Important Subgroups:-

① The Centre of a group → $Z(G) = \{x \in G : x \circ g = g \circ x, \forall g \in G\}$

So, $Z(G)$ is a subset of the group G containing those elements of G that commute with every element of G.

To show: $Z(G) \leq G$.

$Z(G)$ is a non-empty subset of G, as we have $e \in G$, $e \circ g = g \circ e$, $\forall g \in G$. So, $e \in Z(G)$.

Let $a, b \in Z(G)$. Then we have,

$a \circ g = g \circ a$; $b \circ g = g \circ b$, $\forall g \in G$.

$\Rightarrow (a \circ g) \circ \bar{g}^1 = g \circ a \circ \bar{g}^1$, $\forall g \in G$.

$\Rightarrow a \circ (g \circ \bar{g}^1) = g \circ a \circ \bar{g}^1$ [using properties of Group G]

$\Rightarrow a \circ e = g \circ a \circ g^{-1}$

$\Rightarrow a = g \circ a \circ \bar{g}^1$, $\forall g \in G$.

Also, $b \circ g = g \circ b$, $\forall g \in G$

$\Rightarrow (b \circ g) \circ \bar{g}^1 = g \circ b \circ \bar{g}^1$

$\Rightarrow b \circ (g \circ \bar{g}^1) = g \circ b \circ \bar{g}^1$

$\Rightarrow b \circ e = g \circ b \circ \bar{g}^1$

$\Rightarrow b = g \circ b \circ \bar{g}^1$

$\Rightarrow b^{-1} = (g \circ b \circ \bar{g}^1)^{-1}$

$\Rightarrow b^{-1} = g \circ b^{-1} \circ \bar{g}^1$

Therefore, $(a \circ b^{-1}) \circ g$

$= (g \circ a \circ \bar{g}^1) \circ (g \circ b^{-1} \circ \bar{g}^1) \circ g$

$= g \circ a \circ (\bar{g}^1 \circ g) \circ b^{-1} \circ (\bar{g}^1 \circ g) = g \circ a \circ e \circ b^{-1} \circ e$

$= g \circ (a \circ b^{-1})$. [Using the properties of Group G].

$\therefore (a \circ b^{-1}) \circ g = g \circ (a \circ b^{-1})$, $\forall g \in G$

$\Rightarrow a \circ b^{-1} \in Z(G)$ whenever $a, b \in Z(G)$.

$\Rightarrow Z(G) \leq G$.

Note: The elements of the centre of the Group are called the central elements of G.

Remarks: (i) If G be an abelian group, then $Z(G) = G$.

(ii) And $Z(G)$ is a Commutative subgroup of G.

② The Centraliser of an element in a group:

$C(a) = \{x \in G : x \circ a = a \circ x, a \in G\}$.

$C(a) \subseteq G$. $C(a)$ contains those elements of G that commute with the particular element $a \in G$.

To show: $C(a) \leq G$.

$C(a)$ is a non-empty subset of G, as we have for $a \in G$, $a \circ a = a \circ a \Rightarrow a \in C(a)$.

Let $x, y \in C(a)$. Then we have

$x \circ a = a \circ x$ and $y \circ a = a \circ y$

$\Rightarrow (x \circ a) \circ \bar{a}^1 = a \circ x \circ \bar{a}^1$

$\Rightarrow x \circ (a \circ \bar{a}^1) = a \circ x \circ \bar{a}^1$

$\Rightarrow x \circ e = a \circ x \circ \bar{a}^1$

$\Rightarrow x = a \circ x \circ \bar{a}^1$

$\Rightarrow (y \circ a) \circ \bar{a}^1 = a \circ y \circ \bar{a}^1$

$\Rightarrow y = a \circ y \circ \bar{a}^1$

$\Rightarrow y^{-1} = (a \circ y \circ \bar{a}^1)^{-1} = a \circ \bar{y}^1 \circ \bar{a}^1$

[Using Group properties]

Now $(x \circ y^{-1}) \circ a = (a \circ x \circ \bar{a}^1) \circ (a \circ \bar{y}^1 \circ \bar{a}^1) \circ a$

$= a \circ x \circ (\bar{a}^1 \circ a) \circ \bar{y}^1 \circ (\bar{a}^1 \circ a)$

$= a \circ x \circ e \circ \bar{y}^1 \circ e = a \circ (x \circ \bar{y}^1)$

$\Rightarrow x \circ \bar{y}^1 \in C(a)$.

$\therefore$ $C(a) \leq G$.

③ Cyclic subgroup:

$\langle a \rangle = \{a^n : n \in \mathbb{Z}\}$; $a \in G$.

$\langle a \rangle \subseteq G$. $\langle a \rangle$ contains all integral powers of $a \in G$.

$\langle a \rangle$ is called cyclic subgroup of G generated by the element $a \in G$.

To show: $\langle a \rangle \leq G$.

$\langle a \rangle$ is a non-empty subset of G, as we have $a \in \langle a \rangle$.

Let $x, y \in \langle a \rangle$. Then $x = a^r$ and $y = a^s$ for some $r, s \in \mathbb{Z}$.

Now $x \circ \bar{y}^1 = a^r \circ (a^s)^{-1} = a^r \circ \bar{a}^s = a^{r-s} \in \langle a \rangle$, since $r - s \in \mathbb{Z}$.

$\therefore$ $x, y \in \langle a \rangle \Rightarrow x \circ \bar{y}^1 \in \langle a \rangle$

So, $\langle a \rangle \leq G$.

Note: (i) $\langle a\rangle$ is the smallest subgroup of the group (G,o) containing the element a,
i.e., if (K,o) be any subgroup of (G,o) s.t. $a\in K$, then $\langle a\rangle \subset K$.

Because, since $a\in K$ and $K\leq G$, $a^n\in K$, $\forall n\in\mathbb{Z}$.
$\Rightarrow \langle a\rangle \subset K$.

(ii) $\langle a\rangle$ is a commutative subgroup of (G,o).

Because, if $x, y\in\langle a\rangle$, then $x=a^r$, $y=a^s$ for some $r,s\in\mathbb{Z}$.
$\therefore x o y = a^r o a^s = a^{r+s} = a^{s+r} = a^s o a^r = y o x$; $\forall x,y\in\langle a\rangle$.

(iii) If (G,o) be an additive group and $a\in G$. Then
$\langle a\rangle = \{na : n\in\mathbb{Z}\}$.

Examples: (1) In the additive group $(\mathbb{Z},+)$,
$\langle 1\rangle = (\mathbb{Z},+)$, $\langle 2\rangle = (2\mathbb{Z},+)$, $\langle 3\rangle = (3\mathbb{Z},+)$, $\cdots$,
$\langle m\rangle = (m\mathbb{Z},+)$, for m is a (+)ve integer.

(2) In the additive group $(\mathbb{Z}_5,+_5)$,
$\langle\bar{0}\rangle = \{n\bar{0} : n\in\mathbb{Z}\} = \{\bar{0}\}$
$\langle\bar{1}\rangle = \{n\bar{1} : n\in\mathbb{Z}\} = \{\bar{0},\bar{1},\bar{2},\bar{3},\bar{4}\} = \mathbb{Z}_5$,
[Since, $1.\bar{1}=\bar{1}$, $2.\bar{1}=\bar{2}$, $3.\bar{1}=\bar{3}$, $4.\bar{1}=\bar{4}$, $5.\bar{1}=\bar{0}$.]
$\langle\bar{2}\rangle = \{n\bar{2} : n\in\mathbb{Z}\} = \{\bar{0},\bar{1},\bar{2},\bar{3},\bar{4}\} = \mathbb{Z}_5$.
$\langle\bar{3}\rangle = \{n.\bar{3} : n\in\mathbb{Z}\} = \{\bar{0},\bar{1},\bar{2},\bar{3},\bar{4}\} = \mathbb{Z}_5$
$\langle\bar{4}\rangle = \{n.\bar{4} : n\in\mathbb{Z}\} = \mathbb{Z}_5$

Note: $\langle\bar{0}\rangle$ is the trivial cyclic subgroup of $(\mathbb{Z}_5,+_5)$
$\langle\bar{1}\rangle, \langle\bar{2}\rangle, \langle\bar{3}\rangle, \langle\bar{4}\rangle$ are the improper cyclic subgroups.

So, the cyclic subgroup generated by the identity element is the trivial subgroup. And the cyclic subgroup generated by each non-identity element is the improper subgroup.

Multiplicative Cyclic Subgroup

In the Klein's 4-group $(V,\cdot)$, $V=\{e,a,b,c\}$,
where $c=a\cdot b$, $a^2=b^2=c^2=e$.
$\langle e\rangle=\{e\}$, $\langle a\rangle=\{e,a\}$, $\langle b\rangle=\{e,b\}$, $\langle c\rangle=\{e,c\}$,
since $a^2=b^2=c^2=e$.

Here $\langle e\rangle$ is the trivial cyclic subgroup of $(V,\cdot)$,
and $\langle a\rangle$, $\langle b\rangle$, $\langle c\rangle$ are proper " " " "

Product of two subgroups:

Let $H \leq G$, $K \leq G$, then HK is a subset of G,

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

HK is, in general, not a subgroup of G.

When does HK form a subgroup of G?

The necessary and sufficient condition that HK is a subgroup of G iff $HK = KH$.

Necessary part $\longrightarrow$

Let $HK \leq G$. Let $x \in HK$. Then $x^{-1} \in HK$ $[\because HK \leq G]$.

Let $x^{-1} = h_1 k_1$ for some $h_1 \in H$, $k_1 \in K$.

$\Rightarrow (x^{-1})^{-1} = (h_1 k_1)^{-1} = k_1^{-1} h_1^{-1} \in KH$, since $k_1^{-1} \in K$, $h_1^{-1} \in H$.

$\Rightarrow x \in KH$ whenever $x \in HK$.

$\therefore HK \subset KH \longrightarrow$ (i)

Again, let $y \in KH$, then $y = k_2 h_2$ for some $k_2 \in K$, $h_2 \in H$.

Now $h_2^{-1} \in H$, $k_2^{-1} \in K$ $[\because H \leq G, K \leq G]$.

$\Rightarrow h_2^{-1} k_2^{-1} \in HK \Rightarrow (h_2^{-1} k_2^{-1})^{-1} \in HK$ $[\because HK \leq G]$.

$\Rightarrow k_2 h_2 \in HK \Rightarrow y \in HK$, whenever $y \in KH$

$\Rightarrow KH \subset HK \longrightarrow$ (ii)

From (i) & (ii) $\Rightarrow$ $\underline{HK = KH}$ whenever $HK \leq G$.

Sufficient part $\longrightarrow$

Let $HK = KH$.

Let $p, q \in HK$ s.t. $p = h_3 k_3$, $q = h_4 k_4$ for some $h_3, h_4 \in H$ and $k_3, k_4 \in K$.

Now $pq^{-1} = (h_3 k_3)(h_4 k_4)^{-1} = h_3 k_3 k_4^{-1} h_4^{-1} = h_3 (k_3 k_4^{-1}) h_4^{-1}$

$= h_3 k_5 h_4^{-1} = h_3 (k_5 h_4^{-1})$, where $k_5 = k_3 k_4^{-1} \in K$ $[\because K \leq G]$.

$= h_3 (h_5 k_6) = (h_3 h_5) k_6$, where $h_5 k_6 = k_5 h_4^{-1}$ $[\because HK = KH]$ for some $h_5 \in H$, $k_6 \in K$.

$= h_6 k_6$, where $h_6 = h_3 h_5 \in H$ $[\because H \leq G]$.

$\in HK$.

$\therefore p \in HK, q \in HK \Rightarrow pq^{-1} \in HK$

$\therefore \underline{HK \leq G}$ whenever $HK = KH$.

Theorem: If H & K be finite subgroups of a group G. Then $|HK| = \dfrac{o(H) \cdot o(K)}{o(H \cap K)}$.

Ex – 11. S.K. Mapa.

Q.9. Let G be a group and $H \leq G$. Prove that $gHg^{-1} = \{ghg^{-1} : h \in H\}$ is a subgroup of G, g being some fixed element of G.

Note: The subgroup gHg^{-1} of G is called the conjugate subgroup of H by g.

gHg^{-1} is a non-empty subset of G, since $e \in H \Rightarrow geg^{-1} = e \in gHg^{-1}$.

Let $h_1, h_2 \in H$. Then $gh_1g^{-1} \in gHg^{-1}$, $gh_2g^{-1} \in gHg^{-1}$.

And $(gh_1g^{-1})(gh_2g^{-1})^{-1} = (gh_1g^{-1})(gh_2^{-1}g^{-1})$

$= gh_1(g^{-1}g)h_2^{-1}g^{-1} = gh_1eh_2^{-1}g^{-1} = g(h_1h_2^{-1})g^{-1}$

$= gh_3g^{-1}$, where $h_3 = h_1h_2^{-1} \in H$, since $H \leq G$.

$\in gHg^{-1}$.

$\therefore$ $gHg^{-1} \leq G$.

Q.10. Let G be a group in which $(ab)^3 = a^3b^3$, $\forall\, a, b \in G$. Show that (i) $H = \{x^2 : x \in G\}$ is a subgroup of G,

(ii) $K = \{x^6 : x \in G\}$ " " " " G.

Given that $(ab)^3 = a^3b^3 \quad \forall\, a, b \in G \longrightarrow (1)$

$\Rightarrow abababab = a(a^2b^2)b$

$\Rightarrow b(ab)a = a^2b^2$ [by cancellation laws hold in G.]

$\Rightarrow (ba)(ba) = a^2b^2$

$\Rightarrow (ba)^2 = a^2b^2 \longrightarrow (2)$.

(i) Let $x, y \in G$. Then $x^2, y^2 \in H$.

Now $x^2(y^2)^{-1} = x^2(y^{-1})^2 = (y^{-1}x)^2$ [by (2)] $\in H$ [$\because y^{-1}x \in G$]

$\therefore x^2, y^2 \in H \Rightarrow x^2(y^2)^{-1} \in H \Rightarrow H \leq G$.

(ii) Let $x, y \in G$. Then $x^6, y^6 \in K$.

Now $x^6(y^6)^{-1} = x^6(y^{-1})^6 = x^3(x^3(y^{-1})^3)(y^{-1})^3$

$= x^3(xy^{-1})^3(y^{-1})^3$ [by (1), $x \in G$, $y^{-1} \in G$]

$= (x(xy^{-1})y^{-1})^3 = ((xx)(y^{-1}y^{-1}))^3 = (x^2(y^{-1})^2)^3$

$= ((y^{-1}x)^2)^3$ [by (2)] $= (y^{-1}x)^6 \in K$ [$\because y^{-1}x \in G$]

$\therefore x^6(y^6)^{-1} \in K \Rightarrow K \leq G$.

Some Subgroups:

① Find all subgroups of the group $(\mathbb{Z}, +)$.

$(\mathbb{Z}, +)$ is a cyclic group with 1 as a generator.

$\therefore$ Every subgroup of $(\mathbb{Z}, +)$ is cyclic.

$\therefore$ All subgroups of $(\mathbb{Z}, +)$ are given by the cyclic subgroups generated by different elements of $\mathbb{Z}$.

The cyclic subgroup generated by the integer m is $(m\mathbb{Z}, +)$.

$\therefore$ All subgroups of $(\mathbb{Z}, +)$ are $(m\mathbb{Z}, +)$, where $m \in \mathbb{Z}^+$.

② Prove that $(\mathbb{Q}, +)$ is a non-cyclic group. Deduce that $(\mathbb{R}, +)$ is non-cyclic.

If possible, let $(\mathbb{Q}, +)$ be cyclic & $\mathbb{Q} = \langle a \rangle$, $a \neq 0$.

There exists $\frac{1}{2}a \in \mathbb{Q}$ which cannot be expressed as ma, $m \in \mathbb{Z}$.

$\therefore$ $(\mathbb{Q}, +)$ is not cyclic.

If possible let $(\mathbb{R}, +)$ be cyclic, then since $\mathbb{Q} \subset \mathbb{R}$, and $(\mathbb{Q}, +)$ is non-cyclic, then $(\mathbb{R}, +)$ cannot be cyclic, as every subgroup of a cyclic group is cyclic.

③ Let $n \in \mathbb{Z}^+$, S = the set of all n n^{th} roots of unity. Show that $(S, \cdot)$ is a cyclic group. Find all possible generators.

$S = \{1, \alpha, \alpha^2, \cdots, \alpha^{n-1}\}$, $\alpha = \cos\frac{2\pi}{n} + i\sin\frac{2\pi}{n}$.

$(S, \cdot)$ is a finite group of $o(S) = n$.

n is the least +ve integer s.t. $\alpha^n = 1$, $o(\alpha) = n$

$\therefore$ $(S, \cdot)$ is a cyclic group generated by α.

Let $r \in \mathbb{Z}^+$. Then α^r is a generator of the group $(S, \cdot)$ if $r < n$ and $\gcd(r, n) = 1$

Then α^r becomes a special root of the eqn $x^n - 1 = 0$.

$\therefore$ The generators of the cyclic group $(S, \cdot)$ are the special roots of $x^n - 1 = 0$.

Note: For each +ve integer n, $\exists$ a cyclic group of order n.