- finite group
  - An
  - V-Klein's 4 gr
  - Elliptic cu
- Order of an elem
  - Theorem.
  - Subgr
  - Cyclic group
  - Z_n^*
  - Elliptic curve

Finite groups

- $(G, \circ)$, $|G|$ finite group.

Order of a group $\circ(G) = |G|$.

Example:

1. $S = \{1, \omega, \omega^2\}$ when $\omega^3 = 1$. → abelian group.

$(S, \cdot)$ is abelian

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

- is closed ⇐

identity element → 1

inverse of 1 is 1
ω is ω^2
ω^2 is ω.

symmetric about the principal diagonal ⇒ · is commutative

$S \subseteq \mathbb{C}$.

· is associative in $\mathbb{C}$
⇓
· is associative in S.

2. $S = \{1, -1, i, -i\}$ abelian group., when $i^4 = 1$.

3. $\mathbb{Z}_3$ → classes of residues of integers modulo 3.

$(\mathbb{Z}_3, +)$ → abelian group.

$[0]$ → identity element.

inverse of $[0]$ is $[0]$
$[1]$ is $[2]$
$[2]$ is $[1]$.

+	[0]	[1]	[2]
[0]	[0]	[1]	[2]
[1]	[1]	[2]	[0]
[2]	[2]	[0]	[1]

4. $(\mathbb{Z}_n, +_n)$ → abelian group., $n \in \mathbb{N}$.

addition modulo n

- $n = 1$ means trivial group containing the single element $[0]$.

5. $(\mathbb{Z}_n, \cdot)$ not abelian group $\rightarrow [0]$ doesn't have inverse.

$(\mathbb{Z}_n - \{[0]\}, \cdot)$ abelian group when n is prime.

e.g. $\mathbb{Z}_6 - \{[0]\} \ni [2], [3]$

but $[2].[3] = [6] \notin \mathbb{Z}_6 - \{[0]\}$ → not closed.

$\mathbb{Z}_n$, $n = pq$ $\quad [p] \in \mathbb{Z}_n$, $[q] \in \mathbb{Z}_n$

$[p][q] = [0] \notin \mathbb{Z}_n - \{0\}$.

6. $S = \{ z \in \mathbb{C} : z^n = 1 \}$ → set of n distinct n-th roots of unity.

→ abelian group under multiplication

(i) $z_1, z_2 \in S \Rightarrow z_1^n = 1 = z_2^n$

$\therefore z_1^n z_2^2 = 1 \Rightarrow z_1 z_2 \in S$.

S is closed under multiplication.

(ii) $\cdot$ is associative on $\mathbb{C}$, $S \subset \mathbb{C}$, so $\cdot$ is associative in S

iii) $1 \in S$ & $1.z = z.1 = z \ \forall z \in S$

$\Rightarrow 1$ is the identity element of S

iv) $z \in S \Rightarrow z^n = 1 \Rightarrow \frac{1}{z^n} = 1 \Rightarrow \frac{1}{z} \in S$

$\frac{1}{z} \cdot z = z \cdot \frac{1}{z} = 1 \ \forall z \in S$. $\Rightarrow \frac{1}{z}$ is the inverse of z in S.

v) $\cdot$ is commutative in $\mathbb{C}$ & $S \subset \mathbb{C}$, so $\cdot$ is commutative in S.

Theorem if $(G,\circ)$ is a finite group, then in every row (or column) of the composition table, each element of G appears exactly once.

Proof $|G| = n$, $\{a_1, a_2, \ldots, a_n\} \in G$ (list of elements of G) appear in the topmost row and the leftmost column.

Any arbitrary row, say i,

elements in this row $\rightarrow$ $a_i \circ a_1, a_i \circ a_2, \ldots a_i \circ a_n$

$a_1, a_2, \ldots, a_n$ all distinct

$a_i \circ a_1, a_i \circ a_2, \ldots a_i \circ a_n$ all distinct

i.e. $a_i \circ a_r = a_i \circ a_s$

$\Rightarrow a_r = a_s$ by left cancellation law.

$\Rightarrow$ a permutation of the 1st row.

Group U_n $\rightarrow$ $Z_n^* = \{a \in Z_n \mid \gcd(a,n) = 1\}$ cyclic when $n = 2, 4, p^k$ or $2p^k$, p odd prime, $k \geq 1$

$|Z_n^*| = \varphi(n)$, when cyclic, # generators $= \varphi(\varphi(n))$

- $(Z_n, \cdot)$ forms a monoid, $n > 1$
- Consider the set of all units in $Z_n \rightarrow S$
- $(S, \cdot)$ forms an abelian group

Claim $[u]$ in the monoid $(Z_n, \cdot)$ is a unit iff u and n are coprime to n.

proof Thus $[u]$ unit in $(Z_n, \cdot)$

$\Rightarrow \gcd(u,n) = 1$

$[u] \in Z_n$ unit means $\exists [v] \in Z_n$ s.t.

$[u][v] = [1]$

$\Rightarrow uv - 1 = nk$ for some integer k

$\Rightarrow uv - nk = 1$

$\Rightarrow \gcd(u,n) = 1$.

Converse let $u < n$ & $\gcd(u,n) = 1$ (u an integer)

$\Leftarrow$

$up + nq = 1$ for some integers p, q.
(Bezout's identity)

$\Rightarrow up - 1 = nq$

$\Rightarrow up \equiv 1 \pmod{n}$

$\Rightarrow p$ is not a multiple of n

ie $p \equiv r \pmod{n}$, (Division algm)

$0 \leq r < n$.

Then $[r] \in \mathbb{Z}_n$.

$up \equiv ur \pmod{n}$

$\Rightarrow 1 \equiv ur \pmod{n}$

$\Rightarrow [u][r] = [1]$

Since the monoid is commutative, we get

$[u][r] = [r][u] = [1]$

$\Rightarrow$ ~~[r] is the~~ $[u]$ is a unit in the monoid $(\mathbb{Z}_n, \cdot)$.

- $U_n = \{[u] \mid \gcd(u,n) = 1\}$.
  ↳ integers $< n$ & coprime to n

$o(U_n) = |U_n| = \phi(n)$ = Euler's Totient fn.

- n prime, $U_n = \{[1], [2], \cdots, [n-1]\}$
  total $n-1$ elements. ~~$o(U_n)$~~ $o(U_n) = n-1$

Elliptic curve group + associativity hard to prove

$(GF(q)\setminus\{0\}, \cdot)$ group (cyclic)

Symmetric group of degree n (S_n). (order $n!$)?

- $S \to$ set of all permutations on the set $\{1, 2, \cdots, n\}$.

$(S, \cdot)$ forms a non-commutative group for $n \geq 3$.

$\cdot$: multiplication of permutation.

(i) $f, g \in S \Rightarrow fg \in S$.

(ii) a permutation is a bijective mapping from $\{1, 2, \cdots, n\}$ onto itself & multiplication of two permutations is the composition of two bijective mapping.

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

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

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

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

disjoint cycles

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

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

equal

f, h not disjoint.

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

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

unequal.

Since composition of mappings is associative, multiplication of permutations is also associative.

(iii) identity permutation

$i = \begin{pmatrix} 1 & 2 & \cdots & n \\ 1 & 2 & \cdots & n \end{pmatrix} \in S$.

$if = fi = f \quad \forall f \in S$

(iv) inverse of $f \in S$

for each $f = \begin{pmatrix} 1 & 2 & \cdots & n \\ f(1) & f(2) & \cdots & f(n) \end{pmatrix} \in S$, $\exists\ g = \begin{pmatrix} f(1) & f(2) & \cdots & f(n) \\ 1 & 2 & \cdots & n \end{pmatrix} \in S$

s.t. $fg = gf = i$

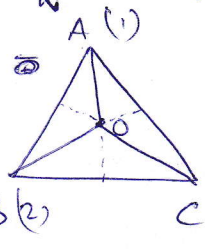
(v) multiplication not commutative.

Symmetric group S_3 of degree 3 (order 3!) → Same as the dihedral group D_3

- S = the set of all permutations on the set $\{1,2,3\}$.

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

$\rho_0 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}$, $\rho_1 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} = (1,2)(1,3)$, $\rho_2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} = (1,3,2)$



ρ_1: rotation of $\triangle ABC$ in the plane about O through 120° (anticlockwise)

ρ_2: rotation of $\triangle ABC$ in the plane about O through 240° (anticlockwise)

$\triangle ABC$ → an equilateral triangle with centroid O.

$\rho_3 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} = (2,3)$: reflexion about AO

$\rho_4 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} = (1,3)$: reflexion about BO

$\rho_5 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} = (1,2)$: reflexion about CO.

(~~Composition~~)

- The six symmetries of the equilateral triangle form a non-commutative group under the composition of symmetries.
- This group is called dihedral group D_3.

(Symmetries of equilateral triangles). → Same as the symmetric gr. S_3

[• S → the set of all points in a Euclidean space (A line is a 1-span, a plane is a 2-span) ∞

- isometry → an isometry of the space is a bijection from S onto S that preserves distance between two points in S.

- Symmetry → a Symmetry of a geometrical figure in a Euclidean space is an isometry that keeps the figure as a whole unchanged.

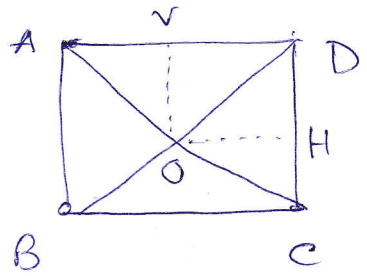
- $\rho_0, \rho_1, \rho_2, \rho_3, \rho_4, \rho_5$ → each is a Symmetry of the triangle ΔABC.

- binary operation → Composition of mappings (Symmetries).

$\circ$	ρ_0	ρ_1	ρ_2	ρ_3	ρ_4	ρ_5
ρ_0	ρ_0	ρ_1	ρ_2	ρ_3	ρ_4	ρ_5
ρ_1	ρ_1	ρ_2	ρ_0	ρ_5	ρ_3	ρ_4
ρ_2	ρ_2	ρ_0	ρ_1	ρ_4	ρ_5	ρ_3
ρ_3	ρ_3	ρ_4	ρ_5	ρ_0	ρ_1	ρ_2
ρ_4	ρ_4	ρ_5	ρ_3	ρ_2	ρ_0	ρ_1
ρ_5	ρ_5	ρ_3	ρ_4	ρ_1	ρ_2	ρ_0

The composition table is not symmetric about the main diagonal.

Symmetries of squares



The eight symmetries of the square ABCD

i = rotation through $0°$
r_1 = rotation through $90°$
r_2 = rotation through $180°$
r_3 = rotation through $270°$

} four rotations in the plane about O anticlockwise

Corresponding permutation of the vertices

$$i = \begin{pmatrix} A & B & C & D \\ A & B & C & D \end{pmatrix}, \quad r_1 = \begin{pmatrix} A & B & C & D \\ B & C & D & A \end{pmatrix} = (ABCD)$$

$$r_2 = \begin{pmatrix} A & B & C & D \\ C & D & A & B \end{pmatrix} = (A,C)(B,D), \quad r_3 = \begin{pmatrix} A & B & C & D \\ D & A & B & C \end{pmatrix} = (ADCB)$$

four rotations out of the plane

h = ~~rotation~~ reflexion about the horizontal line OH
v = rotation about the vertical line OV
d = rotation about the (principal) diagonal OA
d' = rotation about the (other) diagonal OB.

Corresponding permutation of the vertices:

$$h = \begin{pmatrix} A & B & C & D \\ B & A & D & C \end{pmatrix} = (A,B)(C,D), \quad v = \begin{pmatrix} A & B & C & D \\ D & C & B & A \end{pmatrix} = (A,D)(B,C)$$

$$d = \begin{pmatrix} A & B & C & D \\ A & D & C & B \end{pmatrix} = (B,D), \quad d' = \begin{pmatrix} A & B & C & D \\ C & B & A & D \end{pmatrix} = (A,C).$$

Note. The above eight symmetries of the square form a non-commutative group, called the octic group or the dihedral group D_4.

$S = \{i, r_1, r_2, r_3, h, v, d, d'\}$

- Taking $\circ$ as the binary composition on the set S, the composition table is given below:

$\circ$	i	r_1	r_2	r_3	h	v	d	d'
i	i	r_1	r_2	r_3	h	v	d	d'
r_1	r_1	r_2	r_3	i	d'	d	h	v
r_2	r_2	r_3	i	r_1	v	h	d'	d
r_3	r_3	i	r_1	r_2	d	d'	v	h
h	h	d	v	d'	i	r_2	r_1	r_3
v	v	d'	h	d	r_2	i	r_3	r_1
d	d	v	d'	h	r_3	r_2	i	r_2
d'	d'	h	d	v	r_1	r_3	r_2	i

Note - The Symmetries of a regular pentagon form a non-commutative group of order 10; called the dehedral group D_5. They are five rotations about the centre and five reflections about the right bisectors of the sides.

Note The symmetries of a regular n-gon form a non-commutative group of order $2n$, called the dihedral group D_n.

Example: (Klein's 4-group)

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

$\circ$	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

- abelian group of order 4.
- denoted by V. (German word Viergruppe)
- every element of the group is its own inverse.

Example: (Alternating group of order n) $\rightarrow A_n$, $n \geq 4$.

- A_n contains $\frac{1}{2}n!$ elements.
  ↓
  the set of all even permutations on the set $\{1, 2, \cdots, n\}$.
  forms a group w.r.to. multiplication of permutations.
  ↓
  non-commutative.

- A_3
  ↓
  $p_0 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}$, $p_1 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$, $p_3 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$
  $= (1)(2)(3)$ $= (1, 2, 3)$ $= (1, 3, 2)$.

  Commutation group of order 3.

- $S = \{a_1, a_2, \cdots, a_n\}$
- $f : S \to S$ a permutation is a cycle of length r
  if $f(a_{i_1}) = a_{i_2}$, $f(a_{i_2}) = a_{i_3}$, $\cdots f(a_{i_{r-1}}) = a_{i_r}$
  & $f(a_j) = a_j$ for $j \neq i_1, i_2, \cdots, i_r$.
- cycle $(a_{i_1}, a_{i_2}, \cdots, a_{i_r})$ or $(a_{i_2}, a_{i_3}, \cdots, a_{i_r}, a_{i_1})$ etc.
  ↓
  elements of the cycle.
- disjoint cycles have no common elements.
- multiplication of two disjoint cycles is commutative.

Theorem Every permutation of a finite set is either a cycle or can be expressed as a product of disjoint cycles.

Order of a permutation:

- f be a permutation on a finite set S.
- Order of f is the smallest +ve integer n s.t. $f^n = i$, i being the identity permutation.

Theorem The order of an r-cycle is r.

Theorem The order of a permutation on a finite set is the l.c.m. of the lengths of its disjoint cycles.

Transposition A 2-cycle is called a transposition.

- 1-cycle is the identity and it can be expressed as
$$(a_r) = (a_r, a_s)(a_r, a_s).$$
- 2-cycle is itself a transposition.
- 3-cycle $(a_1, a_2, a_3) = (a_1, a_3)(a_1, a_2)$
- r-cycle $(a_1, a_2, \ldots, a_r) = (a_1, a_r)(a_1, a_{r-1}) \cdots (a_1, a_3)(a_1, a_2)$

$$\begin{pmatrix} 1 & 2 & \cdots & a_r & \cdots & a_s & \cdots & n \\ 1 & 2 & \cdots & a_s & \cdots & a_r & \cdots & n \end{pmatrix} \begin{pmatrix} 1 & 2 & \cdots & a_r & \cdots & a_s & \cdots & n \\ 1 & 2 & \cdots & a_s & \cdots & a_r & \cdots & \end{pmatrix}$$
$$= \begin{pmatrix} 1 & 2 & \cdots & a_r & \cdots & a_s & \cdots & n \\ 1 & 2 & \cdots & a_r & \cdots & a_s & \cdots & \end{pmatrix}$$

$$\begin{pmatrix} a_1 & a_2 & a_3 \\ a_3 & a_2 & a_1 \end{pmatrix} \begin{pmatrix} a_1 & a_2 & a_3 \\ a_2 & a_1 & a_3 \end{pmatrix}$$
$$= \begin{pmatrix} a_1 & a_2 & a_3 \\ a_2 & a_3 & a_1 \end{pmatrix}$$

$$\begin{pmatrix} a_1 & a_2 & a_3 \\ a_2 & a_1 & a_3 \end{pmatrix} \begin{pmatrix} a_1 & a_2 & a_3 \\ a_3 & a_2 & a_1 \end{pmatrix}$$
$$= \begin{pmatrix} a_1 & a_2 & a_3 \\ a_3 & a_1 & a_2 \end{pmatrix}$$

Theorem Every permutation on a finite set (containing at least two elements) can be expressed as a product of transpositions. ↓ not unique

- identity permutation
$$i = (a_r, a_s)(a_r, a_p)$$
$$= (a_r, a_1)(a_r, a_s)(a_m, a_n)(a_m, a_n)$$

→ product of transpositions in many ways.
→ # of factors in its decomposition into transpositions is always either odd or even.

Even and odd permutations

A permutation is said to be even if it can be expressed as the product of an even no. of transpositions and odd if it can be expressed as the product of an odd number of transpositions.

- r-cycle $(a_1, a_2, \ldots, a_r) = (a_1, a_r)(a_1, a_{r-1}) \ldots (a_1, a_2)(a_1, a_1)$

  ↓

  odd if r is even

  even if r is odd.

- identity permutation is even permutation as it can be expressed as product of two transpositions

  $(a_r, a_s)(a_r, a_s)$.

- odd × odd → even permutation

  even × even → even

  odd × even → odd.

- inverse of an odd permutation is odd
- inverse of an even permutation is even.

Theorem S finite set

# of odd permutations on S = # of even permutations on S.

Integral powers of an element

- $(G, \circ)$ → a group.
- $a \in G$.

$a^0 = e$

$a^n = a \circ a \circ \cdots \circ a$ (n factors)

$\bar{a}^n = \bar{a}^1 \circ \bar{a}^1 \circ \cdots \circ \bar{a}^1$ (n factors),

n is a +ve integer.

Theorem $a \in G$, $(G, \circ)$ a group.

Then for integers m, n

(i) $a^m \circ a^n = a^{m+n}$

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

(iii) $(a^n)^{-1} = \bar{a}^n$.

Order of an element

$a \in G$, $(G, \circ)$ a group with identity element a.

- order of a $o(a)$ → least +ve integer n s.t. $a^n = e$
- a is said to be of infinite order (or of order zero) if the order of a not finite.

Note. The order of the identity element in a group is 1 & no other element in a group is of order 1.

Ex. i) $S = \{1, \omega, \omega^2\}$, $\omega^3 = 1$. $o(\omega) = 3$, & $o(\omega^2) = 3$.

ii) $(Z_6, +)$, $Z_6 = \{[0], [1], [2], [3], [4], [5]\}$

	↓	↓	↓	↓	↓	↓
order	1	6	3	2	3	6

iii) $(S_3, \cdot)$ $\quad S_3 = \{\rho_0, \rho_1, \rho_2, \rho_3, \rho_4, \rho_5\}$

order $\quad 1 \quad 3 \quad 3 \quad 2 \quad 2$

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

$\quad 2$

v) $(U_8; \cdot)$, $U_8 = \{[1], [3], [5], [7]\}$

$\quad 2$

$(U_8; \cdot)$ → +ve integer < 8 & coprime to 8

vi) $(U_{10}, \cdot)$ $\quad U_{10} = \{[1], [3], [7], [9]\}$

$\quad 4 \quad 2$

$(U_{10}, \cdot)$ → +ve integer < 10, coprime to 10

vii) $(D_4, \circ)$ $\quad D_4 = \{i, r_1, r_2, r_3, h, v, d, d'\}$

$\quad 4 \quad 2 \quad 4 \quad 2$

$(D_4, \circ)$ → dihedral gr. of order 4 → symmetries of a square

viii) $(\mathbb{Z}, +)$ → order of each non-zero element is infinite

Theorem. $a \in G$, $(G, \circ)$ group.

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

ii) $o(a) = n$ and $a^m = e \Rightarrow n \mid m$.

iii) $o(a) = n \Rightarrow a, a^2, \cdots, a^n (= e)$ are distinct elements of G. $(\Rightarrow o(a) \leq o(a))$

iv) $o(a) = n \Rightarrow o(a^m) = \dfrac{n}{\gcd(m,n)}$ for any +ve integer m.

order of power formula: $o(a^m) = \dfrac{o(a)}{\gcd(m, o(a))}$

v) $o(a) = n \Rightarrow o(a^p) = n$ iff p is coprime to n

vi) $o(a)$ infinite & p is any +ve integer $\Rightarrow o(a^p)$ infinite.

Proof (i) Let $o(a)=n$ (finite) $\Rightarrow a^n = e$, n least +ve integer.

$\therefore (\bar{a})^n = \bar{a}^n = (a^n)^{-1} = \bar{e}^1 = e$

if possible, let $\exists\ m < n$ s.t. $(\bar{a}^1)^m = e$

$\Rightarrow \bar{a}^m = e$.

$\therefore \bar{a}^m \in G, a^n \in G \Rightarrow a^{n-m} \in G$, $a^{n-m} = a^n \cdot \bar{a}^m = e \cdot e = e$

& $n-m < n$ $(\rightarrow\leftarrow)$ as $o(a)=n$

$\therefore o(a)=n \Rightarrow o(\bar{a}^1)=n$

in case $o(a)$ infinite, then $o(\bar{a}^1)$ also infinite.

o.w. if $o(\bar{a}^1) = m$ (finite)

Then $\bar{a}^m = e$

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

$\Downarrow$

$a^m = e$.

$\Downarrow$

a is of finite order $(\rightarrow\leftarrow)$

(ii) $o(a)=n \Rightarrow a^n = e$, n is least +ve integer.

$\therefore$ By division algm

$m = nq + r$, $0 \le r < n$

Given $a^m = e$

$\Rightarrow (a^m)^q \cdot a^r = e$

$\Rightarrow (e)^q \cdot a^r = e$

$\Rightarrow a^r = e$, $0 \le r < n$ $(\rightarrow\leftarrow)$ to $o(a)=n$

$\therefore$ $r=0$ i.e. $m = nq$.

(iii) $o(a)=n$

Then $a, a^2, \cdots, a^n (=e)$ all distinct elements of G.

if $a^r = a^s$, $1 \le r < s \le n$

then $a^{s-r} = e$. $(\rightarrow\leftarrow)$ as $0 < s-r < n$

that $o(a)=n$.

(iv) $o(a)=n$

Let $o(a^m) = k$ i.e. $a^{mk} = e$, k is the least +ve integer.

$\Rightarrow n \mid mk$ as $o(a)=n$.

Let $d = \gcd(m,n) \Rightarrow \gcd\left(\frac{m}{d}, \frac{n}{d}\right) = 1$.

Let $\frac{m}{d} = u$, $\frac{n}{d} = v$. $\therefore m = ud$, $n = vd$

$n \mid mk \Rightarrow dv \mid duk \Rightarrow v \mid uk \Rightarrow v \mid k$ as $\gcd(u,v)=1$

Also $(a^m)^v = a^{duv} = (a^u)^n = (a^n)^u = e$ as $o(a)=n$

So $v = k = \frac{n}{d} = \frac{n}{\gcd(m,n)}$

Also $o(a^m)=k$ so

$o(a^m) = k$

$\Rightarrow (a^m)^k = e$, k is least +ve int.

Also $(a^m)^v = e$

So $k \mid v$ by (i).

v) $\gcd(p,n) = 1$.

$o(a) = n$, $o(a^p) = \frac{o(a)}{\gcd(p,n)} = o(a)$.

vi) $o(a)$ infinite; p is any integer.

if possible, let $o(a^p)$ be finite, say m.

$\therefore o(a^p) = m \Rightarrow a^{pm} = e$.

$\Rightarrow a$ is of finite order

$(\rightarrow \leftarrow)$

$\therefore o(a^p)$ is infinite if $o(a)$ is infinite.

Theorem Each element of a finite group is of finite order.

proof: $(G, \circ)$ group, $o(G) =$ finite.

$a \in G$

Then $a, a^2, \ldots$ all elements of G.

cannot be all distinct as G is of finite order

$\therefore a^m = a^n$ for some two integers m, n.

$m > n$.

$\therefore a^{m-n} = e \Rightarrow o(a)$ is finite.

Note: Order of an element in a finite group cannot exceed the order of the group.

(as $a, a^2, \ldots, a^n (= e)$ are all distinct elements of a when $o(a) = n$).

Subgroups

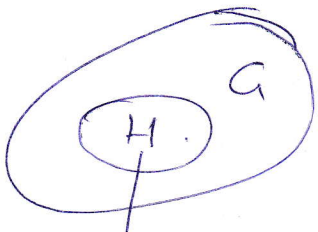
- $(G, \circ) \rightarrow$ a group
- $H \subseteq G \rightarrow$ a non-empty subset of G.
- H is closed (or stable) under $\circ$ if $a \circ b \in H$ ~~whenever~~ $\forall\ a, b \in H$.
- restriction of $\circ$ (when H is closed under $\circ$) is a mapping denoted by $*$

$$* : H \times H \rightarrow H, \text{ defined by}$$
$$a * b = a \circ b \quad \forall\ a, b \in H$$

- $*$ is called the induced composition on H

$H \subseteq G,\ H \neq \phi$

- $(H, \circ)$ is a subgroup of $(G, \circ)$ when $(H, \circ)$ is a group, $\circ$ being the induced composition.



forms a group in its own right — under the induced composition $\circ$.

Examples

1. $(G, \circ)$ a group.

   $G \subseteq G$, so $(G, \circ)$ is a subgroup of $(G, \circ)$ (improper subgroup).

2. $e \rightarrow$ identity element of $(G, \circ)$ (group)

   $(\{e\}, \circ) \rightarrow$ trivial subgroup.

3. $(\mathbb{Q}, +)$ is a group, $(\mathbb{Z}, +)$ is a group, $\mathbb{Z} \subseteq \mathbb{Q},\ \mathbb{Z} \neq \mathbb{Q}$

   $\Rightarrow (\mathbb{Z}, +)$ is a subgroup of $(\mathbb{Q}, +)$

4. $(\mathbb{Q}, +)$ is a group, $(\mathbb{Q}^* = \mathbb{Q} - \{0\}, \cdot)$ is a group but $(\mathbb{Q}^*, \cdot)$ is not a subgroup of $(\mathbb{Q}, +)$.

5. $(G,\circ)$ → abelian group.

Let $(H,\circ)$ be a subgroup of $(G,\circ)$.

Then $(H,\circ)$ is an abelian group.

6. S_3 → non-commutative group.

A_3 is a subgroup of S_3

A_3 is commutative.

Theorem $(H,\circ)$ a subgroup of $(G,\circ)$.

Then (i) $\boxed{e_H = e_G,}$ e_H is the identity element of H, e_G of G.

(ii) if $a \in H$, then (inverse of a in $(H,\circ)$) = (inverse of a in $(G,\circ)$).

Proof (Skip).

(ii) $\bar{a}^1$ → inverse of a in G

a^1 → inverse of a in H

$\bar{a}^1 \circ a = a \circ \bar{a}^1 = e$ in G.

$a^1 \circ a = a \circ a^1 = e$ in H so in G.

$(e_H = e_G = e$ say$)$

$\therefore a \circ \bar{a}^1 = a \circ a^1 = e$ in G

$\Rightarrow \bar{a}^1 = a^1$ in G by left cancellation law in $(G,\circ)$.

(i) $h \circ e_H = e_H \circ h = h \ \forall h \in H$

$h \circ e_G = e_G \circ h = h$

as $h \in H \Rightarrow h \in G$.

$\therefore h \circ e_H = h \circ e_G$ in G.

$\Rightarrow e_H = e_G$ by left Cancellation law in $(G,\circ)$.

Note Every subset of $(G,\circ)$ must contain the element e_G. Therefore, there cannot be two ~~distinct~~ disjoint subgroups of a group.

Theorem $(G,\circ)$ group
$H \subseteq G$, $H \neq \emptyset$.
$(H,\circ)$ is a subgroup of $(G,\circ)$ iff

(i) $a \in H, b \in H \Rightarrow a \circ b \in H$
(ii) $a \in H \Rightarrow \bar{a}^1 \in H$
($\bar{a}^1$: inverse of a in G)

→ Proof
- if $(H,\circ)$ is a subgroup of $(G,\circ)$, then (i), (ii) satisfied
- If (i) & (ii) satisfied.
To prove $(H,\circ)$ is a subgroup.
- closure holds by (i)
- associativity holds since $\circ$ is associative in G & $H \subset G$

Theorem A non-empty subset H of G, when $(G,\circ)$ is a group, is a subgroup of G iff

(i) — $a \in H, b \in H \Rightarrow a \circ \bar{b}^1 \in H$

Proof

- if $(H,\circ)$ subgroup of $(G,\circ)$

Then $b \in H \Rightarrow \bar{b}^1 \in H$ as $(H,\circ)$ is a group
$a \in H, \bar{b}^1 \in H \Rightarrow a \circ \bar{b}^1 \in H$
by closure property of the group $(H,\circ)$.

- by (ii), $a \in H \Rightarrow \bar{a}^1 \in H$.
($\bar{a}^1$: inverse of a in G)
$\therefore \bar{a} \circ a = e \in H$ by (i)
- $e \in H, a \in H \Rightarrow \bar{a}^1$ (the inverse of a in G) must also be the inverse of a in H
$a \in H \Rightarrow \bar{a}^1 \in H$
So, $(H,\circ)$ subgr of $(G,\circ)$

- Conversely, let condition (i) holds.
i.e. $a \in H, b \in H \Rightarrow a \circ \bar{b}^1 \in H$.
- $a \in H, a \in H \Rightarrow a \circ \bar{a}^1 \in H \Rightarrow e \in H$.
(existence of identity in H).
- $e \in H, a \in H \Rightarrow e \circ \bar{a}^1 \in H \Rightarrow \bar{a}^1 \in H$
(existence of inverse of each element in H)
- $a \in H, b \in H \Rightarrow a \in H, \bar{b}^1 \in H \Rightarrow a \circ (\bar{b}^1)^1 \in H \Rightarrow a \circ b \in H$ (closure property)
- as $H \subset G$, $H \neq \emptyset$, $\circ$ is associative in G, $\circ$ is associative in H

$\Leftarrow$ $(H,\circ)$ subgr. of $(G,\circ)$

Theorem $(G,\circ)$ a group.

H non-empty finite subset of G.

Then $(H,\circ)$ is a subgroup of $(G,\circ)$ iff $\boxed{a\in H,\ b\in H \Rightarrow a\circ b\in H}$

Proof - If $(H,\circ)$ subgroup, then the result follows from the closure property of $\circ$.

- Conversely, let $H\subset G$, $H\neq\phi$, finite s.t.

$$\boxed{a\in H,\ b\in H \Rightarrow a\circ b\in H}\ \text{(closure)}$$

Let $h\in H$

Then $h, h^2, h^3, \ldots \in H$ by the given closure property of H

H finite, all cannot be distinct.

$\therefore\ h^r = h^s$ for some $r<s$.

$s-r>0$ the integer.

$\therefore\ \boxed{h^{s-r} = e\in H}$

(identity existence) in H.

Also $s-r\geq 1$ or $s-r-1\geq 0$.

Now $h^{s-r-1}\in H$, $h\in H \Rightarrow h^{r-s-1}\circ h = h^{r-s} = e$

$= h\circ h^{r-s-1}$

$\Rightarrow h\in H$

$\Rightarrow \boxed{h^{-1}\ (= h^{r-s-1})\in H}$

Also associativity holds in H as it is a non-empty subset of G.

$\Rightarrow (H,\circ)$ is a group & hence is a subgroup of $(G,\circ)$.

Note - The Theorem does not hold if H is an infinite subset of G.

e.g. Let $G = (\mathbb{Z}, +)$, $H = \mathbb{N}$
(G: group; H: a non-empty subset of $\mathbb{Z}$ (infinite))

$\mathbb{N}$ is closed under addition, but does not form a group.

$(\mathbb{N}, +)$ not a group.
(no element in $\mathbb{N}$ has its inverse in $\mathbb{N}$
$1 \in \mathbb{N}$ but $-1 \notin \mathbb{N}$.)
$0 \notin \mathbb{N}$

Theorem $(G, \circ)$ group; H, K two subgroups of $(G, \circ)$.
Then $H \cap K$ is a subgroup of $(G, \circ)$.

proof $e \in H$, $e \in K$ so $H \cap K \neq \phi$
($H \cap K$: non-empty subset of G)

Let $a, b \in H \cap K$. $\Rightarrow a, b \in H$ and $a, b \in K$.
$\Rightarrow a \circ b^{-1} \in H$ and $a \circ b^{-1} \in K$ [$\because H, K$ both subgroups of G]
$\Rightarrow a \circ b^{-1} \in H \cap K$

$\therefore H \cap K$ is a subgroup of $(G, \circ)$.

Note Intersection of an arb. family of subgroups of a gr. G is a subgr. of G.

Note: The union of two subgroups of a group G is not necessarily a subgroup of G.

e.g. $G = (\mathbb{Z}, +)$, $H = (2\mathbb{Z}, +)$, $K = (3\mathbb{Z}, +)$
$2 \in H \cup K$, $3 \in H \cup K$ but $2 + 3 = 5 \notin H \cup K$

e.g. $G = (\mathbb{Z}, +)$, $H = (2\mathbb{Z}, +)$, $K = (4\mathbb{Z}, +)$ $\rightarrow H \cup K = K$ subgr. of G

Theorem Let $(G,\circ)$ be a group and H, K be two subgroups of $(G,\circ)$. Then HUK forms a subgroup of $(G,\circ)$ iff either $H \subset K$ or $K \subset H$.

proof:

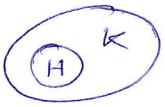
- if $H \subset K$ then $HUK = K$
  or if $K \subset H$ then $HUK = H$

  In any case, HUK is a subgroup.

- if HUK is a subgroup, we have to prove that either $H \subset K$ or $K \subset H$.

~~i.e. either $K \subset H$ or $H \subset K$ i.e. $K = H$~~

Claim i.e. either $H - K$ or $K - H$ is empty.



$H - K = \phi$

$H \cap \bar{K} = \phi$

(proof of the claim)

if not, let both $H - K$ and $K - H$ be non-empty.

Let $a \in H - K$ and $b \in K - H$.

$\Rightarrow a \in H$, but $a \notin K$; $b \in K$, but $b \notin H$.

$\therefore a \in HUK$ and $b \in HUK$

As HUK is a subgroup, it follows that

$$\boxed{a \circ b \in HUK} \quad \text{---} (1)$$

$\Rightarrow a \circ b \in H$ or $a \circ b \in K$

~~if $a \circ b \in H$, then~~

But $a \in H$ & $a \circ b \in H \Rightarrow \bar{a}^1 \circ (a \circ b) \in H$ as H is a subgr. of G.

$\Rightarrow b \in H$, contradiction.

Also $b \in H$ & $a \circ b \in H \Rightarrow (a \circ b) \circ \bar{b}^1 \in K$ as K is a subgr. of G

$\Rightarrow a \in K$, a contradiction.

$\therefore a \circ b$ neither belongs to H nor belongs to K.

This contradicts (1).

Hence our assumption that both $H - K$ and $K - H$ non-empty is wrong.

$\therefore$ either $H \subset K$ or $K \subset H$.

Converse: if $H \subset K$ then $HUK = K$ or if $K \subset H$ then $HUK = H$. In any case, HUK is a subgr. of G.

Note. A group cannot be the union of two proper subgroups.

- Let H and K be subgroups of a group $(G, \circ)$.
Then $HK = \{hk : h \in H, k \in K\}$ may not be a subgroup of $(G, \circ)$.

e.g. $G = S_3$, $H = \{\rho_3, \rho_0\}$, $K = \{\rho_4, \rho_0\}$

Then $HK = \{\rho_3\rho_4, \rho_3, \rho_4, \rho_0\} = \{\rho_1, \rho_3, \rho_4, \rho_0\}$.
Which is not a subgroup of S_3.

$KH = \{\rho_4\rho_3, \rho_4, \rho_3, \rho_0\} = \{\rho_2, \rho_3, \rho_4, \rho_0\}$
Which is not a subgroup of S_3.

Theorem Let H and K be subgroups of a group G.
Then HK is a subgroup of G iff $HK = KH$.

proof:

- Let HK be a subgroup of G.
Let $x \in HK$. Then $x^{-1} \in HK$ as HK is a subgr. of G.
Let $x^{-1} = h_1 k_1$. Then $x = k_1^{-1} h_1^{-1} \in KH$.
Thus $x \in HK \Rightarrow x \in KH$
$\therefore HK \subseteq KH$ —— (1)

- Let $k_2 h_2 \in KH$. Then $k_2 \in K$, $h_2 \in H$.
So $k_2^{-1} \in K$, $h_2^{-1} \in H \Rightarrow h_2^{-1} k_2^{-1} \in HK$.
As HK is a subgr. of G, we have $(h_2^{-1} k_2^{-1})^{-1} \in HK$
i.e. $k_2 h_2 \in HK$.
$\therefore KH \subseteq HK$ —— (2)
So (1), (2) $\Rightarrow HK = KH$.

Converse Let $HK = KH$.
Let $p, q \in HK$
Claim $pq \in HK$ & $p^{-1} \in HK$.

proof Let $p = h_1 k_1$, $q = h_2 k_2$.
Then $pq = h_1 (k_1 h_2) k_2$
$= h_1 (h_2 k_1) k_2$ (as $HK = KH$)
$= (h_1 h_2)(k_1 k_2) \in HK$.
Also $p^{-1} = k_1^{-1} h_1^{-1} \in KH = HK$.

Note: • if G is a commutative group, then HK is a subgroup of G.

• HK is a subgroup of G $\not\Rightarrow$ G is commutative.

e.g. $G = S_4$ noncommutative group

$H = \{I, (1,2,3), (1,3,2)\}$, $K = \{I, (3,3)\}$

$HK (= KH)$ is a subgroup, but G is non-commutative

Theorem Let H and K be finite subgroups of a group G s.t. HK is a subgroup of G. (i.e. $HK = KH$)

Then $o(HK) = \dfrac{o(H)\, o(K)}{o(H \cap K)}$

Proof Let $o(H) = m$, $o(K) = n$, $o(H \cap K) = p$,

$H = \{h_1, h_2, \cdots, h_m\}$

$K = \{k_1, k_2, \cdots, k_n\}$, $H \cap K = \{t_1, t_2, \cdots, t_p\}$.

$HK = \{h_i k_j \mid 1 \le i \le m,\ 1 \le j \le n\}$.

The elements $h_i k_j$ in the list HK may not be all distinct.

# of times $h_1 k_1$ appears in HK

Let $h_1 k_1 = h_r k_s$ for some r, s, $1 \le r \le m$, $1 \le s \le n$.

$\Leftrightarrow h_1^{-1} h_r = k_1 k_s^{-1} = t$ (say)

$h_1^{-1} h_r \in H$, $k_1 k_s^{-1} \in K \Leftrightarrow t \in H \cap K$.

Also $h_1^{-1} h_r = t \Leftrightarrow h_r = h_1 t$

$k_1 k_s^{-1} = t \Leftrightarrow k_s = k_1 t^{-1}$

$\Leftrightarrow h_1 k_1 = (h_1 t)(k_1 t^{-1})$ for some $t \in H \cap K$

$\Leftrightarrow h_1 k_1$ appears p times in the list HK.

$\therefore o(HK) = \dfrac{mn}{p} = \dfrac{o(H)\, o(K)}{o(H \cap K)}$.

(2) H, K finite subgrs. of $(G, \circ)$.

Corollary: If $H \cap K = \{e\}$, then $|(HK)| = o(H) \cdot o(K)$.

(HK need not be subgroup of G here).

Proof:

$$HK = \{hk \mid h \in H, k \in K\}$$

Claim $\#$ in the list HK is $o(H) \cdot o(K)$.

Let $h_1 k_1 = h_2 k_2$ for some $h_1, h_2 \in H$, $k_1, k_2 \in K$ with $h_1 \neq h_2$, $k_1 \neq k_2$.

$\Rightarrow h_1^{-1} h_2 = k_1 k_2^{-1} \neq e$. (~~as the equality~~ implies $h_1^{-1} h_2 = e \in H \cap K$)

$h_1^{-1} h_2 \in H$, $k_1 k_2^{-1} \in K$, $\rightarrow = t$ (say).

$\in H \cap K$.

Thus $h_1^{-1} h_2 \in H \cap K$, also as $h_1 \neq h_2$, $h_1^{-1} h_2 \neq e$, gives a contradiction that $H \cap K = \{e\}$.

$\therefore$ No two elements in HK are equal.

$\therefore |(HK)| = o(H) \cdot o(K)$.

Example: Let $A = \{\rho_0, \rho_3\}$

$B = \{\rho_0, \rho_4\}$ be subgroups of S_3.

Then $A \cap B = \{\rho_0\}$.

$AB = \{\rho_0\rho_0, \rho_0\rho_4, \rho_3\rho_0, \rho_3\rho_4\}$

$= \{\rho_0, \rho_4, \rho_3, \rho_1\}$ $\rightarrow$ not a subgr of S_3

~~$o(A)$~~ ~~$o(AB) =$~~

But $|AB| = 4 = o(A) \cdot o(B)$

Examples (Subgroups).

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

($GL(2,\mathbb{R})$ is the general linear group of all real non-singular matrices of order 2 w.r.to matrix multiplication).

• H is denoted by $SL(2,\mathbb{R})$, is the special linear group of order 2 over $\mathbb{R}$)

1) H is non-empty as $I_2 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \in H = SL(2,\mathbb{R})$.

2) $A \in H, B \in H \Rightarrow |A| = 1, |B| = 1 \Rightarrow |AB| = 1 \Rightarrow AB \in H$

3) $A \in H \Rightarrow |A| = 1 \Rightarrow |A^{-1}| = \frac{1}{|A|} = 1 \Rightarrow A^{-1} \in H$.

Therefore, H is a subgroup of $GL(2,\mathbb{R})$.

Example:

S_3

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

each is a subgroup of S_3.

To show this, construct the composition table for each

$\cdot$	ρ_0	ρ_1	ρ_2
ρ_0	ρ_0	ρ_1	ρ_2
ρ_1	ρ_1	ρ_2	ρ_0
ρ_2	ρ_2	ρ_0	ρ_1

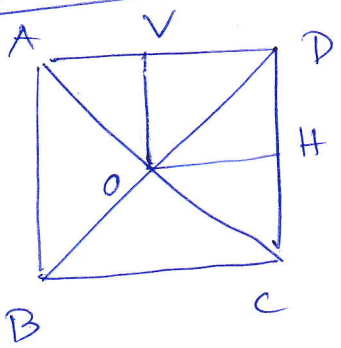
$\cdot$	ρ_0	ρ_3
ρ_0	ρ_0	ρ_3
ρ_3	ρ_3	ρ_0

$\cdot$	ρ_0	ρ_4
ρ_0	ρ_0	ρ_4
ρ_4	ρ_4	ρ_0

$\cdot$	ρ_0	ρ_5
ρ_0	ρ_0	ρ_5
ρ_5	ρ_5	ρ_0

Example: D_4 (Dihedral group / Octic group)

Symmetries of a square



Composition table shows that each of these finite subsets is closed under multiplication.

- $\{i, r_1, r_2, r_3\}$
- $\{i, r_2, h, v\}$
- $\{i, r_2, d, d'\}$
- $\{i, r_2\}$
- $\{i, h\}$
- $\{i, v\}$
- $\{i, d\}$
- $\{i, d'\}$

4 rotation in the plane about O

$i \rightarrow$ rotation through $0°$
$r_1 \rightarrow$ $90°$
$r_2 \rightarrow$ $180°$
$r_3 \rightarrow$ $270°$

4 rotation out of the plane

$h \rightarrow$ rotation about OH
$v \rightarrow$ rotation about OV
$d \rightarrow$ rotation about OA
$d' \rightarrow$ rotation about OB

$$D_4 = \{i, r_1, r_2, r_3, h, v, d, d'\}$$

Example: Q_8 → The group of unit quaternions.

$$Q_8 = \{I, -I, J, -J, K, -K, L, -L\}$$

$$I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad -I = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}, \quad J = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}, \quad -J = \begin{pmatrix} -i & 0 \\ 0 & i \end{pmatrix}$$

$$K = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \quad -K = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, \quad L = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}, \quad -L = \begin{pmatrix} 0 & -i \\ -i & 0 \end{pmatrix}$$

- Q_8 is a subgroup of $GL(2, \mathbb{C})$, the general linear group of degree 2 over $\mathbb{C}$.
- Q_8 is the group of all invertible complex matrices of order 2 & is a subset of all complex matrices

$$\left\{ \begin{pmatrix} u & v \\ -\bar{v} & \bar{u} \end{pmatrix} \middle| u, v \in \mathbb{C} \right\}$$ where $\bar{u}$ is the complex conjugate of u

$I^2 = K^2 = L^2 = -I$

$JK = L, \quad KJ = -L$

$KL = J, \quad LK = -J$

$LJ = K, \quad JL = -K$

Q_8 — $\{I, -I, L, -L$

$\{I, -I\}$ $\{I, -I, J, -J\}$ $\{I, -I, K, -K$

each forms a subgroup of Q_8.

Construct the composition table for the set Q_8.

	I	$-I$	J	$-J$	K	$-K$	L	$-L$
I	I	$-I$	J	$-J$	K	$-K$	L	$-L$
$-I$	$-I$	I	$-J$	J	$-K$	K	$-L$	L
J	J	$-J$	$-I$	I	L	$-L$	$-K$	K
$-J$	$-J$	J	I	$-I$	$-L$	L	K	$-K$
K	K	$-K$	$-L$	L	$-I$	I	J	$-J$
$-K$	$-K$	K	L	$-L$	I	$-I$	$-J$	J
L	L	$-L$	K	$-K$	$-J$	J	$-I$	I
$-L$	$-L$	L	$-K$	K	J	$-J$	I	$-I$

Some important Subgroups of a group

1. The centre of a group

- $(G, \circ)$ → a group.
- $H = \{x \in G \mid x \circ g = g \circ x \ \forall \ g \in G\}$ → Centre of G, denoted by $Z(G)$

i.e. each element in H commutes with all elements of G.

- claim $(H, \circ)$ is a subgroup of $(G, \circ)$

$Z(G)$ is a commutative subgroup of G

proof

- let $p \in H, q \in H$

$\Rightarrow p \circ g = g \circ p$ & $q \circ g = g \circ q \ \forall g \in G$.

$\therefore (p \circ q) \circ g = p \circ (q \circ g) = p \circ (g \circ q)$

$= (p \circ g) \circ q$.

$\forall g \in G$

$\Rightarrow p \circ q \in H$. — (1)

$Z(G) = G$ if G is commutative group

- let $p \in H$

$\Rightarrow p \circ g = g \circ p \ \forall g \in G$.

$\therefore p^{-1} \circ g = (p^{-1} \circ g) \circ (p \circ p^{-1})$

$= p^{-1} \circ (g \circ p) \circ p^{-1}$

$= p^{-1} \circ (p \circ g) \circ p^{-1}$

$= (p^{-1} \circ p) \circ g \circ p^{-1}$

$= g \circ p^{-1}$

$\Rightarrow p^{-1} \in H$. — (2)

(1), (2) $\Rightarrow$ H is a subgroup of G.

2. The centraliser of an element in a group.

- $(G, \circ)$ → group, $a \in G$
- $H = \{x \in G \mid x \circ a = a \circ x\}$ → Centralizer of the element a, denoted by $C(a)$

i.e. each element of H commutes with the particular element a.

Claim $(H, \circ)$ is a subgroup of $(G, \circ)$.

proof

- let $p \in H, q \in H \Rightarrow p \circ a = a \circ p$ and $q \circ a = a \circ q$.

$$\therefore (p \circ q) \circ a = p \circ (q \circ a) = p \circ (a \circ q)$$
$$= (p \circ a) \circ q$$
$$= (a \circ p) \circ q$$
$$= a \circ (p \circ q)$$

$\Rightarrow p \circ q \in H$ — (1)

- let $p \in H \Rightarrow p \circ a = a \circ p$.

$$\therefore p^{-1} \circ a = (p^{-1} \circ a) \circ (p \circ p^{-1})$$
$$= p^{-1} \circ (a \circ p) \circ p^{-1}$$
$$= p^{-1} \circ (p \circ a) \circ p^{-1}$$
$$= (p^{-1} \circ p) \circ a \circ p^{-1}$$
$$= a \circ p^{-1}$$

$\Rightarrow p^{-1} \in H$ — (2)

(1), (2) $\Rightarrow$ H is a subgroup of G.

3. Cyclic subgroup generated by an element

. $(G, \circ)$ → a group, $a \in G$

. $H = \{a^n \mid n \in \mathbb{Z}\}$ → cyclic subgr. of G, denoted by $\langle a \rangle$

i.e. each element of H is an integral power of a particular element a of G.

Claim H is a subgroup of G.

Proof $p \in H, q \in H \Rightarrow p = a^r, q = a^s$ for some integers r, s

$\Rightarrow p \circ q = a^{r+s} \in H$ — (1)

as $r+s$ is an integer

$p \in H \Rightarrow p = a^r$ for some integer r

$\Rightarrow p^{-1} = a^{-r} \in H$ as $-r$ is an integer — (2)

(1), (2) $\Rightarrow H$ is a subgroup of G.

Note. $\langle a \rangle$ → Smallest subgroup of G containing a.

i.e. if K is any subgroup of G containing a, then $\langle a \rangle \subset K$.

[$a \in K \Rightarrow a^n \in K$ for every $n \in \mathbb{Z} \Rightarrow \langle a \rangle \subset K$]

Note $\langle a \rangle$ → commutative subgroup of G.

[$p, q \in \langle a \rangle \Rightarrow p = a^r, q = a^s$ so $p \circ q = a^{r+s} = q \circ p$

$\Rightarrow \langle a \rangle$ is commutative].

Example: (cyclic subgroups)

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

   - $\langle 1 \rangle = \{1\}$ (trivial subgroup)
   - $\langle i \rangle = \{1, i, -1, -i\}$ (group S itself)
   - $\langle -1 \rangle = \{1, -1\}$ (proper subgroup)
   - $\langle -i \rangle = \{1, i, -1, -i\}$ (group S itself)

2. $(\mathbb{Z}_5, +)$, $\mathbb{Z}_5 = \{[0], [1], [2], [3], [4]\}$

   $\langle [0] \rangle = \{[0]\}$ (trivial subgroup)

   $\langle [1] \rangle = \{[0], [1], [2], [3], [4]\}$ (group $\mathbb{Z}_5$ itself)

   $\langle [2] \rangle = \mathbb{Z}_5 = \langle [3] \rangle = \langle [4] \rangle$ (group $\mathbb{Z}_5$ itself)

3. $S_3 = \{\rho_0, \rho_1, \rho_2, \rho_3, \rho_4, \rho_5\}$

   $\langle \rho_0 \rangle = \{\rho_0\}$ (trivial subgroups)

   $\langle \rho_1 \rangle = \{\rho_0, \rho_1, \rho_2\}$ (proper $\otimes$ subgroup)

   $\langle \rho_2 \rangle = \{\rho_0, \rho_1, \rho_2\}$ (")

   $\langle \rho_3 \rangle = \{\rho_0, \rho_3\}$ (")

   $\langle \rho_4 \rangle = \{\rho_0, \rho_4\}$ (")

   $\langle \rho_5 \rangle = \{\rho_0, \rho_5\}$ (")