Conjugate Elements:

Let G be a group. Define a relation $\sim$ on G as for $a, b \in G$, $a \sim b \Leftrightarrow$ there exists $c \in G$ s.t. $a = c^{-1}bc$.

The above relation is an equivalence relation as,

(i) Reflexive Property:-

Since $a = a^{-1}aa$, $\forall a \in G$

Reflexivity holds

(ii) Symmetric Property:-

Let $a \sim b$ then $a = c^{-1}bc$ for some $c \in G$

$\Rightarrow cac^{-1} = b$

$\Rightarrow b = (c^{-1})^{-1}ac^{-1}$. $\quad c^{-1} \in G$

$\therefore b \sim a$.

Thus symmetric property holds.

(iii) Transitive Property:-

Let for $a, b, c \in G$, $a \sim b$ and $b \sim c$. Then there exists d and f in G s.t.

$a = d^{-1}bd$ and $b = f^{-1}cf$

$\cancel{a = b\, d^{-1}f^{-1}cdb = df}$

$\therefore a = d^{-1}f^{-1}cfd = (fd)^{-1}c(fd)$ $\quad [\because f, d \in G \Rightarrow fd \in G]$

Thus transitivity holds.

Hence the relation is an equivalence relation.

* Let $cl(a)$ denotes the equivalence class of a in G

i.e $cl(a) = \{x \in G : x \sim a\}$

$= \{x \in G : x = y^{-1}ay, y \in G\}$

$= \{y^{-1}ay : y \in G\}$

$=$ Set of all conjugate of a in G.

* If G acts on itself by conjugation i.e

$$g.a = gag^{-1}, \text{ then}$$

$$G_a = \{g \in G : g.a = a\}$$
$$= \{g \in G : gag^{-1} = a\}$$
$$= \{g \in G : ga = ag\} = C_G(a) = N(a)$$

$\therefore\ G_a = C_G(a) = N(a),\ \forall a \in G.$

And $O_a = \{g.a : g \in G\}$
$$= \{gag^{-1} : g \in G\} = cl(a).$$

Now by Orbit-Stablizer theorem,

$$|O_a| = |G : G_a|$$
$$\Rightarrow |cl(a)| = |G : N(a)| = |G : C_G(a)|$$

If G is finite, then $|cl(a)| = \dfrac{|G|}{|N(a)|}$,

i.e $|cl(a)| \,\big|\, |G|$.

So number of conjugates of a in G is the index of $N(a)$ in G.

<u>Result</u>: Prove that, $cl(a) = \{a\} \Leftrightarrow a \in Z(G)$.

<u>Proof</u>: let $cl(a) = \{a\}$

$$\Rightarrow gag^{-1} = a$$
$$\Rightarrow ga = ag\ \forall g \in G$$
$$\Rightarrow a \in Z(G).$$

<u>Conversely</u>, let $a \in Z(G)$

$$\Rightarrow ga = ag\ \forall g \in G.$$

Suppose $x \in cl(a)$

$$\Rightarrow x = gag^{-1}, \text{ for some } g \in G.$$
$$\Rightarrow x = agg^{-1} = ae$$
$$\Rightarrow x = a.$$

Thus $cl(a) = \{a\} \Leftrightarrow a \in Z(G)$.

Result: Suppose $a \in G$ has only two conjugates in G, then show that $N(a)$ is a normal subgroup of G.

Solⁿ: Suppose that $a \in G$ has only two conjugates in G.

So a, gag^{-1}, for some $\exists\, g \in G$ are two conjugates of a in G.

To show, $N(a) \trianglelefteq G$. for This, we will show that $N(a)$ has index 2 in G. i.e.

$$G = N(a) \cup N(a)g.$$

let $x \in G$. Consider $x^{-1}ax$

$\therefore\ x^{-1}ax = a$ or $x^{-1}ax = g^{-1}ag$

$\Rightarrow\ xa = ax$ $\quad\Rightarrow\ axg^{-1} = xg^{-1}a$

$\Rightarrow\ x \in N(a)$ $\quad\Rightarrow\ xg^{-1} \in N(a)$

$\Rightarrow\ x \in N(a)g$

$\therefore\ x \in N(a) \cup N(a)g.$

$\therefore\ G \subseteq N(a) \cup N(a)g$

$\Rightarrow\ G = N(a) \cup N(a)g$ $\quad$] $\because N(a) \subseteq G$ & $N(a)g \subseteq G$.

$\therefore N(a)$ has index 2.

Hence $N(a)$ is a normal subgroup of G.

* But converse is not true.

G is abelian $\Leftrightarrow$ $cl(a) = \{a\}$, $\forall a \in G$

Proof: Let G is abelian. Then $G = Z(G)$.

$\therefore\ a \in G \Leftrightarrow a \in Z(G)$, $\forall\, a \in G$

$\Leftrightarrow cl(a) = \{a\}$, $\forall\, a \in G$.

$N(a) = G \Leftrightarrow cl(a) = \{a\}$

Proof: let $N(a) = G$

So $g \in G = N(a) \Leftrightarrow ga = ag\ \forall\, g \in G$

$\Leftrightarrow\ a \in Z(G)$

$\Leftrightarrow\ cl(a) = \{a\}$.

Class Equation:-

Let G be a finite group and $g_1, g_2, \cdots, g_r$ be representation of the distinct conjugacy class of G not contained in the centre of G, then

$$|G| = |Z(G)| + \sum_{i=1}^{n} |G : C_G(g_i)|.$$

Proof: Let G acts on itself by conjugation i.e. $g.a = gag^{-1}$, $\forall\, a, g \in G$.

Then $O_a = cl(a)$, $\forall\, a \in G$.

The relation '.' is an equivalence relation. So G partitioned into disjoint classes, i.e.

$$G = \bigcup_{g \in G} cl(g)$$

$$\Rightarrow \quad |G| = \sum_{g \in G} |cl(g)|$$

$$= \sum_{g \in Z(G)} |cl(g)| + \sum_{\substack{g \notin Z(G) \\ g \in G}} |cl(g)|$$

We know that $g \in Z(G) \Leftrightarrow cl(g) = \{g\}$

$$\Rightarrow |cl(g)| = 1, \text{ for } g \in Z(G).$$

Thus, $$|G| = \sum_{g \in Z(G)} 1 + \sum_{\substack{g \notin Z(G) \\ g \in G}} |cl(g)|$$

Suppose $g_1, g_2, -- g_r$ are representation of the distinct conjugacy class of G not contained in $Z(G)$.

$$\therefore \sum_{\substack{g \in G \\ g \notin Z(G)}} |cl(g)| = \sum_{i=1}^{r} |cl(g_i)| = \sum_{i=1}^{r} |G : C_G(g_i)|$$

Hence $$|G| = |Z(G)| + \sum |G : C_G(g_i)|$$

This is known as Class Equation.

Examples.

(1) If G is an abelian group, then $G = Z(G)$.
Let $o(G) = n$. Then class equation of G canbe written as $|G| = Z(G)$.

$$= 1+1+1+ \cdots \text{ (n times)}$$

(2) $Q_8 = \{\pm 1, \pm i, \pm j, \pm k\}$

$Z(Q_8) = \{1, -1\}$.

Now $C_{Q_8}(i) = \langle i \rangle = \{\pm 1, \pm i\} = \langle -i \rangle = C_{Q_8}(-i)$

$C_{Q_8}(j) = \langle j \rangle = \{\pm 1, \pm j\} = \langle -j \rangle = C_{Q_8}(-j)$

$C_{Q_8}(k) = \langle k \rangle = \{\pm 1, \pm k\} = \langle -k \rangle = C_{Q_8}(-k)$

For $a \in Q_8$ and $a \notin Z(Q_8)$

$$|Q_8 : C_{Q_8}(a)| = 2.$$

So 'i' has two conjugates in Q_8 i.e i & $-i = kik^{-1}$
'j' has two conjugates in Q_8 i.e j & $-j = iji^{-1}$
'k' has two conjugates in Q_8 i.e k & $-k = jkj^{-1}$.

Thus $\{1\}, \{-1\}, \{i, -i\}, \{j, -j\}, \{k, -k\}$ are distinct conjugate classes. So class equation of Q_8 canbe written as

$$|Q_8| = |Z(Q_8)| + \sum_{\substack{a \in Q_8 \\ a \notin Z(Q_8)}} |Q_8 : C_{Q_8}(a)|$$

$$= 1+1+2+2+2.$$

(3) $D_4 = \{R_0, R_{90}, R_{180}, R_{270}, H, V, D, D'\}$

$Z(D_4) = \{R_0, R_{180}\}$

$\therefore$ $cl(R_0) = \{R_0\}$ and $cl(R_{180}) = \{R_{180}\}$.

Now, $C_{D_4}(R_{90}) = \langle R_{90} \rangle = \{R_0, R_{90}, R_{180}, R_{270}\} = \langle R_{270} \rangle = C_{D_4}(R_{270})$

$C_{D_4}(H) = \langle \{H, V\} \rangle = \{R_0, R_{180}, H, V\} = C_{D_4}(V)$

$C_{D_4}(D) = \langle \{D, D'\} \rangle = \{R_0, R_{180}, D, D'\} = C_{D_4}(D')$.

for $a \in D_4$ & $a \notin Z(D_4)$, we have

$$|D_4 : C_{D_4}(a)| = 2$$

So R_{90} has two conjugates in D_4 ie R_{90} & $R_{270} = DR_{90}D^{-1}$

'H' has two conjugates in D_4 ie H & $V = DHD^{-1}$,

'D' has two conjugates in D_4 ie D & $D' = VDV^{-1}$,

Thus $\{R_0\}$, $\{R_{180}\}$, $\{R_{90}, R_{270}\}$, $\{H, V\}$, $\{D, D'\}$ are distinct conjugate classes of D_4.

So class equation of D_4 can be written as

$$|D_4| = |Z(D_4)| + \sum_{\substack{a \in D_4 \\ a \notin Z(D_4)}} |D_4 : C_{D_4}(a)|$$

$$= 1+1+2+2+2.$$

<u>Theorem</u>:- If a group has order p^n, p a prime and $n \in \mathbb{N}$, then G has non-trivial centre.

<u>Proof</u>: Let G be a group and $o(G) = p^n$, p is prime & $n \in \mathbb{N}$.

If G is abelian, then $G = Z(G) = p^n > 1$.

So G has non-trivial centre.

If G is not abelian, then $G \neq Z(G)$.

ie $o(Z(G)) < o(G) = p^n$.

Now for any $x \in G$ such that $x \notin Z(G)$, we have

$xy \neq yx$, for some $y \in G$.

So $y \notin N(x)$, $\forall x \in G$ & $x \notin Z(G)$.

$\therefore$ $N(x) < G$

The class equation of G is given by

$$|G| = |Z(G)| + \sum_{i=1}^{r} |G : C_G(g_i)|,$$

where $g_1, g_2, \ldots, g_r$ are representation of nontrivial distinct conjugacy classes of G not contained in centre of G.

So, for each $g_i \in G$ and $g_i \notin Z(G)$, we have.

$C_G(g_i) = N(g_i) < G$.

and $Z(G) < N(g_i) = C_G(g_i)$ $\mid \because g_i \notin Z(G)$ but $g_i \in C_G(g_i)$

$\therefore \quad Z(G) < C_G(g_i) < G \; ; \forall \; g_i \in G \;\&\; g_i \notin Z(G)$.

$\Rightarrow |G : C_G(g_i)| > 1 \;, \forall \; g_i \in G \;\&\; g_i \notin Z(G)$.

$\Rightarrow |G : C_G(g_i)| \,\Big|\, |G| = p^n, \; \forall \; g_i \in G \;\&\; g_i \notin Z(G)$.

$\Rightarrow p \,\big|\, |G : C_G(g_i)| \; ; \forall \; g_i \in G \;\&\; g_i \notin Z(G)$

$\Rightarrow p \,\Big|\, \sum_{\substack{g \in G \\ g \notin Z(G)}} |G : C_G(g_i)|$

i.e. $\quad p \,\Big|\, \sum_{i=1}^{r} |G : C_G(g_i)|$

Thus $\quad p \,\Big|\, \left(|G| - \sum_{i=1}^{r} |G : C_G(g_i)|\right)$

By class equation of G, we get

$$|Z(G)| = |G| - \sum_{i=1}^{r} |G : C_G(g_i)|$$

$\therefore \quad p \mid Z(G)$.

$\Rightarrow |Z(G)| > 1$.

i.e. G has non-trivial centre.

Moreover, we claim that $|Z(G)| \neq p^{n-1}$ if $o(G) = p^n, n \in \mathbb{N}$.

Suppose that $|Z(G)| = p^{n-1}$, p is prime & $n \in \mathbb{N}$.

Now $\quad \left|\frac{G}{Z(G)}\right| = p$

$\Rightarrow \frac{G}{Z(G)}$ is cyclic

$\Rightarrow G$ is abelian

$\Rightarrow G = Z(G) = p^n$, a contradiction,

Thus $\quad |Z(G)| \neq p^{n-1}$

\# If G is non-abelian group and $|G| = p^3$, then $|Z(G)| = p$.

Since $|G| = p^3$, so $|Z(G)| > 1$ (by previous result)

As G is non-abelian, $Z(G) \neq G$. So $|Z(G)| < p^3$.

but $|Z(G)| \neq p^{3-1} = p^2$, so $Z(G) = p$.

\# A group of order p^2 is abelian. as $o(G) = p^2$ and $|Z(G)| > 1$ & $|Z(G)| \neq p^{2-1} = p$

So $|Z(G)| = p^2 = |G|$; Thus G must be abelian.

Ex: If G is a non-abelian group of order p^3, then find the number of distinct conjugacy classes of G.

Sol^n: Given G is a non-abelian and $o(G) = p^3$, p a prime

Then $|Z(G)| = p$.

Let k be the number of distinct conjugacy classes of G.

Then we have p classes of size 1, as $|Z(G)| = p$.

Since $Z(G) < N(a) \leq G, a \notin Z(G)$

$\therefore \ |N(a)| = p^2 . \Rightarrow |G : N(a)| = p$.

So remaining $(k-p)$ classes have order p.

Now by class equation of G, we have.

$$|G| = |Z(G)| + \sum_{\substack{a \in G \\ a \notin Z(G)}} |G : N(a)|$$

$$\Rightarrow p^3 = p + p(k-p) = p(k-p+1)$$

$$\Rightarrow p^2 = k - p + 1$$

$$\Rightarrow k = p^2 + p - 1.$$

* $|Q_8| = 8 = 2^3$, $|Z(Q_8)| = 2$

Number of distinct conjugacy classes of $Q_8 = 2^2 + 2 - 1$
$= 5$

Q. Find the class equation of a non-abelian group of order 15.

Sol^n: Let G be a non-abelian group of order 15. So $G \neq Z(G)$ and thus $|Z(G)| < |G| = 15$.

So possible order of $Z(G)$ are 1, 3, 5.

If $|Z(G)| = 5$, then $\left|\frac{G}{Z(G)}\right| = 3 \Rightarrow \frac{G}{Z(G)}$ is cyclic $\Rightarrow G$ is abelian, a contradiction.

If $|Z(G)| = 3$, then $\left|\frac{G}{Z(G)}\right| = 5 \Rightarrow G$ is abelian, a contradiction.

So $|Z(G)| = 1$. So there is only one conjugate class of order 1.

The rest are of order either 3 or 5.

Thus the class equation of G is given by

$$|G| = 15 = 1 + 3 + 3 + 3 + 5.$$