

# **GATE CSE NOTES**

by  
**Joyoshish Saha**



Downloaded from <https://gatetcsebyjs.github.io/>

With best wishes from Joyoshish Saha

# (Group) Theory

Monday

28

- Cryptography
- Network Security
- Binary Operation (\*)

\* defined on a non empty set  $S$  as a mapping  $f : S \times S \rightarrow S$  ( $S, *$ )

$\Rightarrow \forall a, b \in S \quad a * b$  is defined.

$$f(a, b) = c \quad a, b, c \in S$$

$$\Rightarrow a * b = c$$

$\Rightarrow \forall a, b \in S \quad a * b$  is unique.

e.g.  $a * b = a + b$  on  $\mathbb{R}$  ( $\mathbb{R}, +$ )

$$\left. \begin{array}{l} a + b \in \mathbb{R} \\ \forall a, b \in \mathbb{R} \end{array} \right\}$$
 So, a valid  
 $a + b$  is unique. binary op<sup>n</sup>.

e.g.  $a * b = \sqrt{ab}$  ( $\mathbb{R}, *$ )

Essential

Job to do

Phone No.

$a, b = 1 \quad \sqrt{1} = \pm 1$	$\therefore$ So, not a binary op <sup>n</sup> .
-----------------------------------	---



As $a * b$ not unique.
------------------------

APRIL

2014

29

119-246  
18th Week

Tuesday eg  $a * b = \frac{a}{b}$  ( $R, *$ )

$\%$   $\notin R$  Not bin. op<sup>n</sup>

eg  $a * b = \frac{a}{b}$  ( $R - \{0\}, *$ )  
↳ Binary op<sup>n</sup>

### \* Properties

1. Closure :  $(S, *)$   $\forall a, b \in S, a * b \in S$

2. Associative :  $\forall a, b, c \in S$

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

3. Identity :  $\exists e \in S$  s.t.  $\forall a \in S$

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

4. Inverse :  $\forall a \in S \exists a^{-1} \in S$  s.t.

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

5. Commutative :  $a * b = b * a \quad \forall a, b \in S$

Essential

Job to do

Phone No.

T	F	S	S	M	T	W	T	F	S	S	M	T	W	T	F	S	S	M	T	W	T	F	S	
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

125-240  
19th Week

## CAIDIC

Monday

05

- Semi Group : Closure, Associative
- Monoid : Closure, Associative, Identity
- Group : Closure, Associative, Identity, Inverse
- Abelian Group : Closure, Associative, Identity, Inverse, Commutative.

### \* Group - Properties

1.  $e$  is unique. (Identity elem)

2. Left identity = Right identity

$$a * e = e * a$$

3.  $a^{-1}$  is unique  $\forall a \in S$

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

| Proof:  $(a * b)(a * b)^{-1} = e$  |  $a * b = ab$

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

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

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

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

MAY

2014

06

126-239  
19th WeekTuesday 5.  $(a^{-1})^{-1} = a$ 

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

6. Left Right cancellation allowed in group.

$$ab = ac \Leftrightarrow b = c$$

$$a^{-1}ab = a^{-1}ac \Rightarrow b = c$$

7. If  $a x = b$  $x = a^{-1}b$  is unique

$$x a = b$$

 $x = b a^{-1}$  is unique

8. Cayley's Table of a finite group has no repetitions in any row or column.

*	a	b
a	a	b
b	b	a

*	a	b
a	a	a
b	b	a

Essential

Job to do

Phone No.

(2)

S	M	T	W	T	F	S	S	M	T	W	T	F	S	S	M	T	W	T	F	S	S	M	T						
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30

155-210

23rd Week

Q1 Fill

*	a	b	c	d
Q	a	b	c	d
b	b	c	d	a
c	c	d	a	b
d	d	a	b	c

Wednesday

04

## \* Abelian Group - Properties $(G, *)$

1.  $(G, *)$  is abelian iff  $a * b = b * a \forall a, b \in G$  (commutative)
2.  $\forall a \in G \quad a^{-1} = a \Rightarrow (G, *)$  is abelian.

$$a \cdot a^{-1} = a \cdot a$$

$$a^2 = e$$

$$(ab)(ab) = e \quad \Rightarrow ababba = ba$$

$\swarrow$        $\nwarrow$

$$ba \quad ba \quad \Rightarrow abab^2a = ba$$

$$\Rightarrow abaa = ba \quad | \quad b^2 = e$$

$$\Rightarrow ab = ba$$

↓

Commutative

Essential

Job to do

Phone No.

JUNE

05

Thursday 3. A group  $G$  is Abelian iff

$$(ab)^2 = a^2 b^2 \quad \blacksquare$$

$$G \text{ is Abelian} \Leftrightarrow (ab)^2 = a^2 b^2$$

$$\begin{aligned} \text{Proof. } \Rightarrow & (ab)^2 = (ab)(ab) = a(ba)b \\ & = aabb \sim \text{Commu} \\ & = a^2 b^2 \end{aligned}$$

$$\Leftarrow (ab)^2 = a^2 b^2$$

$$(ab)(ab) = aabb$$

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

$$\Rightarrow bab = abb$$

$$\Rightarrow bab b^{-1} = abbb^{-1}$$

$$\Rightarrow ba = ab \sim \text{commute}$$

## \* Special Groups (Cryptography)

### 1. Addition Modulo $(\mathbb{Z}_m, +_m)$

Essential

Job to do

Phone No.

$$\mathbb{Z}_m = \{0, 1, 2, \dots, m-1\}$$

$$a +_m b = (a + b) \bmod m$$

S	M	T	W	T	F	S	S	M	T	W	T	F	S	S	M	T	W	T	F	S	S	M	T						
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30

162-203  
24th Week

$(\mathbb{Z}_m, +_m) \rightsquigarrow \text{Abelian group}$  Wednesday

Closure  $\checkmark e \in (0, m-1)$

Associative

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

$$= (a + b + c) \bmod m$$

Identity  $a +_m e = e +_m a = a$

$$e = 0$$

Inverse  $a +_m a^{-1} = a^{-1} +_m a = e = 0$

$$(a + a^{-1}) \bmod m = 0$$

$$\Rightarrow a^{-1} = m - a \quad \in \mathbb{Z}_m$$

$$a + a^{-1} = km$$

$$a^{-1} = km - a$$

$$k = 1$$

Commutative  $a +_m b = b +_m a$

$$(a+b) \bmod m = (b+a) \bmod m$$

Essential

Job to do

Phone No.

So, Abelian Group  $\checkmark$

JUNE

2014

12

Thursday 2. Multiplication Modulo  $(\mathbb{Z}_m, \times_m)$

163-202  
24th Week

Often defined on prime numbers.

$$\mathbb{Z}_m \{1, 2, \dots, m\}$$

$$\text{or } (\mathbb{Z}_p, \times_p)$$

$$\mathbb{Z}_p \{1, 2, \dots, p\} \quad p \text{ is prime}$$

$$a \times_p b = (a \times b) \bmod p \quad \text{identity} = 1$$

When  $p$  is prime number  $(\mathbb{Z}_p, \times_p)$  is an Abelian Group.

3. Permutation (Group)

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

$$f: \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}^{\text{IP}}$$

$S$  = Set of all permutation  $f^n$ s on  $A$ .

$$|S| = 3! = 6 \quad S = \{f_1, \dots, f_6\}$$

$(S, \circ)$   $\rightarrow$  Composition operator  $f \circ g = f(g())$

$$\bullet \text{ identity} = \ell = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}$$

Essential

Job to do

Phone No.

$$f_1 \left( \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}^{-1} \right) = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} | f_1^{-1}$$

inverse

(3)

S	M	T	W	T	F	S	S	M	T	W	T	F	S	S	M	T	W	T	F	S	S	M	T						
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30

157-208  
23rd Week

Friday

06

Commutative

$$\begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} ? = f_2 \circ f_1$$

$f_1$                        $f_2$

$$\begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} \neq \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$$

So, not an Abelian group. ■\* Powers of an element ( $a$ ) in Group  $(G, *)$ 

■  $a \in G$      $\underline{n \in \mathbb{Z}}$      $a^n$

$$\boxed{a^0 = e} \quad a^1 = a \quad a^2 = a * a \quad \dots$$

$$a^{-1} = \text{inv}(a) = (a)^{-1} \quad | \quad a^{1.5} \text{ not defined}$$

✓  $a^{-2} = (a^2)^{-1} = \text{inv}(a^2)$      $\rightarrow$  not  $(a^{-1})^2$   
 $\cdot (a^m)^n = a^{mn}$      $(\text{inv}(a))^2$

$$a^m \cdot a^n = a^{m+n}$$

\* Order of a Group  $(G, *)$ 

Essential	Job to do	Phone No.
order	$\leftarrow o(G) =  G  \quad \# \text{elements in } G$ Can be $\infty$	

07

Saturday

158-207  
23rd WeekOrder of an element  $a \in G$ 

$\circ(a) = \text{smallest } n \in \mathbb{Z} \text{ such that}$   
 can be  $\infty$

$$a^n = e$$

eg	*	a b c d	$e = a^1$
	a	a b c d	
✓	b	b c d a	$\circ(a) = 1$ as $a^1 = e$
	c	c d a b	$\circ(b) = 4$ as $b^4 = e$
	d	d a b c	$\circ(c) = 2$
			$\circ(d) = 1$
			$b * b = e$
			$b * e = d$
			$b * d = a$
		$\circ(G) = 4$	

08 Sunday

$$\Rightarrow \circ(a) \leq \circ(G) \quad a \in G$$

$\Rightarrow \circ(a)$  divides  $\circ(G)$  for finite group

$\Rightarrow$  for finite group,  $\circ(a)$  exists & finite

$\Rightarrow \circ(G) = \text{prime} \Rightarrow p$  implies



Identity  $\leftarrow \circ(a) = 1 \text{ or } p$

$\circ(e) = 1 \quad \circ(a) = p \quad \forall a \in G, a \neq e$

Essential

Job to do

Phone No.

$\Rightarrow \circ(a * b) = \circ(b * a)$  for all groups

$$\circ(ab) = n \Leftrightarrow (ab)^n = e$$

S	M	T	W	T	F	S	S	M	T	W	T	F	S	S	M	T	W	T	F	S	S	M	T						
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30

160-205  
24th Week

Monday

09

$$ab \underbrace{ab ab \dots ab}_{n \text{ times}} = e$$

↓

$$a(ba)^{n-1} b = e$$

$$(ba)^n = e$$

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

$$\Rightarrow (ba)^{n-1} = (ba)^{-1}$$

$$\Rightarrow (ba)^n = e. \quad \blacksquare \quad (ab)^n = e = (ba)^n$$

## ※ Cyclic Group

A group  $(G, *)$  iff  $\exists g \in G$  s.t.  $\blacksquare$

$$\forall a \in G, a = g^n \quad n \in \mathbb{Z}$$

→ Multiple  $g$ 's may exist.  $g_2$

generator

$$\text{eg } (\mathbb{Z}, +) \quad g = +1, -1 \quad e = 0$$

$$0 = 1^0 \text{ or } (-1)^0$$

Essential	$1 = 1^1$	Job to do	$-1 = (-1)^1$	Phone No.
-----------	-----------	-----------	---------------	-----------

$$2 = 1+1 = 1^2 \quad | \quad -2 = (-1)^2$$

$$3 = 1+1+1 = 1^3$$

10

- Tuesday •  $e$  cannot be the generator.

unless  $e$  is the only element in  $G$ .

- If  $g$  is a generator,  $g^{-1}$  is also a generator.

proof  $\forall a, a = g^n \Rightarrow a = (g^{-1})^{-n} \quad n \in \mathbb{Z}$

- A cyclic group is always Abelian.



$$\forall a, b \quad a = g^n \quad b = g^m \quad n, m \in \mathbb{Z}$$

$$ab = g^{n+m} = g^m \cdot g^n = ba$$

An Abelian grp need not be cyclic.  
 $(\mathbb{R}, +)$

- A non-abelian group is always non-cyclic.

e.g.  $(\mathbb{Z}_m, +_m)$  Addition modulo group is cyclic.

$$g = 1, m-1$$

Essential

Job to do

Phone No.


F	S	S	M	T	W	T	F	S	S	M	T	W	T	F	S	S	M	T	W	T	F	S	S	S						
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31

213-152  
31st Week



(4)

0 |

eg  $*$  | a b c d

Friday

a | a b c d

$$g = ?$$

b | b c d a

$$d = ?$$

c | c d a b

$$\begin{cases} a^1 = a \\ a^2 = a \cdot a = a \end{cases}$$

$$e = a$$

d | d a b c

$$\begin{cases} a^3 = a \\ a^n = a \end{cases}$$

$$\left\{ \begin{array}{l} b^1 = b \\ b^2 = b \cdot b = c \\ b^3 = b \cdot b \cdot b = c \cdot b = d \\ b^4 = d \cdot b = a \end{array} \right.$$

$$\begin{cases} g = b \\ g = d \end{cases}$$

Inv(b)

$$b * x = x * b = a$$

$$x = d$$

$$\begin{cases} g = d \\ g = b \end{cases}$$

Inv(c)

$$c * x = x * c = a$$

$$x = c$$

$$\left\{ \begin{array}{l} c^1 = c \\ c^2 = c \cdot c = a \\ c^3 = a \cdot c = c \\ c^4 = c \cdot c = a \end{array} \right.$$

X

Generators are b, d.

Also, as generator exists, it's a cyclic group.

Essential

Job to do

Phone No.

AUGUST

02

Saturday

\* Property - Cyclic group

1. For every group having order = prime #  
then it's cyclic.

$$o(G) = \text{Prime no.}$$

$$\text{generator} = G - \{e\}$$

2.  $(G, *)$  is cyclic  $\Leftrightarrow \exists a \text{ s.t. } o(a) = o(G)$

$$\phi(n) \quad \text{Euler Totient F^n}$$

$\hookrightarrow$  # generators of a cyclic group of order n

03 Sunday

$$\phi(n) = n-1 \text{ if } n \text{ is prime}$$

If n is not prime then we use concept of prime factorization.

$$n = p_1^{m_1} p_2^{m_2} p_3^{m_3} \dots$$

eg If  $n = 60 = 2^2 \cdot 3^1 \cdot 5^1$

$$\begin{aligned} \phi(n) &= (p_1^{m_1} - p_1^{m_1-1}) (p_2^{m_2} - p_2^{m_2-1}) \dots \\ &= (2^2 - 2^1) (3^1 - 3^0) (5^1 - 5^0) \\ &= 16 \end{aligned}$$

F	S	S	M	T	W	T	F	S	S	M	T	W	T	F	S	S	M	T	W	T	F	S	S							
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31

216-149  
32nd Week

✓  $(n = p^1 \quad \phi(n) = p^1 - p^0 = n - 1)$  Monday

04

Again,  $\phi(n) = \# \text{integers } i \text{ (from 1 to } n) \text{ s.t. } \gcd(i, n) = 1$

$\phi(60) \rightarrow \underbrace{1, \dots, 60}$

relatively prime id n

16 relatively primes of 60

3. If  $g_1, g_2, \dots, g_k$  are generators of cyclic group of order  $n$ , then  $g_i = g_j^x \wedge g_i, g_j$

4.  $\text{o}(g_i)$  is a relative prime of  $\text{o}(G)$ .

\* Subgroup  $(G, *) \hookrightarrow (H, *)$

STRATEGIC PLANNING  
ORGANIZATION

$(H, *)$  is a subgroup of  $(G, *)$  iff

- i)  $H \subseteq G$
- ii)  $(H, *)$  is also group.

e.g.  $\{\text{id}, *\}$  is a trivial subgroup of  $(G, *)$

Essential

Also,

Job to do

Phone No.

$(G, *)$  subgroup of  $(G, *)$

AUGUST

2014

05

Tuesday

217-148  
32nd Week

eg Non trivial subgroup.

$(\mathbb{Z}_4, +_4)$  Addition modulo 4  
 $\downarrow \{0, 1, 2, 3\}$

$(\{0, 2\}, +_4)$  ? subgroup or not  
 $\downarrow$  group?

$$0 +_4 0 = 0$$

$$0 +_4 2 = 2$$

$$2 +_4 2 = 0$$

Closure ✓

Similarly,

Associative, Identity, Inverse

So, a group.

Hence, subgroup of  $(\mathbb{Z}_4, +_4)$

\* Subgroup - Properties

1.  $A \subseteq G ; B \subseteq G$

If A and B are subgroups of G, then  $A \cap B$  is

also a subgroup.

$A \cup B$  need not be a subgroup

eg  $A = (\{0, 2\}, +_4)$

$B = (\{0, 1\}, +_4)$

$(\mathbb{Z}_4, +_4)$

$A \cup B = (\{0, 1, 2\}, +_4)$

$1 + 2 = 3$  not closed!

not subgroup.

Essential

Job to do

Phone No.

F	S	S	M	T	W	T	F	S	S	M	T	W	T	F	S	S	M	T	W	T	F	S	S	S						
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31

218-147  
32nd Week

# \* Lagrange's Theorem

Wednesday

06

$\circ(H)$  divides  $\circ(G)$  where  $H$  is a subgroup of  $(G, *)$

2. If  $|G| = \text{prime}$ ,  $\circ(G) = p^1$  <sup>no proper</sup> <sub>subgroup</sub>

✓ 3. If  $(H, *), (K, *)$  are subgroups of  $(G, *)$  then  $(HK, *)$  is also a subgroup.  $(H \cap K, *)$  need not be.

✓ 4. If  $(H, *), (K, *)$  are subgroups of  $(G, *)$

$$\boxed{\begin{matrix} HK \\ \text{set name} \end{matrix}} = \left\{ h * k \mid h \in H, k \in K \right\}$$

then  $(HK, *)$  is also a subgroup.

✓ 5.  $\circ(HK) = \frac{\circ(H) \cdot \circ(K)}{\circ(H \cap K)}$

$$\circ(H \cap K) \leq \circ(H)$$

$$\circ(HK) \mid \circ(H)$$

Job to do

Phone No.

$$\circ(H \cap K) \leq \circ(K)$$

$$\circ(HK) \mid \circ(K)$$

$$\circ(H \cap K) \mid \circ(H)$$

$$\circ(H \cap K) \mid \circ(K)$$

AUGUST

201  
21  
32nd

07

Thursday

\* Subgroup ~ Alternate def<sup>n</sup>.

If \* is a binary operator on set H,

$(H, *)$  is a subgroup of  $(G, *)$  if

(i)  $H \subseteq G$

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

From here we can prove

H is a group.

Essential

Job to do

Phone No.

(2)

## Groups

### \* Algebraic structure.

A nonempty set  $S$  is called an algebraic structure wrt binary operation  $*$  if  $(a * b) \in S$   $\forall a, b \in S$  i.e.  $*$  is closure operation on  $S$ .

e.g.  $S = \{1, -1\}$

$$* \rightarrow x$$

$(S, *)$  is an algebraic structure.

e.g.  $S = \{a, b\}$ .

$(P(A), U)$  is an algebraic structure.

e.g.  $R = \{\text{reflexive relations}\}$

$(R, U), (R, \cap)$  are as.

### \* Semi Group.

An algebraic structure  $(S, *)$  is called a semigroup if  $(a * b) * c = a * (b * c) \forall a, b, c \in S$  i.e.  $*$  is associative on  $S$ .

e.g.  $(N, *) \rightarrow AS \rightarrow \text{Semigroup}$

$(N, +) \rightarrow AS \rightarrow \text{Semigroup}$

$(Z, -) \rightarrow AS \rightarrow \text{Not a semigroup}$

$(Q^*, +) \rightarrow \text{Not AS} \quad a + (-a) = 0 \notin Q^*$

$(Q^*, *) \rightarrow AS \rightarrow \text{Semigroup}$

$(P(A), U) \rightarrow AS \rightarrow \text{Semigroup}$

$(P(A), \cap) \rightarrow AS \rightarrow \text{Semigroup}$

\* Monoid : A semigroup  $(S, *)$  is called a monoid if there exists an element  $e \in S$  such that  $(a * e) = (e * a) = a \quad \forall a \in S$ .

The element  $e$  is called identity element of  $S$  wrt  $*$ .

e.g.  $(\mathbb{N}, *) \rightarrow AS, SG \rightarrow e = 1$  Monoid

$(\mathbb{N}, +) \rightarrow AS, SG \rightarrow e = 0 \in \mathbb{N}$  Not Monoid.

$(\mathbb{Z}, +) \rightarrow AS, SG \rightarrow e = 0 \in \mathbb{Z}$  Monoid

$(P(A), U) \rightarrow AS, SG \rightarrow e = \emptyset \in P(A)$  Monoid

\* Group : A monoid  $(S, *)$  with identity element  $e$  is called a group if to each element  $a \in S$ , there exists an element  $b \in S$ , such that  $(a * b) = (b * a) = e$ , The  $b$  is called the inverse of element  $a$ , denoted as  $a^{-1}$ .

e.g.  $(\mathbb{Z}, +) \quad a + (-a) = 0 \rightarrow$  Group

w  $\left\{ \begin{array}{ll} (\mathbb{Q}, \cdot) & a \cdot \frac{1}{a} = 1 \mid a=0 \Rightarrow \frac{1}{a} \notin \mathbb{Q} \text{ Not Group} \\ (\mathbb{Q}^*, \cdot) & a^{-1} = \frac{1}{a} \quad \text{Group} \end{array} \right.$

$(P(A), U) \quad e = \emptyset \quad$  Not Group

\* In a group  $(G, *)$ , following hold good —

1. The identity element of  $G$  is unique.
2. The inverse of any element in  $G$  is unique.
3. The inverse of identity element  $e$  is  $e$  itself.
4. Cancellation laws.

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

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

$$5. \quad (a * b)^{-1} = b^{-1} * a^{-1} \quad \forall a, b \in G$$

## \* Abelian Group. (Commutative Group)

A group  $(G, *)$  is said to be abelian if

$$(a * b) = (b * a) \quad \forall a, b \in G.$$

e.g.  $(\mathbb{Z}, +)$        $a + b = b + a$     Abelian

$$(\mathbb{R}^*, \cdot) \quad a \cdot b = b \cdot a \quad \text{Abelian}$$

$$(\mathbb{M}, *) \rightarrow \text{AS} \rightarrow \text{SG} \rightarrow \text{Monoid} \rightarrow \text{Group}$$

$\downarrow$   
 $AB \neq BA$

set of all non-singular  
matrices.      Not Abelian Group

Q Which is/are true?

I. In a group  $(G, *)$  with an identity element 'e' if  
 $a * a = a$  then  $a = e$

II. In a group  $(G, *)$ , if  $a^{-1} = a \quad \forall a \in G$ , then  $G$  is  
abelian group.

III. In a group  $(G, *)$ , if  $(a * b)^2 = a^2 * b^2 \quad \forall a, b \in G$   
then  $G$  is abelian group.

$\rightarrow$  I.  $a * a = a.$

$$\Rightarrow a * a = a * e.$$

$$\Rightarrow a = e.$$

II.  $a^{-1} = a.$

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

$$\Rightarrow a * b = b * a \quad [\because a^{-1} = a]$$

III.  $a^2 \approx a * a$

$$(a * b)^2 = \underline{(a * b) * (a * b)} = a^2 * b^2 = \underline{a * a * b * b}$$

$$\Rightarrow a * (b * a) * b = a * a * b * b$$

$$\Rightarrow b * a = a * b.$$

$$a * b = a^{-1} * b^{-1}$$

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

$$= b * a$$

Q. If  $A = \{1, 3, 5, 7, \dots\}$  &  $B = \{2, 4, 6, \dots\}$  Which is a semigroup?

- a)  $(A, +)$       c)  $(B, +)$   
 ✓ b)  $(A, \cdot)$       d)  $(B, \cdot)$

$$\rightarrow a) 1+3=4 \notin A$$

b) Closure & associativity ✓

c) ✓ d) ✓

Alg. Str.	→ Closure
SemiG	→ Associativity
Monoid	→ Identity element $a * e = e * a = a$
Group	→ Inverse $a * b = b * a = e$
Abelian	→ Commutative $a * b = b * a$ .

Q.  $A = \{1, 2, 3, 4, \dots\}$  & a binary operation  $*$  is defined by  $a * b = a^b \forall a, b \in A$ . Which's T?

- a)  $(A, *)$  is semigroup but not monoid.  
 b)  $(A, *)$  is a monoid but not a group.  
 c)  $(A, *)$  is a group.  
 ✓ d)  $(A, *)$  is not a semi group.

$$\rightarrow a * b = a^b. \quad \text{Closure} \quad ((a * b) * c) ? = (a * (b * c))$$

$$(a^b)^c \quad a * b^c \\ a^{bc} \neq a^{b^c} \quad \text{Not semigroup.}$$

Q. Let  $A = \{x \mid 0 < x \leq 1\}$  and  $x$  is a real number } then  $A$  wrt multiplication is ~

- a) A semigroup but not monoid  
 ✓ b) A monoid but not a group  
 c) A group  
 d) Not a semigroup.

$$\rightarrow \text{Closure} \quad \text{Associative} \quad \text{Monoid} \\ \checkmark 0 \cdot 1 \Rightarrow \frac{1}{0 \cdot 1} \text{ Not a group}$$

Q Let  $A$  is set of all integers & a binary operation ' $*$ ' is defined by  $(a * b) = \min(a, b)$ , then  $(A, *)$  is Semigroup.

→ Closure property ✓

Associativity ✓

$$(a * b) * c \stackrel{?}{=} a * (b * c)$$

$$\min(\min(a, b), c) \quad a * \min(b, c)$$

$$\min(a, b, c) \quad \min(a, b, c)$$

Identity element

$$a * e = a. \quad \times$$

Q.  $S$  be set of all bit strings including the null string ' $\epsilon$ '. '+' denotes string concatenation.

$$(S, +) \text{ is } S = \{\epsilon, 0, 1, 00, 01, \dots\} \quad \underline{\text{Monoid}}$$

→ Closure ✓

Associative ✓

$$(a * b) * c \stackrel{?}{=} a * (b * c).$$

$$abc \quad abc.$$

Identity element.  $\epsilon. \quad \checkmark$

$$\text{Inverse } a + b = \epsilon \quad \times$$

Q Let  $A$  = set of all +ve rational numbers & a binary operation ' $*$ ' is defined as  $(a * b) = \frac{ab}{3} \forall a, b \in A$ .

a)  $(A, *)$  is group      Closure ✓

b) identity is 3      Associative ✓

c) inverse of  $a$  is  $\frac{3}{a}$

$$\frac{ab}{3} * c \stackrel{?}{=} a * \frac{bc}{3}$$

identity element ✓

$$\frac{abc}{9} \quad \frac{abc}{9}$$

$$a * e = a \Rightarrow e = 3.$$

inverse element. ✓

$$a * b = e \Rightarrow b = \frac{9}{a}$$

Q.  $A = \text{set of all real numbers}$ . \* be a binary operation  $(a * b) = a + b + ab$  then which's true?

1.  $(A, *)$  is a group.

2. Identity element is  $-1$ .

3. Inverse of  $2 = -\frac{2}{3}$

→ Closure ✓

Associative. ✓

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

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

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

Identity element ✓

$$a * e = a \Rightarrow a + e + ae = a \Rightarrow e(1+a) = 0$$

$$e = 0$$

Inverse. ✗

$$a * b = e \Rightarrow a + b + ab = 0 \Rightarrow b(1+a) = -a$$

$$b = \frac{-a}{1+a} \quad \text{for } a = \neq -1, \frac{1}{0}$$

$$\text{Inverse of } 2 \text{ is } -\frac{2}{3}$$

Q. Which is not a group?

a)  $\{0, \pm 2, \pm 4, \dots\}$  wrt '+'

b)  $\{0, \pm k, \pm 2k, \dots\}$  wrt '+'

c)  $\{2^n \mid n \text{ is an integer}\}$  wrt multiplication

d) set of all complex numbers wrt multiplication

→ a) group      b) group      c) Closure ✓

associative ✓

$$2^a * (2^b * 2^c) = (2^a * 2^b) * 2^c$$

identity ✓

$$2^0 * 2^0 = 2^0$$

$$2^{-1} = 2^1$$

group.

d)  $a+ib$ .

closure ✓

associative ✓

identity ✓

inverse ✗

$$(a+ib)^{-1} = \frac{1}{a+ib}$$

$$\begin{cases} a=0 \\ b=0 \end{cases} \quad X$$

## \* Finite Group.

A group with finite no. of elements.

$O(G) \rightarrow$  order of finite group.

✓ eq.  $(\{0\}, +)$        $(\{1, -1\}, *)$        $(\{1, -1, i, -i\}, *)$

$(\{i\}, *)$        $(\{1, \omega, \omega^2\}, *)$

Composition table

	1	-1
1	1	-1
-1	-1	1

Check properties  
on this

✓ eq.  $(\{0, 1, 2, \dots, (m-1)\}, \oplus_m)$  |  $\oplus_m$ : addition modulo m

\*  $a \oplus_m b = \begin{cases} (a+b) < m \Rightarrow a+b \\ (a+b) > m \Rightarrow (a+b) \% m. \end{cases}$

✓ eg.  $(S_m, \otimes_m)$        $\otimes_m = (a \times b) \% m$

\*  $S_m$  - Set of +ve integers  $< m$   
& relatively prime to m

$(S_{10} = \{1, 3, 7, 9\}, \otimes_{10})$

Q. If  $G = \{1, 3, 5, 7\}$  is a group wrt  $\otimes_8$ , which isn't true?

a) Inverse of 1 is 1      ✓ Inverse of 5 is 7

b)  $1 \otimes_8 3 = 3$       d)  $1 \otimes_8 7 = 7$ .

→  $1 \otimes_8 1 = 1$        $5 \otimes_8 5 = 1$  ✓

$3 \otimes_8 3 = 1$        $7 \otimes_8 7 = 1.$

Q. Which is a group?

a)  $\{1, 2, 3, 4, 5\}$  wrt  $\otimes_6$

b)  $\{0, 1, 2, 3, 4, 5\}$  wrt  $\otimes_6$

c)  $\{1, 2, 3, 4, 5, 6\}$  wrt  $\otimes_7$

d)  $\{1, 2, 3, 4, 5, 6\}$  wrt  $\otimes_7 \oplus_7$

$$\left\{ \begin{array}{l} \otimes_m = S_m \\ \oplus_m = \{0, \dots, m-1\} \end{array} \right.$$

finite groups

## \* Order of an element of a group.

Let  $(G, *)$  be a group, and  $a \in G$ , then order of element 'a' is the smallest +ve integer  $n$  such that  $a^n = e$  element 'a' is identity element.

e.g.  $(\{1, -1\}, *)$        $I = 1$ .

Order of identity element always 1.

Order of  $1 = 1$

Order of  $-1 = 2$

e.g.  $(\{1, \omega, \omega^2\}, *)$        $I = 1$

Order of group - #elems in group.

$O(1) = 1$

$O(\omega^2) = 3$

$O(\omega) = 3$

→ Order of any element (of finite group)  
always divides order of the group.

e.g.  $(\{0, 1, 2\}, \oplus_3)$        $I = 0$

$1 \oplus_3 2 = 0$

$O(0) = 1$

$O(1) = 3$

$O(2) = 3$

→ Orders of  $a$  and  $a^{-1}$  are same.

Q. T/F.

1) In a group  $(\mathbb{Z}, +)$ , order of any element except 0 does not exist. F

2. In the group  $(\mathbb{Q}^*, \cdot)$ , where  $\mathbb{Q}^*$  is a set of all non zero rational numbers, order of any element except 1 does not exist. F

↳ exists for  $1, -1$

\* Subgroup.

$(G, *)$  be a group. A subset  $H$  of  $G$  is a subgroup of  $G$  if  $(H, *)$  is a group.

e.g. Let  $(G, *)$  be a group with identity element  $e$ , then  $\{e\}$  and  $G$  are the trivial subgroups of ' $G$ '.

Any subgroup that is not a trivial subgroup is called proper subgroup.

e.g.  $G = (\{1, -1, i, -i\}, *)$  then

$H = (\{1, -1\}, *)$  is a proper subgroup.

Th. Let  $H$  be a nonempty subset of a group  $(G, *)$ .

$H$  is a subgroup of  $G$  iff  $a * b^{-1} \in H \forall a, b \in H$ .

Th. Let  $H$  be a nonempty finite subset of a group

$(G, *)$ .  $H$  is a subgroup of  $G$  iff  $(a * b) \in H \forall a, b \in H$ .

Th. Lagrange's theorem.

If  $H$  is a subgroup of finite group  $(G, *)$ , then  $O(H)$  is the divisor of  $O(G)$ . The converse of the above theorem need not be true.

Q.  $G = (\{0, 1, 2, 3, 4, 5\}, \oplus_6)$  is a group. Which is/are subgroup?

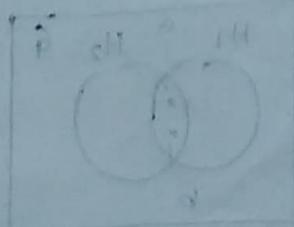
x a)  $H_1 = \{1, 3\}$  ✓ d)  $\{0, 2, 4\}$

x b)  $\{1, 5\}$  x e)  $\{0, 2, 3, 5\}$ . 4 does not divide 6.

✓ c)  $\{0, 3\}$

→ a)  $\begin{array}{c|cc} & 1 & 3 \\ \hline 1 & & 2 \\ 3 & & 1 \end{array}$  b)  $\begin{array}{c|cc} & 1 & 5 \\ \hline 1 & & 2 \\ 5 & & 1 \end{array}$  c)  $\begin{array}{c|cc} & 0 & 3 \\ \hline 0 & & 3 \\ 3 & & 0 \end{array}$

d)  $\begin{array}{c|ccc} & 0 & 2 & 4 \\ \hline 0 & & 2 & 4 \\ 2 & & 4 & 0 \\ 4 & & 0 & 2 \end{array}$



$$\text{Q. } G = (\{1, 2, 3, 4, 5, 6\}, \otimes_7)$$

Which are subgroups?

~~a)~~  $H_1 = \{1, 6\}$   $\times_c) \{1, 3, 5\}$

~~b)~~  $\{1, 2, 4\}$   $\times_d) \{1, 2, 3, 5\}$  4 doesn't divide 6

$$\rightarrow \begin{array}{c|cc} & 1 & 6 \\ \hline 1 & 1 & 6 \\ 6 & 6 & 1 \end{array}$$

$$\begin{array}{c|cccc} & 1 & 2 & 4 \\ \hline 1 & 1 & 2 & 4 \\ 2 & 2 & 4 & 1 \\ 4 & 4 & 1 & 2 \end{array}$$

$$\begin{array}{c|ccc} & 1 & 3 & 5 \\ \hline 1 & 1 & 3 & 5 \\ 3 & 3 & 2 & \\ 5 & & & \end{array}$$

Q.  $(G, *)$  be a group of order  $p$  where  $p$  is a prime no, then the no. of proper subgroups of  $G$  is  $0$ .

$$\rightarrow O(G) = p$$

$$O(H) \rightarrow 1/p$$

Q. T/F.

\* \* \* 1. Union of any 2 subgroups of  $G$  is also a subgroup of  $G$ .  $\text{(F)}$

\* 2. Intersection of any 2 subgroups of  $G$  is also a subgroup of  $G$ .  $\text{(T)}$

3. Union of 2 subgroups  $H_1$  &  $H_2$  of a group  $(G, *)$  is also a subgroup of  $G$ .  $\text{(F)}$

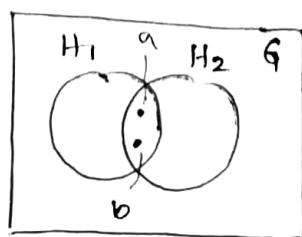
4. Every subgroup of an abelian group is also an abelian group.  $\text{(T)}$

$$\rightarrow 1. (S_8, \otimes_8) = (\{1, 3, 5, 7\}, \otimes_8)$$

$(1, 3), (1, 5)$  subgroups.

$(1, 3) \cup (1, 5) = (1, 3, 5)$  Not a subgroup.

2.

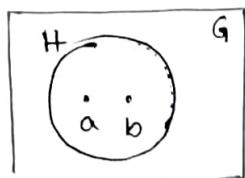


$$a * b \in H_1$$

$$a * b \in H_2$$

$$a * b \in H_1 \cap H_2$$

4.



$$a * b = b * a$$

Q If  $(G, *)$  is a cyclic group with generator 'a'

Theorem

\*\* then

\* (i)  $a^{-1}$  is also a generator T

(ii) Order of generator =  $O(G)$ . T

Cyclic group : A group  $(G, *)$  if there exists an element  $a \in G$  s.t. every element of  $G$  can be written as  $a^n$  for some integer  $n$ . Then  $a$  is called generating element /generator.  
 Eg  $(\{1, -1\}, *)$   $(-1)^1 = -1$   $(-1)^2 = 1$   
 $(\{1, \omega, \omega^2\}, *)$ ,  $(\{1, -1, i, -i\}, *)$ .  
 $(\{0, 1, 2, 3\}, \oplus_4)$   
 ↴ inverses

→  $(\{0, 1, 2, 3\}, \oplus_4)$

$$\begin{array}{llll} 1^1 = 1 & 1^2 = 2 & 1^3 = 3 & 1^4 = 0 \\ 3^1 = 3 & 3^2 = 2 & 3^3 = 1 & 3^4 = 0 \end{array} \quad O(1) = O(G).$$

Th. Let  $(G, *)$  be a cyclic group of order  $n$  with generator 'a' then  
 no. of relatively primes  $\phi(n)$   $\phi(7) = 6$   $\phi(3) = 2$

- \* i) No. of generators in  $G = \phi(n)$ , Euler's function of  $n$   
 ii)  $a^m$  is also a generator of  $G$  if  $\text{GCD}(m, n) = 1$ .  
 ( $m, n$  relatively prime)

Q.  $(G, *)$  be a cyclic group of order 8 with generator a.

- i) No. of generators in  $G = ?$   
 ii) Which isn't a generator of  $G$ ?  
 ✓ a)  $a^2$    b)  $a^3$    c)  $a^5$    d)  $a^7$

•  $\phi(77) = \phi(7) \cdot \phi(11)$   
 $= 6 \times 10 = 60$

•  $\phi(n) = \phi(p) \phi(q)$   
 when  $n = p \cdot q$ .  
 $p, q$  primes

No. of generators 60.

•  $\phi(35) = \phi(7) \phi(5) = 24$ .

$$\rightarrow \phi(p^n) = p^n - p^{n-1}$$

✓ eg.  $\phi(25) = \phi(5^2) = 5^2 - 5^1 = 20$

$\rightarrow$  eg.  $24 = 2^2 \times 3 \times 7$   
 $= \phi(2^2) \phi(3) \phi(7)$   
 $= (2^2 - 2^1) \times 2 \times 6 = 24$ .

Q. Find out generators.

1.  $(\{1, 2, 3, 4, 5, 6\}, \otimes_7)$

2.  $(\{0, 1, 2, 3, 4\}, \oplus_5)$

3.  $(\{1, 3, 5, 7\}, \otimes_8)$

$\rightarrow 1. \phi(6) = 2$

$S_6 = \{1, 5\}$  (Check till ~~4, 5, 6~~ 3, because

$2^1 = 2$

$2^2 = 4$

$2^3 = 1$

↓

2 can't be a gen<sup>r</sup>

order of group = order of generator

$(\text{gen}^n)^n = \text{Identity}$

Here 1.

$3^1 = 3, 3^2 = 2, 3^3 = 3^2 \times 3 = 2 \times 3 = 6,$

$3^4 = 4, 3^5 = 5, 3^6 = 1.$

3 is a generator.

It's a cyclic group.  $\Rightarrow 3^1$  &  $3^5$  are gen's.

3 and 5 are gen's.

2.  $S_5 = \{1, 2, 3, 4\} \Rightarrow \phi(5) = 4$

$1^1 = 1, 1^2 = 2, 1^3 = 3, 1^4 = 4, 1^5 = 0$

1 is a gen<sup>r</sup>  $\Rightarrow$  It's a cyclic group

$1^1, 1^2, 1^3, 1^4$  are gen's

1, 2, 3, 4 are gen's

3.  $(\{1, 3, 5, 7\}, \otimes_8)$ .

$$S_4 = \{1, 3\} \cancel{\times} \cancel{\times}$$

$$5^1 = 5$$

$$5^2 = 1$$

$$3^1 = 3 \Rightarrow 3 \text{ isn't genr}$$

$$\begin{array}{c} 7^1 = 7 \\ 7^2 = 1. \end{array}$$

Not a cyclic group.

$$3^2 = 1.$$

No generators.

\* For cyclic groups, following properties hold good.

\* \* 1. Every cyclic group is abelian group. (Converse not true always)

$$a * b = g^n * g^m = g^{m+n} = g^m * g^n = b * a$$

✓ 2. Every group of prime order is cyclic & so

every group of prime order is abelian group.

3. Every subgroup of a cyclic group is also cyclic, but the generator of the subgroup need not be same as that of the cyclic group.

e.g.  $G = \{1, -1, i, -i\}$ ;  $H = \{1, -1\}$ . So,  $H$  is a sub-group of  $G$ .

gen's of  $G \Rightarrow i, -i$

gen' of  $H \Rightarrow -1$

✓ 4. Let  $(G, *)$  be a group of even order, then there exists at least one element  $a \in G$  ( $a \neq e$ ) such that  $a^{-1} = a$ .

$$( \overset{\text{identity}}{\underset{\text{identity}}{\underset{\uparrow}{a}}, \underset{\uparrow}{b}, \underset{\uparrow}{c}, \underset{\uparrow}{d}} )$$