Centre of a Group

Let G be a group. Let $Z(G) = \{x \in G \mid xg = gx \ \forall g \in G\}$ then $Z(G)$ is called centre of the group.

Theorem ~~Let Z(G)~~
Centre of a group G is a subgroup of G.

Proof: Let $Z(G)$ be the centre of the group.
Then $Z(G) \neq \phi$ as $e \in Z(G)$.

Again $x, y \in Z(G) \Rightarrow xg = gx$ and $yg = gy$ $\forall g \in G$.

$\therefore (xg)^{-1} = (gx)^{-1}$ and $(yg)^{-1} = (gy)^{-1}$
$\Rightarrow g^{-1}x^{-1} = x^{-1}g^{-1}$ and $g^{-1}y^{-1} = y^{-1}g^{-1}$ $\forall g \in G$

Now $g(xy^{-1}) = (gx)y^{-1} = (xg)y^{-1} = (xg)y^{-1}(gg^{-1})$
$= xg(y^{-1}g^{-1})g = xg(g^{-1}y^{-1})g$
$= x(gg^{-1})y^{-1}g = (xy^{-1})g \ \forall g \in G$

$\Rightarrow xy^{-1} \in G$
Hence $Z(G)$ is a subgroup of G.

Cyclic subgroup
$H = \{a^n \mid n \in Z\}$ is called cyclic subgroup of the group G, generated by a and is denoted by $\langle a \rangle$

Theorem: Every sub-group of a cyclic group is cyclic.

Proof: Let H be a sub-group of G.
If H be a trivial group, then $H = \{e\}$ is cyclic.

If H be a non-trivial subgroup of G and let $x(\neq e) \in H$. Since $G = \langle a \rangle$ cyclic and $x \in G$ ($\because H \subseteq G$), $x = a^k$ for some integer $k \neq 0$.

Now $x \in H \Rightarrow x^{-1} \in H \Rightarrow a^k \in H$ and $a^{-k} \in H$ for some integer $k \neq 0$. $\Rightarrow$ some +ve integral power of $a \in H$.

Let m be the least +ve integer such that $a^m \in H$.

We claim that $H = \langle a^m \rangle$

Let $y \in H$. Then $y \in G \Rightarrow y = a^b$ for some ~~integer~~ +ve integer b.

By division algorithm, $\exists$! $q, r \in \mathbb{Z}$ such that $b = qm + r$, $0 \leq r < m$.

Since $\langle H, \cdot \rangle$ is a group, $a^m \in H \Rightarrow a^{-qm} \in H$

Therefore $a^b \in H$, $a^{-qm} \in H \Rightarrow a^{b-qm} \in H$

$\Rightarrow a^r \in H$.

But m being a least +ve integer $a^m \in H$, $0 \leq r < m$ and $a^r \in H$, is a contradiction.

Hence it is possible only when $r = 0$.

Consequently $b = qm$ and hence $y = a^b \Rightarrow y = a^{qm} = (a^m)^q$, q is an integer.

$\therefore H = \{a^m\}$ is a cyclic group.

Ex: Find the cyclic sub-group of $\langle Z_{30}, + \rangle$ generated by 25.

Ans: g.c.d$(25, 30) = 5$, $[5] = [5].[1]$, generates a subgroup H containing $\frac{30}{5} = 6$ elements.

Thus $H = \{[0], [5], [10], [15], [20], [25]\}$, which is cyclic.