1> GROUP ABELIAN $a \in G$, $b \in G$

1> $a \circ b \in G$ Closure.

2.> $a \circ (b \circ c) = (a \circ b) \circ c$ Associa

3.> Identity $e \circ a = a \circ e = a$

4.> Inverse $a \circ a^{-1} = a^{-1} \circ a = e$.

5> Comm $a \circ b = b \circ a$

Quasigroup $(G, \circ)$ if for each element $a, b \in G$ $a \circ x = b$ $y \circ a = b$ has a unique sol in G
$x = a^{-1} \circ b$ $y = b \circ a^{-1}$

Monoid a semigroup containing identity element is monoid.

2> CANCELLATION LAW left $a \circ b = a \circ c \Rightarrow b = c$
right $a \circ b = c \circ b \Rightarrow a = c$

Groupoid $(G, \circ)$ closure property holds

* $(a \circ b)^{-1} = b^{-1} \circ a^{-1}$
* $(G, \circ) \longrightarrow$ group.
$a \in G$ $aG = G$. $aG = \{ a \circ g \mid g \in G \}$.

Semigroup $\rightarrow$ Associativity property holds.

5> FINITE GROUP. $(G, \circ)$ is finite.
$O(G) = |G|$ - cardinality of G.

<i> $S = \{1, \omega, \omega^2\}$. $(S, \cdot) \rightarrow$ abelian group.
Composition table

	1	ω	ω^2
1	1	ω	ω^2
ω	ω	ω^2	1.
ω^2	ω^2	1	ω.

→ closure prop holds.
→ $e = 1$.
→ Inverse $\left[\begin{array}{l} 1 \rightarrow \omega^3 \\ \omega \rightarrow \omega^2 \\ \omega^2 \rightarrow \omega \end{array} \right]$
→ associative and commutative.
∴ Abelian Group.

<ii> $(Z_3, +)$ $= \{[0], [1], [2]\}$
Composition table

	[0]	[1]	[2]
[0]	[0]	[1]	[2]
[1]	[1]	[2]	[0]
[2]	[2]	[0]	[1].

✓✓✓ Abelian group.

<iii> $(Z_n, \cdot) \longrightarrow$ Not a group (inverse of 0)
$(Z_n - \{0\}, \cdot) \longrightarrow$ $n =$ prime abelian group.
$n \neq$ prime Not group ($\times$ closure).
$Z_6 - \{0\}$ $[2] \times [3] = [0]$
0 not included

(iv) $Z = \{ z \in C, z^n = 1 \}$.
abelian under Multiplication.

SUBGROUPS

1) $(G,\circ)$ is a group.
$H \subseteq G$ Non empty subset
H is closed under $\circ$ $\quad a \circ b \in H \;\; \forall a \in H, b \in H$
$H \times H \to H$

$(\{e\},\circ) \to$ trivial subgroup
$(G,\circ) \to$ Improper subgroup.
$(\mathbb{Z},+)$ is subgroup $(\mathbb{Q},+)$

$(H,\circ)$ is subgroup $(G,\circ)$ iff
- $e_H = e_G$
- Inverse of a in $(H,\circ)$ = inverse of a in $(G,\circ)$

$a \circ b^{-1} \in H$
1) $a \in H \;\; b \in H \;\; a \circ b \in H$
2) $a \in H \;\; a^{-1} \in H$

2) No 2 subgroups of a group are disjoint $\{e\}$ is common in all.

3) $(G,\circ)$ is a group 2 subgroups H, K.
(i) $H \cap K$ is a subgroup
(ii) $H \cup K$ is a subgroup iff either $H \subset K$ or $K \subset H$

$G \to (\mathbb{Z},+)$	$H \to (2\mathbb{Z},+)$ $K \to (3\mathbb{Z},+)$ $H \cup K \notin$ subgroup.	$H \to (2\mathbb{Z},+)$ $K \to (4\mathbb{Z},+)$ $H \cup K \to$ Subgroup

H, K are finite subgroup
$$\boxed{o(HK) = \frac{o(H)\,o(K)}{o(H \cap K)}}$$

(iii) $HK = \{h \circ k : h \in H, k \in K\}$ may not be subgroup $\quad G = S_3 \;\; H = \{\rho_3, \rho_0\} \;\; K = \{\rho_4, \rho_0\}$.
$HK = KH \to$ Subgroup

(iv) G is commutative group.
HK is subgroup of G.

$$H = \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} : \begin{vmatrix} a & b \\ c & d \end{vmatrix} = 1 \right\} \text{ is a subgroup } GL(2,\mathbb{R}).$$

$\boxed{\text{Subgroups of } S_3} \longrightarrow$
$\{\rho_0 \;\; \rho_1 \;\; \rho_2\}$
$\{\rho_0 \;\; \rho_3\}$
$\{\rho_0 \;\; \rho_4\}$
$\{\rho_0 \;\; \rho_5\}$.

CYCLIC GROUPS

every group of prime order is cyclic

1.> $(G,\circ)$ is cyclic $G = \{a^n, n \in \mathbb{Z}\}$
$a \in G$. $G = \langle a \rangle$ ← generator.

$(G,+)$ is cyclic $G = \{na, n \in \mathbb{Z}\} = \langle a \rangle$

⟨i⟩ $(\mathbb{Z},+)$ is cyclic $\langle 1 \rangle$ $\langle -1 \rangle$

⟨ii⟩ $(\mathbb{Z}_4,+)$ is cyclic $\langle [1] \rangle \langle [3] \rangle$

⟨iii⟩ $S = \{1,-1,i,-i\}$ is cyclic $\langle i \rangle$ $\langle -i \rangle$

⟨iv⟩ Kleins Group V not cyclic.

2.> a is generator of cyclic group then a^{-1} is also generator of cyclic group. $(G,\circ)$

V, S_n, D_n are not abelian ∴ Not cyclic.

3.> 

every cyclic group is abelian
Not vice versa!

4.> if $G = \langle a \rangle$ $O(a) = n$ $G = \{a, a^2, a^3, \dots, a^n = e\}$.

if $G = \langle a \rangle$ if $O(a) = \infty$ G is infinite.
if $O(a) = n$ $O(G) = n$.

5.> $(G,\circ)$ is a cyclic group $\langle a \rangle$ is generator.
$\langle a^r \rangle$ is also generater.

$\boxed{\begin{array}{c} r, r \in \mathbb{Z}^+ \\ r < n \\ GCD(r,n) = 1 \end{array}}$ coprime

if $r < n$ & $GCD(r,n) = 1$ $\boxed{O(a^r) = \dfrac{O(a)}{gcd(r, O(a))}} = n = O(a)$

6.> Total No of generators of finite cyclic group of order n is $\phi(n)$

Euler Torsion formulae $\phi(x) = x\left(1-\frac{1}{p_1}\right)\left(1-\frac{1}{p_2}\right) \cdots \left(1-\frac{1}{p_i}\right)$

$\phi(p) = p-1$; p = prime

$\phi(1) = 1$.

7.> Every Subgroup of cyclic group is cyclic.

8.> A cyclic group of prime order has no non trivial subgroups.

$(G,\circ)$ is finite group $\to$ every row/col can take element of G only once.

4) Symmetric Groups (S).

$S \to$ set of all permutations of $\{1,2,3,4,\dots,n\}$

$(S,\circ)$ forms non commutative group. $n>3$.

Symmetric group $(S\circ S)\to S$ bijection from set to itself.

$n=4$ $\quad S = \{1,2,3,4\}$

$$e = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix}.$$

$$\text{Inverse} - \begin{pmatrix} 1 & 2 & 3 & 4 \\ f(1) & f(2) & f(3) & f(4) \end{pmatrix}.$$

$$\text{is} \quad \begin{pmatrix} f(1) & f(2) & f(3) & f(4) \\ 1 & 2 & 3 & 4 \end{pmatrix}$$

$$f = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 3 & 4 & 2 \end{pmatrix} = (2,3,4).$$

$$g = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 4 & 3 & 2 \end{pmatrix} = (2,4).$$

$$h = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 1 & 4 \end{pmatrix} = (1,3).$$

$$gh = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix}$$

$$hg = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix}.$$

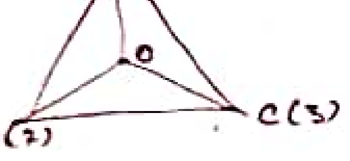
equal $\Rightarrow$ disjoint cycle $\{g,h\}$

Dihedral group $\to$ group of symmetries of polygon includes reflection & rotation.

Symmetric group of order 3. (S_3) & (D_3)

S = set of all permutations of $\{1,2,3\}$

$= \{\rho_0, \rho_1, \rho_2, \rho_3, \rho_4, \rho_5\}$.



$$\rho_0 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} \quad \rho_1 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \quad \rho_2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$$

$$\rho_3 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} \quad \rho_4 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} \quad \rho_5 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}.$$

Alternating group (A_n) $\frac{1}{2}n!$ elements $\quad n \geq 4$.

Set of all even permutations / odd perm

$A_3 \quad \rho_0\begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} \quad \rho_1\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \quad \rho_3\begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$

---

2 cycle is transposition. every cycle can be represented as a product of transposition.

even permutation $\to$ product of even no of transposition.

9> Every Non-Trivial Subgroup of Infinite Subgroup is Infinite.

10> A cyclic group of finite order 'n' has one and only one subgroup of order 'd' for every d, divisor of n.

$(Z, +)$ is cyclic group $\langle 1 \rangle$

$(mZ, +)$

$(-mZ, +)$.

$(Q, +)$ Not cyclic.

$(R, +)$ Not cyclic.

$(S, \cdot)$ Cyclic $\langle \alpha \rangle$ of (n^{th} Root of Unity) $\alpha = e^{i2\pi/n}$.

→ G must contain at least one element of order (2).

11> $O(a)$. $O(b)$ → coprime

$O(a \circ b) = O(a) \cdot O(b)$

Order $\longrightarrow$ least +ve integer s.t $a^n = e$.

order of identity element = 1
(only)

$(Z_6, +)$

$[0]$	$[1]$	$[2]$	$[3]$	$[4]$	$[5]$
1	6	3	2	3	6

$(S_3, \cdot)$ $\{ f_0 \;\; f_1 \;\; f_2 \;\; f_3 \;\; f_4 \;\; f_5 \}$

f_0	f_1	f_2	f_3, f_4, f_5
1	3	3	2

$(V, \cdot)$ $\{ e, a, b, c \}$

e	a, b, c
1	2

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

ii) $o(a) = n \quad o(a^m) = \dfrac{n}{gcd(m, n)}$ +ve 'm'

iii) $o(a) = n \quad o(a^p) = n$ p is coprime to n