \rangle$ is called abelian if Commutativity satisfies i.e.

$$a * b = b * a \quad \forall\, a, b \in G$$

Comm:

$$\left.\begin{array}{l} a+b = b+a \\ a \cdot b = b \cdot a \end{array}\right]$$

$a - b \neq b - a$ not commutative

$\langle G, * \rangle$ is abelian if

$(\mathbb{R} - \{0\}, \cdot)$ is abelian group.

if $a \cdot b = b \cdot a \ \forall\ a, b \in \mathbb{R}$

($\because$ Commutativity Holds in Reals)

Hence, its abelian

Which of following is abelian

1. $(\mathbb{R}, \cdot) \longrightarrow$ not group ($\because$ Inverse not exists)
2. $(\mathbb{N}, +) \longrightarrow$ not group ($\because$ Identity not exists)
3. $(\mathbb{Z}, \cdot) \longrightarrow$ not a group ($\because$ Inverse not exists)
4. $(\mathbb{R} - \{0\}, \cdot) \longrightarrow$ abelian group.

① Closure ✓ ② Asso. ✓

③ Id. = $a + \underline{0} = a = \underline{0} + a$

$0 \notin \mathbb{N} \Rightarrow$

$(\mathbb{Z}, \cdot) \rightarrow \quad a * b = e =$

$a \cdot \frac{1}{a} = 1$

$\frac{1}{a} \notin \mathbb{Z} = \{0, \pm 1, \pm 2, \text{---} \}$

Qu: Consider the set of +ve integers 'I'

& Binary operation is defined as

$$a * b = \frac{ab}{4} \quad \forall\ a, b \in I$$

Check $(I, *)$ is a group or not?

Sol: $I = \{1, 2, 3, 4, \text{-------}\}$

① Closure: $a * b = \frac{ab}{4} \notin I$

$5 * 3 = \frac{5 \cdot 3}{4} = \frac{15}{4} \notin I \rightarrow$ Closure not satisfies.

Hence, $(I, *)$ not a group.

Que: I = Set of +ve integers

$$a * b = \frac{ab}{4} \quad \forall\ a, b \in I$$

$a * e = \frac{ae}{4}$

find the identity element for $<I, *>$.

Sol: e is identity if

$a * e = a = e * a$

$a * b = \frac{ab}{4}$

$\frac{ae}{4} = a$

$\Rightarrow \frac{ae}{4} - a = 0 \Rightarrow a\left[\frac{e}{4} - 1\right] = 0$

either $\underbrace{a = 0}_{\text{not possible}}$ or $\left[\frac{e}{4} - 1\right] = 0$

$\Rightarrow \frac{e}{4} - 1 = 0$

$\Rightarrow \frac{e}{4} = 1$

$\Rightarrow \boxed{e = 4}$

Qu: If G = Set of +ve Rationals = $\frac{p}{q}$ form $q \neq 0$

$a * b = \frac{ab}{2} \quad \forall\ a, b \in G$

Check $\langle G, * \rangle$ is a group or not?

Sol: (1) closure: yes

(2) Associativity: yes

$(a * b) * c = \left(\frac{ab}{2}\right) * c = \frac{\left(\frac{ab}{2}\right) \cdot c}{2} =$

$a * (b * c) = a * \left(\frac{bc}{2}\right) = \frac{a\left(\frac{bc}{2}\right)}{2} =$

(3) Identity:

$a * e = a = e * a$

$\frac{ae}{2} = a$

$\Rightarrow a\left[\frac{e}{2} - 1\right] = 0 \Rightarrow a = 0$ or $\frac{e}{2} - 1 =$

$\frac{e}{2} = 1 \Rightarrow \boxed{e=2}$

$e = 2 \in G \rightarrow$ yes

(4) Inverse:

$a * b = e = b * a$

$\underbrace{a * b = 2} = b * a$

$\frac{ab}{2} = 2 \Rightarrow ab = 4$

$\Rightarrow \boxed{b = \frac{4}{a} \quad a \neq 0}$

$b = \frac{4}{a} \in G \Rightarrow$ exists yes

Hence, G is group

Ques:

If G is the set of all the non zero reals and binary operation is defined as

a * b = ab/4 for all a,b in G

binary operation

$$a * b = \frac{ab}{4} \quad \forall\, a, b \in G$$

Check whether G is a group or not?

Sol: ① closure: $\underset{\text{Real}}{a} * \underset{\text{Real}}{b} = \frac{\overset{\text{Real}}{ab}}{4} \to$ Real

Yes

② Associativity:

$$(a * b) * c = \left(\frac{ab}{4}\right) * c = \frac{\left(\frac{ab}{4}\right)c}{4}$$

$$(a * b) * c = \frac{abc}{16} \checkmark$$

$$a * (b * c) = a * \left(\frac{bc}{4}\right) = \frac{a\left(\frac{bc}{4}\right)}{4}$$

$a * b = \frac{ab}{4}$

$$= \frac{abc}{16} \checkmark$$

Yes

③ Identity: $a * e = a = e * a$

$\boxed{a * b = \frac{ab}{4}}$

$$\frac{ae}{4} = a$$

$$\Rightarrow \frac{ae}{4} - a = 0$$

$$= a\left[\frac{e}{4} - 1\right] = 0$$

either

either $\underbrace{a = 0}_{\text{not possible}}$ or $\underbrace{\frac{e}{4} - 1 = 0}_{\text{only possible}}$

G = Non-zero Reals $\qquad \boxed{e = 4} \in G$

$\Rightarrow$ Identity exists in G always unique

④ Inverse :

$a * b = e$

$\frac{ab}{4} \overset{?}{=} 4$

$b = 16/a$

$a * b = e = b * a$

$a * b = 4 = b * a$

$\frac{ab}{4} = 4$

$\Rightarrow b = \frac{16}{a \neq 0} \in G$ Yes

$\downarrow$ Non-zero Reals

$\Rightarrow$ Inverse exists.

⑤ Commutative :

$a * b = \frac{ab}{4} \rightarrow$ Reals

$b * a = \frac{ba}{4} \rightarrow$ Reals

$\Rightarrow a * b = b * a$ Yes

$\Rightarrow (G, *)$ is an abelian group.

Thursday, April 01, 2021
11:41 AM

Group Theory

Qu: If G is set of all real numbers except $\frac{-1}{2}$ & Binary operation

$$a*b = a+b+2ab \quad \forall\ a,b \in G$$

Check whether G is an abelian group?

Sol: (1) Closure: $a, b \in G$ (real but not $\frac{-1}{2}$)

$$a*b = \underbrace{a+b+2ab} \longrightarrow \text{Real}$$

If $a+b+2ab = \frac{-1}{2} \longrightarrow$ not possible

$$2(a+b+2ab) = -1$$

$$2a + 2b + 4ab + 1 = 0$$

$$1(1+2a) + 2b(1+2a) = 0$$

$$(1+2a)(1+2b) = 0$$

either $1+2a = 0$ or $1+2b = 0$

$\Rightarrow \underbrace{a = -\frac{1}{2}}_{\text{not possible}}$ or $\underbrace{b = -1/2}_{\text{not possible}}$

$\therefore\ a*b \in G \Rightarrow$ closure satisfied.

(2) Associativity: $(a*b)*c = (a+b+2ab)*c$

$$= (a+b+2ab) + c + 2(a+b+2ab)c$$

$$= a+b+2ab+c+2ac+2bc+4abc$$

$a*(b*c) =$

$\Longrightarrow a*b = a+b+2ab$

$b*c =$

$$= a*(b+c+2bc)$$

$= a + b + c + 2bc + 2a(b+c+2bc)$

$= a + b + c + 2bc + 2ab + 2ac + 4abc$

$\therefore$ Asso. Holds in G.

(3) Identity: $\underbrace{a * e = a}$ $= e * a$

$$a + e + 2ae = a$$

$$e + 2ae = 0$$

$$e(1+2a) = 0$$

either $\boxed{e = 0}$ or $1 + 2a = 0$ ← not Possible

$a = \frac{-1}{2}$

$e = 0 \in G$

$\Rightarrow$ Identity exists in G.

(4) Inverse: $a * b = e = b * a$

$$a * b = 0$$

$$a + b + 2ab = 0$$

$b \neq \frac{-1}{2}$

$$b + 2ab = -a$$

$$b(1 + 2a) = -a$$

If $b \neq \frac{-1}{2}$ → $b = \frac{-a}{1+2a \neq 0}$ → exists $(\because a \neq \frac{-1}{2})$

$\therefore b \in G \Rightarrow$ Inverse exists

(5) Commutative: $a * b = a + b + 2ab$ → Reals

$b * a = b + a + 2ba$ → Reals

$\therefore a * b = b * a$

Hence, <G, *> is an abelian group.

Qu: G is set of all Rationals except 1

$a * b = a + b - ab \longrightarrow$ Rational

Sol ① Closure: Ration Rational

not possible $\longrightarrow$ If $a + b - ab = 1$ not possible

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

$\therefore$ Closure True.

② Associativity: $a * (b * c) = a * (b + c - bc)$

$= a + (b + c - bc) - a(b + c - bc)$

$= a + b + c - bc - ab - ac + abc$

$(a * b) * c = (a + b - ab) * c$

$= a + b - ab + c - (a + b - ab) \cdot c$

$= a + b - ab + c - ac - bc + abc$

③ Identity: $a * e = a = e * a$

$a + e - ae = a$

$\Rightarrow e - ae = 0 \Rightarrow e(1-a) = 0$

$\Rightarrow \boxed{e = 0}$ or $1 - a = 0 \Leftarrow$ not possible

Rational

$e \in G$

④ Inverse: $a * b = e = b * a$

$a * b = 0$

$a + b - ab = 0$

$b - ab = -a \Rightarrow$

$b(1-a) = -a \Rightarrow \boxed{b = \frac{-a}{1-a}}$ $\neq 0$

$b = \frac{a}{a-1} \in G$, Inverse exists

$1-a \neq 0$

$b = \dfrac{a}{a-1} \in G$, Inverse exists

(5) Comm. :
$a * b = a + b - ab$ Rationals
$b * a = b + a - ba$.
$\Rightarrow a * b = b * a$.

Hence, $\langle G, * \rangle$ is abelian group.

Order of Group

If $(G,*)$ is a group then no. of elements in G is called as order of group.

Notation: $O(G)$ or $|G|$

Finite Group: $O(G) =$ Finite $\longrightarrow$?

Infinite Group: $O(G) =$ Infinite

Que: If $G = \{1, -1, i, -i\}$ finite

Then check G is an abelian group under multiplication.

Note: If G is finite then write Composition Table.

Sol: Composition Table

Mul. operation →

$\cdot$	1	-1	i	$-i$
$\boxed{1}$ (Identity)	$\boxed{1}$	-1	i	$-i$
-1	-1	$\boxed{1}$	$-i$	i
i	i	$-i$	-1	$\boxed{1}$
$-i$	$-i$	i	$\boxed{1}$	-1

① Closure:
all entries are in G
Yes ✓

② Associative:
∵ Asso. Holds

$$\begin{array}{c|cccc} -i & -i & i & \boxed{1} & -1 \end{array}$$

$\because$ Asso. Holds for Multiplication.

③ Identity: $a * e = a = e * a$

$e = 1 \in G$, exists

④ Inverse: Inverse of $1 = 1$

$$\left.\begin{array}{l} -1 = -1 \\ i = -i \\ -i = i \end{array}\right\} \text{all in } G$$

it exists

⑤ Commutative:

$$\begin{bmatrix} 1 & -1 & i & -i \\ -1 & 1 & -i & i \\ i & -i & -1 & 1 \\ -i & i & 1 & -1 \end{bmatrix}^T$$

$$= \begin{bmatrix} 1 & -1 & i & -i \\ -1 & 1 & -i & i \\ i & -i & -1 & 1 \\ -i & i & 1 & -1 \end{bmatrix} \Rightarrow \text{Symm. Matrix}$$

$\Rightarrow$ Commutative Holds.

Hence, $(G, \cdot)$ is an abelian group.

Qu:

$$\underbrace{a * b}_{\text{inverse of } a} = \underline{e} = b * a$$

Que: If $G = \{1, \omega, \omega^2\}$ Then, $(G, \cdot)$

is an abelian group or not

Sol: G = Cube roots of unity

$\underbrace{x^3 = 1}$ $\Rightarrow$ $x = (1)^{1/3} \rightarrow$ cube roots of 1

$x^3 - 1^3 = 0$

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

$a^3 - b^3 = (a-b)(a^2+ab+b^2)$

either $x - 1 = 0$, $x^2+x+1 = 0$

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

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

$x = \frac{-1+\sqrt{3}i}{2}, \frac{-1-\sqrt{3}i}{2}$

ω ω^2 Notation

$x^3 - 1 = 0$

$\omega^3 - 1 = 0$

$\omega^3 = 1$

$\boxed{\omega^3 = 1}$

Composition Table

$\cdot$	1	ω	ω^2
Identity = $\boxed{1}$	$\boxed{1}$	ω	ω^2
ω	ω	ω^2	$\boxed{1}$
ω^2	ω^2	$\boxed{1}$	ω

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

① Closure : Yes

② Asso : Yes Multiplication

③ Identity: $e = 1 \in G$ Yes

④ Inverse: Inverse of $1 = 1$

$\left.\begin{aligned} \omega &= \omega^2 \\ \omega^2 &= \omega \end{aligned}\right\}$ All In G

Inverse exists

⑤ Commutative: ∵ Matrix is symm.

Yes, True

Hence, $(G, \cdot)$ is an abelian Group.

Que: Composition Table

*	a	b	c	d	f
a	b	f	d	a	c
b	f	c	a	b	d
c	d	a	f	c	b
Id. d	a	b	c	d	f
f	c	d	b	f	a

① Find Identity element

② Is group commutative

③ Inverse of $c = ?$

④ Is there $x \in G$, such that $x^3 = d$

Sol: ① $e = d$

② Yes, Symm. Matrix

③ Inverse of $c = a$

④ $x^3 = d$ Only if $x = d$

∵ d is Identity &

$(d * d) * d = d * d = d$

Friday, April 02, 2021
1:42 PM

Addition modulo 'n' operation

Notation: $+_n$

$\Longrightarrow \quad a +_n b = r \pmod{n}$

→ r is remainder when $a+b$ divided by n

eg: $2 +_4 8 = 2 \pmod{4}$

r is remainder when $2+8$ is div. by 4

eg: $5 +_3 7 = 0 \pmod{3}$

$3 +_2 8 = 1 \pmod{2}$

Multiplication Modulo 'n'

Notation → $\times_n$

$a \times_n b = r \pmod{n}$

r is remainder when $a \times b$ is divided by n

eg: (1) $2 \times_3 8 = 1 \pmod{3}$

(2) $5 \times_5 7 = 0 \pmod{5}$

Que: If $G = \{0, 1, 2, 3, 4, 5\}$ → finite then

Check: G forms a group under addition modulo 6 operation.

Sol: Composition Table

$+_6$	0	1	2	3	4	5
0	$\boxed{0}$	1	2	3	4	5
1	1	2	3	4	5	$\boxed{0}$
2	2	3	4	5	$\boxed{0}$	1
3	3	4	5	$\boxed{0}$	1	2
4	4	5	$\boxed{0}$	1	2	3
5	5	$\boxed{0}$	1	2	3	4

$0 +_6 0$

$0 +_6 1$

$0 +_6 2$

inv. of $0 = 0$

" " $1 = 5$

$2 = 4$

$3 = 3$

$4 = 2$

$5 = 1$

1. Closure : Yes $\because$ all elts are from G in Table

2. Asso : Yes

3. Identity : $e = 0 \in G$ exits

   $\because a * e = a = e * a$

4. Inverse : Inv. of $0 = 0$

   $1 = 5$

   $2 = 4$

   $3 = 3$

   $4 = 2$

   $5 = 1$

   $\therefore$ inverse exists for each element

5. Commutative : Yes $\because a +_6 b = b +_6 a$

   $\forall a, b \in G$

All entries above & below diagonal are same.

Hence, $(G, +_6)$ is an abelian group

Que: If $G = \{0, 1, 2, 3, 4, 5, 6\}$ finite. Check $(G, \times_7)$ is a group or not?

Sol: Composition Table:

$0 \times 0 = 0 \to$ Div by 7 rem $= 0$

$0 \times 1 \to 0 \to$

0×2

$1 \times 0 \to 0$

$1 \times 1 = 1$

Identity

$\times_7$	0	1	2	3	4	5	6
0	0	0	0	0	0	0	0
1	0	$\boxed{1}$	2	3	4	5	6
2	0	2	4	6	$\boxed{1}$	3	5
3	0	3	6	2	5	$\boxed{1}$	4
4	0	4	$\boxed{1}$	5	2	6	3
5	0	5	3	$\boxed{1}$	6	4	2
6	0	6	5	4	3	2	$\boxed{1}$

$\because$ Inverse of zero does not exist

$\Rightarrow (G, \times_7)$ is not a group

But $(G, \times_7)$ is a monoid (as closure, Asso & Indentity Holds)

If $G = \{1, 5, 7, 11\}$ then check $(G, \times_{12})$ is group or not?

$\times_{12}$	1	5	7	11
$\boxed{1}$	$\boxed{1}$	5	7	11
5	5	$\boxed{1}$	11	7
7	7	11	$\boxed{1}$	5
11	11	7	5	$\boxed{1}$

Identity →

1. Closure → True.
2. Asso → True
3. Identity → $1 \in G$
4. Inverse: Inv. of 1 = 1
   5 = 5
   7 = 7
   11 = 11
5. Comm → True

Hence $(G, \times_{12})$ is an abelian group.

Que: * | a | b c d.

Que:

*	a	b ✓	c	d ✓
a	b	c	d	a
b	a	b	c	d
c	d	c	a	b
d	c	d	a	b

(1) Comm → NO

(2) Identity → NO

(3) Inverse → NO for b & c

Identity → not exist

$a * e = a = e * a$

$b * a = a$ ✓

$b * b = b$ ✓

$b * c = c$ ✓

$b * d = d$ ✓

$a * b = c$?

$b * b = b$ ✓

$c * b = c$ ✓

$d * b = d$ ✓

Que: G = Set of 2x2 matrices over Reals.

G → Infinite

$\begin{bmatrix} a & b \\ c & d \end{bmatrix} \rightarrow a, b, c, d \rightarrow$ Reals

Check G is group under Matrix multiplication or not?

$A_{m \times n} \quad B_{p \times q}$

$[\ \ ]_{2\times2} [\ \ ]_{2\times2}$

$[\ \ ]_{2\times2}$

(1) closure:

$m \times n$ $\quad p \times q$

① Closure: $\quad A_{2\times 2} \quad B_{2\times 2} \longrightarrow [AB]_{2\times 2} \longrightarrow$ Yes

$\quad [\quad]_{2\times 2}$

② Asso. : $\quad (AB)C = A(BC) \longrightarrow$ yes True.

$$\begin{bmatrix} 2 & 3 \\ 4 & 5 \end{bmatrix} \begin{bmatrix} -1 & 0 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} & \\ & \end{bmatrix}_{2\times 2} \in G$$

③ Identity : $\quad A \cdot I = A = I \cdot A$

$\quad \downarrow I_{2\times 2} \in G \quad$ Yes

④ Inverse: $\quad A A^{-1} = I = A^{-1} A$

$A A^{T} = I$?

$\downarrow$ exists for each A — ?

A^{-1} exists only if $|A| \neq 0$

$\Rightarrow$ Inverse not exists.

$\Rightarrow (G, \cdot)$ is a monoid.

$G \rightarrow$ Set of 2×2 non-singular ($\det \neq 0$) matrices over Reals

Then $(G, \cdot)$ is group. (not abelian)

Then $(G, \cdot)$ is group. (not abelian)

$AB = BA \longrightarrow$ not always

SUBGROUP

If $(G,*)$ is a group and H is a non-empty subset of G such that $(H,*)$ is a group.
Then, H is called as subgroup of G.

$G = \{1,2,3,4,5\}$
Subset $= \{1,2\}$
$\{1\}, \{3\}$
$\{1, 2, 3, 4, \cancel{5}\}$

eg: ✓ $G = \{1, -1, i, -i\}$
$(G, \cdot)$ is an abelian group

Let $H = \{1, i\}$ → Yes a non-empty subset of G

Is $(H, \cdot)$ is a group ?

$\cdot$	1	i
1	1	i
i	i	-1

⇒ Colsure not Holds
⇒ $(H, \cdot)$ is not a group

Hence $(H, \cdot)$ is not a subgroup

Now, let $K = \{1, -1\} \to$ non-empty subset of G

Is $(K, \cdot)$ a group ?

$\cdot$	1	-1
1	$\boxed{1}$	-1
-1	-1	$\boxed{1}$

$\}$ in K

(1) closure ✓
(2) Asso. ✓
(3) $Id = 1 \in K$ ✓
(4) Inverse of $1 = 1$
$-1 = -1$
in K

Hence, $(K, \cdot)$ is a group.

$\therefore (K, \cdot)$ is a subgroup of G

$\cdot$	i	$-i$
i	-1	1
$-i$	1	-1

$\to$ not a group

eg: $G = \{1, \omega, \omega^2\}$
is an abelian group under multiplication

Let $H = \{1, \omega\}$

$\Rightarrow$ H is a non empty subset of G

$\cdot$	1	ω
1	1	ω
ω	ω	ω^2

not in H

But not a subgroup.

let $K = \{1\}$ → non-empty subset of G

Also, $(K, \cdot)$ is a group [∵ Id = 1, inv. of 1 = 1

Hence, $(K, \cdot)$ is subgroup of $(G, \cdot)$

Qu: G = Set of Integers, $*$ = Addition

Then $(G, +)$ is an abelian group.

even integers → $H = \{0, \pm 2, \pm 4, \pm 6, \text{------}\}$

⇒ H is non-empty subset of G

$(H, +)$ is group ?

(1) Closure: ✓ ∵ Sum of 2 even nos. is again even

(2) Asso: ✓ ∵ Addition

(3) Identity: $a + e = a = e + a$

⇒ $e = 0 \in H$ ✓

(4) Inverse: $a + b = e = b + a$

$a + (-a) = 0 = (-a) + a$

$2 + (-2) = 0$

even even

Yes ✓

Hence, $(H,+)$ is a group

$\therefore$ $(H,+)$ is subgroup of $(G,+)$

Let $\underline{\text{odd}}$ $K = \{\pm 1, \pm 3, \pm 5, \pm 7, \text{------}\}$

(1) Closure: odd + odd = even $\notin K$

$\Rightarrow$ $(K,+)$ not a group.

RESULTS: (1) Identity is unique

(2) Inverse of each element is unique

(3) A non-empty subset H of a group $(G,\cdot)$. Then H is a subgroup iff. $\boxed{ab^{-1} \in H}$ $\forall\ a, b \in H$

for Theory

(4) Intersection of two subgroups is again a subgroup.

i.e. If H, K subgroups then $H \cap K$ is also subgroup.

eg: ✓ G = set of integers, Addition $= *$

$(G, +)$ is abelian group

✓ H = even integers = Multiples of 2

✓ $H = \{0, \pm 2, \pm 4, \text{-- --}\} \rightarrow$ subgroup

Now, K = Multiples of 3 $\rightarrow$ non-empty subset of G

✓ $K = \{0, \pm 3, \pm 6, \pm 9, \text{-- ----}\}$

① closure ✓ ② Asso ✓

③ $Id = 0 \in K$ ④ Inverse ✓ $a \rightarrow -a$

$\Rightarrow (K, +)$ is a group

$\Rightarrow (K, +)$ is subgroup of $(G, +)$

Also, $H \cap K = \{0, \pm 6, \pm 12, \pm 18, \text{——}\}$

① closure ✓ ② Asso ✓

③ $Id = 0 \in H \cap K$ ④ Inverse $a \rightarrow -a$.

$\therefore (H \cap K, +)$ is subgroup of $(G, +)$

5. Union of 2 subgroups may or may not be a subgroup.

above eg: $H \cup K = \{0, \pm 2, \pm 3, \pm 4, \pm 6, \ldots\}$

1. closure: $2, 3 \in H \cup K$

$$2 + 3 = 5 \notin H \cup K$$

$\therefore$ $H \cup K$ is not a subgroup.

$(H, *) \to$ group & H is non-empty subset of G.

Then $(H, *)$ is subgroup of $(G, *)$

<u>COSETS</u>: Let $(H, *)$ be a subgroup of $(G, *)$. If $a \in G$ Then

$H * a$ right

$a * H$ left

Set $H * a = \{ h * a : h \in H \}$ is called as right coset of H in G determined by a.

<u>eg</u>: $\underline{G} = \{1, -1, i, -i\}$ is an abelian group under multiplication

$* =$ Mul.

Also, $H = \{1, -1\}$ is a subgroup of G

let $a = 1$

Right coset $H \cdot a = \{ ha : h \in H \}$

$H \cdot 1 = \{ h(1) : h \in H \}$

$$H \cdot 1 = \{h : h \in H\} = \{1, -1\}$$

Right coset for $a = -1$

$$Ha = \{ha : h \in H\}$$

$$H(-1) = \{h(-1) : h \in H\}$$

$$= \{-h : h \in H\}$$

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

Right coset for $a = i$

$$H(i) = \{h(i) : h \in H\}$$

$$= \{1(i), -1(i)\}$$

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

Right coset for $a = -i$

$$H(-i) = \{1, -1\}(-i)$$

$$= \{1(-i), (-1)(-i)\}$$

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

Sets

$\{1, 2, 3\}$
$\{3, 2, 1\}$ equal

order does not matter

Distinct Right cosets are only 2

ie. $\{1, -1\}$ & $\{i, -i\}$

i.e. $\{1, -1\}$ & $\{i, -i\}$

Union of All Distinct Right Cosets of H in G = Group G

i.e. $\{1, -1\} \cup \{i, -i\} = \{1, -1, i, -i\} = G$

Que: $G = \{1, \omega, \omega^2\}$ is abelian group under multiplication.

$1 \leftarrow \omega^3$

$\boxed{H = \{1\}}$ ✓

(1) closure: $1 \cdot 1 = 1 \in H$

(2) Asso: $1 \cdot (1 \cdot 1) = (1 \cdot 1) \cdot 1$

(3) Iden: $a \cdot e = a = e \cdot a$
$1 \cdot 1 = 1$ yes

(4) Inverse: $a \cdot b = 1 = b \cdot a$
$1 \cdot 1 = 1$ yes

Hence $(H, \cdot)$ is group

$\therefore$ $(H, \cdot)$ is subgroup of $(G, \cdot)$

$\rightarrow G = \{1, \omega, \omega^2\}$

$a \in G$, $\xrightarrow{\text{let}}$ $a_1 = 1$, $a_2 = \omega$, $a_3 = \omega^2$

Right cosets $Ha_1 = \{1\}$ 7 all Right

Right cosets $Ha_1 = \{1\}$
$Ha_2 = \{\omega\}$
$Ha_3 = \{\omega^2\}$ } all Right cosets are distinct (different)

Union of cosets $= \{1, \omega, \omega^2\} = G$

Left cosets $a_1 H = \{1\}$
$a_2 H = \{\omega\}$
$a_3 H = \{\omega^2\}$

$a \times b = b \times a$

Here, all Right cosets = left cosets

Normal Subgroup: A subgroup H of G is said to be normal if $\boxed{H * a = a * H}$ $\forall a \in G$

ie. if Right cosets = left cosets

In above examples, $H = \{1, -1\}$ is normal group as all Right & left cosets are same all Right & left cosets are same

noemal

$$\boxed{H * a = a * H} \quad \forall a \in G$$

$\underbrace{a * b = b * a}_{\text{Commutative}}$

RESULT: Every subgroup of an abelian group is always noemal.