GATE CSE NOTES

by

UseMyNotes

Group Theory

Monday 28

- Cryptography
- Network Security

- **Binary Operation (*)**

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

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

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

$\Rightarrow \quad a * b = c$

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

eg $a * b = a + b$ on $\mathbb{R}$ $(\mathbb{R}, +)$

$a + b \in \mathbb{R} \quad \forall a, b \in \mathbb{R}$

$a + b$ is unique.

} So, a valid binary op^n.

eg $a * b = \sqrt{ab}$ $(\mathbb{R}, *)$

$a, b = 1 \quad \sqrt{1} = \pm 1$

So, not a binary op^n.

As $a * b$ not unique.

29 Tuesday

eg $a * b = a/b$ $(\mathbb{R}, *)$

$0/0 \notin \mathbb{R}$ Not bin. op^n

eg $a * b = a/b$ $(\mathbb{R} - \{0\}, *)$

↳ Binary op^n

✻ 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 : $a * b = b * a$ $\forall a, b \in S$

Essential	Job to do	Phone No.

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

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

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

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

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

Essential bob to do Phone No.

06 Tuesday 5. $(a^{-1})^{-1} = a$

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

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

If $xa = b$

$x = ba^{-1}$ is unique.

8. A cayley's table of a finite group has no repetitions in any row or column.

Cayley's Table

*	a	b
a	a	b
b	b	a

*	a	b
a	a	a
b	b	a

X

Essential | Job to do | Phone No.

Q1 Fill

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

Abelian Group – Properties $(G, *)$

1. $(G, *)$ is abelian iff $a * b = b * a \quad \forall a, b \in G$ (Commutative)

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

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

$$a^2 = e$$

$$(ab)(ab) = e \Rightarrow abab\,ba = ba$$

(ba ↖ ↗ ba)

$$\Rightarrow ab\,a\,b^2a = ba$$

$$\Rightarrow abaa = ba \mid b^2 = e$$

$$\Rightarrow ab = ba$$

↓

Commutative

Essential	Job to do	Phone No.

3. A group G is Abelian iff $(ab)^2 = a^2b^2$

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

Proof. $\Rightarrow$ $(ab)^2 = (ab)(ab) = a(ba)b$
$= aabb \sim$ Commu
$= a^2b^2$

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

$(ab)(ab) = aabb$

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

$\Rightarrow$ $bab = abb$

$\Rightarrow$ $bab\,b^{-1} = abb\,b^{-1}$

$\Rightarrow$ $ba = ab$ ~ commute

✱ Special Groups (Cryptography)

1. Addition Modulo $(Z_m, +_m)$

Essential | Job to do | Phone No.

Z_m $\{0, 1, 2, \cdots, m-1\}$

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

162-203
24th Week

Wednesday

$(Z_m, +_m) \rightsquigarrow$ Abelian group

$+_m$	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

$m =$

Closure ✓ $\in (0, m-1)$

Associative

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

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

Identity $\quad a +_m e = e +_m a = a$

$$e = 0$$

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

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

$$\Rightarrow \quad a^{-1} = m - a \in Z_m$$

$$a + a^{-1} = k\,m$$

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

$$k = 1$$

Commute $\quad a +_m b = b +_m a$

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

Essential | Job to do | Phone No.

So, Abelian Group ✓

12 Thursday

2. Multiplicatio Modulo (Z_m, X_m)

Often defined on prime numbers.

$Z_m \{1, 2, \ldots, m\}$ or (Z_p, X_p)

$Z_p \{1, 2, \ldots, p\}$ $p \rightsquigarrow$ prime

$a \, X_p \, b = (a \times b) \bmod p$ | identity = 1

When p is prime number (Z_p, X_p) is an Abelian Group.

3. Permutation (Group)

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

$f : \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$ IP / OP

S = Set of all permutation f^ns on A.

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

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

- identity = $e = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}$

Essential | Job to do | Phone No.

- inverse

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

157-208
23rd Week

Friday 06

Commutative

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

f_1 $\qquad$ 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, *)

$a \in G \qquad n \in \mathbb{Z}$ $\qquad$ $\boxed{a^n}$

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

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

$a^{-2} = (a^2)^{-1} = inv(a^2)$

$a^{1.5}$ not defined

not $(a^{-1})^2$

$(inv(a))^2$

- $(a^m)^n = a^{mn}$

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

※ Order of a Group (G, *)

Essential

order ← $o(G) = |G|$ #elems in G

Job to do

can be ∞

Phone No.

07 Saturday

158-207
23rd Week

Order of an element $a \in G$

$o(a)$ = smallest $n \in \mathbb{Z}$ such that $a^n = e$

can be ∞

eg

$*$	a	b	c	d
a	a	b	c	d
b	b	c	d	a
c	c	d	a	b
d	d	a	b	c

$e = a^1$

$o(G) = 4$

$o(a) = 1$ as $a^1 = e$

$o(b) = 4$ as $b^4 = e$

$b*b = c$
$b*c = d$
$b*d = a$

$o(c) = 2$

$o(d) = 4$

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

08 Sunday

$\Rightarrow o(a)$ divides $o(G)$ for finite grou

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

$\Rightarrow o(G) =$ prime $= p$ implies

$o(a) = 1$ or p

identity $\leftarrow o(e) = 1 \quad o(a) = p \quad \forall a \in G, a \neq e$

Essential | Job to do | Phone No.

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

$o(ab) = n \iff (ab)^n = e$

160-205
24th Week

Monday 09

$ab\,ab\,ab \cdots ab = e$ (n times)

$(ba)^n = e$

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

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

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

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

※ Cyclic Group

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

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

→ Multiple g's may exist. g ↘ generator

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

$0 = 1^0$ or $(-1)^0$

$1 = 1^1$ | $-1 = (-1)^1$

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

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

Essential | Job to do | Phone No.

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

- A cyclic group is always Abelian.

↓

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

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

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

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

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

$g = 1, m-1$

Essential	Job to do	Phone No.

eg

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

$g = ?$

$a^1 = a$ $\quad e = a$

$a^2 = a \cdot a = a$

$a^3 = a$ X

$a^n = a$

$b^1 = b$

$b^2 = bb = c$

$b^3 = b \cdot b \cdot b = c \cdot b = d$

$b^4 = d \cdot b = a$

$g = b$ ✓

Inv(b) $\quad b * x = x * b = a$

$x = d$

$g = d$ ✓

Inv(c) $\quad c * x = x * c = a$

$x = c$

$c^1 = c$

$c^2 = c \cdot c = a$

$c^3 = a \cdot c = c$

$c^4 = c \cdot c = a$

X

Generators are b, d.

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

02 Saturday

✻ Property - Cyclic group

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

$o(G)$ = Prime no.

generator = $G - \{e\}$

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

$\phi(n)$ Euler Totient Fⁿ

↳ # generators of a cyclic group of order n

03 Sunday

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

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

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

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

$$\phi(n) = (p_1^{m_1} - p_1^{m_1-1})(p_2^{m_2} - p_2^{m_2-1}) \cdots$$

$$= (2^2 - 2^1)(3^1 - 3^0)(5^1 - 5^0)$$

$$= 16$$

Essential Job to do Phone No.

$(n = p^1 \quad \phi(n) = p^1 - p^0 = n - 1)$ Monday 04

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

$\Downarrow$

relatively prime with n

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

16 relatively primes of 60

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

4. $o(g_i)$ is a relative prime of $o(G)$.

※ Subgroup $(G, *) \curvearrowright (H, *)$

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

i) $H \subseteq G$

ii) $(H, *)$ is also group.

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

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

Essential | Job to do | Phone No.

eg Non trivial subgroup.

$(Z_4, +_4)$ Addition modulo 4

$\hookrightarrow \{0, 1, 2, 3\}$

$(\{0, 2\}, +_4)$? subgroup or not —

↓ group?

$0 +_4 0 = 0$

$0 +_4 2 = 2$

$2 +_4 2 = 0$

Closure ✓ Similarly, Associative, Identity, Inverse

So, a group.

Hence, subgroup of $(Z_4, +_4)$

※ 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 $A = (\{0, 2\}, +_4)$

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

$(Z_4, +_4)$

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

$1 +_4 2 = 3$ not closed!

↓

not subgroup.

218-147
32nd Week

Wednesday 06

Lagrange's Theorem

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

2. If $|G|$ = prime, $o(G) = p \begin{cases} \to 1 \\ \to p \end{cases}$ no proper subgroup

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

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

$$\left[\underbrace{HK}_{\text{set name}} = \{ h * k \mid h \in H, k \in K \}\right]$$

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

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

$o(H \cap K) \leq o(H)$ | $o(HK) \mid o(H)$

$o(H \cap K) \leq o(K)$ | $o(HK) \mid o(K)$

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

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

Essential Job to do Phone No.

07 Thursday

※ Subgroup ~ Alternate def^n.

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.

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.

eg. $S = \{1, -1\}$

$* \rightarrow \times$

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

eg. $A = \{a, b\}$.

$(P(A), \cup)$ is an algebraic structure.

eg. $R = \{$ reflexive relations $\}$

$(R, \cup)$, $(R, \cap)$ are a.s.

* 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.

eg. $(\mathbb{N}, *) \rightarrow$ AS $\rightarrow$ Semigroup

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

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

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

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

$(P(A), \cup) \rightarrow$ AS $\rightarrow$ Semigroup

$(P(A), \cap) \rightarrow$ AS $\rightarrow$ 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 $*$.

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

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

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

$(P(A), \cup) \rightarrow$ AS, SG $\rightarrow$ $e = \phi \in P(A)$ 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}.

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

$(\mathbb{Q}, \cdot)$ $a \cdot \frac{1}{a} = 1 \mid a = 0 \Rightarrow \frac{1}{a} \notin \mathbb{Q}$ Not Group

$(\mathbb{Q}^*, \cdot)$ $a^{-1} = \frac{1}{a}$ Group

$(P(A), \cup)$ $e = \phi$ 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. $(a * b)^{-1} = b^{-1} * a^{-1} \quad \forall a, b \in G$

* Abelian Group. (Commutative Group)

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

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

eg. $(\mathbb{Z}, +)$ $\quad a+b = b+a$ Abelian

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

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

$AB \neq BA$

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 $x^{-1} = x \; \forall \; x \in G$, then G is abelian group.

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

→ I. $a * a = a.$

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

$\Rightarrow a = e.$

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

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

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

$= b * a$

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

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

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

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

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

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

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

a) $(A,+)$ c) $(B,+)$

b) $(A,\cdot)$ d) $(B,\cdot)$

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

→ a) $1+3 = 4 \notin A$

b) Closure & associativity ✓

c) ✓ d) ✓

Q. $A = \{1,2,3,4,\ldots\}$ & 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.

→ $a*b = a^b$. Closure ✓

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

$(a^b)^c \qquad a*b^c$

$a^{bc} \neq a^{b^c}$ 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.

→ Closure ✓

Associative ✓

Monoid ✓

$0.1 \to \frac{1}{0.1}$ 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

$a * e = a$. ✗

Q. S be set of all bit strings including the null string 'ϵ'. '+' denotes string concatenation. $(S, +)$ is $S = \{\epsilon, 0, 1, 00, 01, \ldots\}$ Monoid

→ Closure ✓

Associative ✓

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

abc $\quad$ abc.

Identity element. ϵ. ✓

Inverse $a + b = \epsilon$ ✗

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

b) identity is 3

c) inverse of a is $9/a$

Closure ✓

Associative ✓

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

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

identity element ✓

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

inverse element. ✓

$a * b = e \Rightarrow b = 9/a$

Q. A = 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. ✗

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

$b = \frac{-a}{1+a}$ | for $a = \cancel{-1}$, $\frac{1}{0}$.

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

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 ✓ $e = 1$

inverse $2^a \cdot b = 1 \Rightarrow b = 2^{-a}$

group.

d) $a+ib$.

closure ✓

associative ✓

identity ✓

inverse ✗ $\frac{1}{(a+ib)}$ $a=0$, $b=0$ ✗

* Finite Group.

A group with finite no. of elements.

$O(G)$ → order of finite group.

eg $(\{0\}, +)$ $(\{1\}, *)$ $(\{1,-1\}, *)$ $(\{1,-1,i,-i\}, *)$

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

Composition table

	1	-1
1	1	-1
-1	-1	1.

Check properties on this

eg. $(\{0,1,2,\ldots,(m-1)\}, \oplus_m)$ | $\oplus_m$ 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 c) Inverse of 5 is 7

b) " " 3 is 3 d) " " 7 is 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 $\otimes_7 \oplus_7$

$\begin{cases} \otimes_m - S_m \\ \oplus_m - 0 \ldots m-1 \end{cases}$

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 $a^n = e$

a^n is identity element.

Order of identity element always 1.

eg. $(\{1, -1\}, *)$ $\quad I = 1$.

Order of $1 = 1$

Order of $-1 = 2$. $\quad [(-1)^2 = 1]$

Order of group = # elems in group.

eg. $(\{1, \omega, \omega^2\}, *)$ $\quad I = 1$

$O(1) = 1$ $\quad O(\omega^2) = 3$ $\quad O(G) = 3$.

$O(\omega) = 3$

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

eg. $(\{0, 1, 2\}, \oplus_3)$ $\quad I = 0$

$O(0) = 1$ $\quad O(G) = 3$

$O(1) = 3$

$O(2) = 3$

$1 \oplus_3 2 = 0$

→ Orders of a and a^{-1} are same.

Q. T/F.

1) In a group $(Z, +)$, order of any element except 0 does not exist. T

2. In the group $(G^*, \cdot)$, where G^* 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.

eg 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 ?

* ✗ a) $H_1 = \{1,3\}$ ~~d)~~ $\{0,2,4\}$

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

✓ c) $\{0,3\}$

→ a)

	1	3
1	2	4
3		

b)

	1	5
1	2	0
5		

c)

	0	3
0	0	3
3	3	0

d)

	0	2	4
0	0	2	4
2	2	4	0
4	4	0	2

Q. $G = (\{1, 2, 3, 4, 5, 6\}, \circledast_7)$

Which are subgroups?

a) $H_1 = \{1, 6\}$ ✓ c) $\{1, 3, 5\}$

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

→

$\circledast_7$	1	6
1	1	6
6	6	1

$\circledast_7$	1	2	4
1	1	2	4
2	2	4	1
4	4	1	2

$\circledast_7$	1	3	5
1	1	3	5
3	3	2	
5			

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

→ $O(G) = p$

$O(H) \rightarrow 1/p$

Q. T/F.

*** 1. Union of any 2 subgroups of G is also a subgroup of G. (F)

* 2. Intersection of any 2 subgroups of G is also a subgroup of G. (T)

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

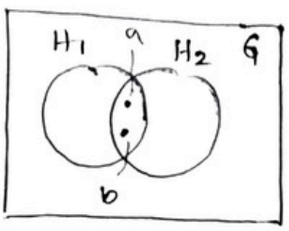
4. Every subgroup of an abelian group is also an abelian group. (T)

→ 1. $(S_8, \circledast_8) = (\{1, 3, 5, 7\}, \circledast_8)$

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

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

2.

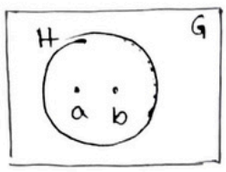


$a * b \in H_1$

$a * b \in H_2$

$a * b \in H_1 \cap H_2$

1.



$a * b = b * a$.

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

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

$1^1 = 1$ $1^2 = 2$ $1^3 = 3$ $1^4 = 0$ $\quad O(1) = O(G)$.

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

Th. Let $(G,*)$ be a cyclic group of order n with generator 'a' then

no. of relatively primes. $\phi(7) = 6$ $\phi(3) = 2$

* i) No. of generators in $G = \phi(n)$, Euler's function of n

ii) a^m is also a generator of G if $GCD(m,n) = 1$. (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

- $\phi(77) = \phi(7)\,\phi(11)$

$= 6 \times 10 = 60$

No. of generators 60.

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

- $\phi(35) = \phi(7)\,\phi(5) = 24$.

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

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 3, because order of group = order of generator

$2^1 = 2$

$2^2 = 4$

$2^3 = 1$

$(gen^r)^n$ = Identity

↓

Here 1.

⇓

2 can't be a gen^r

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

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

⇓

3 is a generator.

⇓

It's a cycle group $\Rightarrow$ 3^1 & 3^5 are gen^{r}s

⇓

3 and 5 are gen^{r}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^r $\Rightarrow$ It's a cyclic group

⇓

$1^1, 1^2, 1^3, 1^4$ are gen^{r}s

⇓

1, 2, 3, 4 are gen^{r}s

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

$S_4 = \{1, 3\}$

$3^1 = 3$ $\Rightarrow$ 3 isn't gen^r

$3^2 = 1$.

$5^1 = 5$

$5^2 = 1$

$7^1 = 7$

$7^2 = 1$.

Not a cyclic group.

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.

eg. $G = \{1, -1, i, -i\}$; $H = \{1, -1\}$. So, H is a subgroup of G.

gen^{r}s of G $\Rightarrow i, -i$

gen^r of H $\Rightarrow -1$

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

identity

(a, b, c, d)