UNIT – 4 [Class Eqns & Sylow's Theorems].

Conjugacy relation and conjugacy classes:–

A relation ρ defined on a group G by "$x \rho y$ iff y is conjugate to x", is an equivalence relation on G.
$\rho = \{(x,y) \in G \times G : y = gxg^{-1}$ for some $g \in G\}$.

Because, for any $x \in G$, $x = exe^{-1} \Rightarrow x\rho x$ (ρ is reflexive).

For $x, y \in G$ and $x\rho y$, $\exists$ an element $g \in G$ s.t. $y = gxg^{-1}$.
$\Rightarrow x = g^{-1}yg = pyp^{-1}$ where $p(=g^{-1}) \in G$
$\Rightarrow y\rho x$ (ρ is symmetric)

For $x, y, z \in G$ and $x\rho y$, $y\rho z$. The $\exists$ $g, h \in G$ s.t.
$y = gxg^{-1}$, $z = hyh^{-1} \Rightarrow z = h(gxg^{-1})h^{-1} = (hg)x(hg)^{-1}$
$\Rightarrow x\rho z$, since $hg \in G$.

$\therefore$ ρ is transitive.
$\therefore$ ρ is an equivalence relation on G.

① ρ is said to be the conjugacy relation on G. And G is partitioned into ρ-equivalence classes, called the conjugacy classes.

For $a \in G$, the conjugacy class of $a = cl(a) = \{gag^{-1} : g \in G\}$.
So, $cl(a)$ is the set of those elements which are conjugate to a.

② $cl(a) = \{a\}$ if $a \in Z(G)$ and conversely. Trivial Conjugacy class.

$a \in Z(G) \Rightarrow gag^{-1} = agg^{-1} = ae = a$, $\forall g \in G$. [$\because$ a Commutes with each $g \in G$].
$\Rightarrow cl(a) = \{a\}$.

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

Note: (i) The elements of $Z(G)$ are self-conjugate elements.
(ii) If $a \in Z(G)$, $cl(a) = \{a\}$, is called a trivial conjugacy class.

Theorem: If G is a finite group, and $a \in G$, then $|cl(a)| = [G : C(a)]$, where $C(a)$ is the centralizer of a in G.

Proof: The two conjugates of a determined by g and h in G are gag^{-1} and hah^{-1} respectively.

Now $gag^{-1} = hah^{-1} \Leftrightarrow (h^{-1}g)a = a(h^{-1}g) \Leftrightarrow h^{-1}g \in C(a)$.

$\Leftrightarrow gC(a) = hC(a)$

$\therefore$ Two conjugates gag^{-1} and hah^{-1} of a are

(i) same if g and h belong to the same left coset of $C(a)$ in G.

(ii) different if g and h " " " different " " ".

Therefore, the no. of distinct conjugates of a in G equals to the no. of different left cosets of $C(a)$ in G.

$\therefore |cl(a)| = [G : C(a)]$. (proved)

Note: $O(G) = [G : C(a)] \cdot O(C(a))$.

$= |cl(a)| \cdot O(C(a))$.

$\Rightarrow |cl(a)|$ is a divisor of $O(G)$.

CLASS EQUATION

Theorem: If G be a finite group and Z be its centre, then show that $O(G) = O(Z) + \sum_{i=1}^{m} |C_i|$, where $|C_i|$ denotes the number of distinct elements in the conjugacy class C_i.

Proof: If $a \in Z$, then $cl(a) = \{a\}$, so that $|cl(a)| = 1$.

If $a \in G - Z$, then $|cl(a)| = [G : C(a)]$, $C(a)$ is the centraliser of a.

Let $C_i = cl(a_i)$, $a_i \in G - Z$; $i = 1, 2, \dots, m$; be distinct conjugacy classes of $G-Z$.

G is partitioned into distinct conjugacy classes.

$\therefore O(G) = O(Z) + |G - Z|$

$= O(Z) + |cl(a_1)| + |cl(a_2)| + \dots + |cl(a_m)|$.

i.e; $O(G) = O(Z) + \sum_{i=1}^{m} |C_i|$

$O(G) = O(Z) + |C_1| + |C_2| + \dots + |C_m|$ is called the class equation of G.

Class Equation :

Let us suppose G is a finite group. Then the number of conjugacy classes are finite.

$\therefore$ G can be partitioned into distinct conjugacy classes as follows:

$$G = cl(a_1) \cup cl(a_2) \cup cl(a_3) \cup \cdots \cup cl(a_n).$$

Let $a \in G$ s.t. $a \in Z(G)$. Then $cl(a) = \{a\}$ so that $|cl(a)| = 1$.

If $a \in G - Z(G)$, then $cl(a) \cap Z(G) = \phi$. Hence we can partition G as follows:

$$G = Z(G) \cup cl(x_1) \cup cl(x_2) \cup \cdots \cup cl(x_m),$$ where $cl(x_i)$ are the distinct conjugacy classes containing more than one element such that $cl(x_i) \cap Z(G) = \phi$.

$$\therefore \quad |G| = |Z(G)| + \sum_{i=1}^{m} |cl(x_i)| \longrightarrow$$ class equation of a finite group G.

We have $|cl(a)| = [G : C(a)]$.

So the class equation of a finite group G can be written as

$$|G| = |Z(G)| + \sum_{i=1}^{m} [G : C(x_i)] = |Z(G)| + \sum_{i=1}^{m} \frac{|G|}{|C(x_i)|}.$$

Note: $a \in Z(G) \Rightarrow cl(a) = \{a\}$, called trivial conjugacy class and $cl(x_i)$ are the distinct non-trivial conjugacy classes.

④ OR

Example: Find the conjugacy classes in the group S_3 and write down the class equation

$S_3 = \{\rho_0, \rho_1, \rho_2, \rho_3, \rho_4, \rho_5\}$, $\rho_0 = i$, $\rho_1 = (1\,2\,3)$, $\rho_2 = (1\,3\,2)$, $\rho_3 = (2\,3)$, $\rho_4 = (1\,3)$, $\rho_5 = (1\,2)$.

$cl(\rho_0) = \{x \rho_0 x^{-1} ;\ x \in S_3\} = \{\rho_0\} = Z(G)$.

$\therefore$ ρ_0 is a self-conjugate element.

$cl(\rho_1) = \{x \rho_1 x^{-1} ;\ x \in S_3\}$

Now we have $o(\rho_1) = 3$, $o(\rho_3) = o(\rho_4) = o(\rho_5) = 2$.

$\therefore$ ρ_3, ρ_4, ρ_5 cannot be conjugate to ρ_1, since every conjugate to an element must have the same order as that of the element.

$\therefore cl(\rho_1) = \{\rho_1, \rho_2\}$.

$\rho_3 \rho_1 \rho_3^{-1} = \rho_3 \rho_1 \rho_3 = \rho_2 \Rightarrow \rho_2$ is conjugate to ρ_1

$\rho_4 \rho_3 \rho_4^{-1} = \rho_4 \rho_3 \rho_4 = \rho_5 \Rightarrow \rho_5$ " " " ρ_3.

$\rho_5 \rho_3 \rho_5^{-1} = \rho_5 \rho_3 \rho_5 = \rho_4 \Rightarrow \rho_4$ " " " ρ_3.

$\therefore cl(\rho_3) = \{\rho_3, \rho_4, \rho_5\}$

$\therefore S_3 = cl(\rho_0) \cup cl(\rho_1) \cup cl(\rho_3)$

The class equation of S_3 is given by

$$o(S_3) = o(Z) + |cl(\rho_1)| + |cl(\rho_3)|$$

$$6 = 1 + 2 + 3.$$

<u>Theorem</u>: If G be a group and $O(G) = p^r$, p is a prime and r be a +ve integer, then G has a non-trivial centre. [i.e. $Z(G) \neq \{e\}$].

<u>Proof</u>: Trivial case: $\rightarrow$ If G be abelian then $Z(G) = G$. Therefore we assume that G is a non-abelian group.

Since G is a finite group, the number of conjugacy classes is finite. Let the distinct conjugacy classes of $G - Z$ be $cl(a_i)$, $a_i \in G - Z$, $i = 1, 2, \cdots, m$.
We have $|cl(a_i)| = [G : C(a_i)]$, where $C(a_i)$ is the centraliser of a_i in G.
Then We have the class equation of G:

$$O(G) = O(Z) + |cl(a_1)| + |cl(a_2)| + \cdots + |cl(a_m)|.$$

Now each $|cl(a_i)|$ is a divisor of $O(G)$ and $|cl(a_i)| > 1$.
$\Rightarrow$ each $|cl(a_i)|$ is p, or p^2, $\cdots$, or p^r. [$\because p$ is prime]
Since $p \mid O(G)$ and $p \mid |cl(a_i)|$ for each $i = 1, 2, \cdots, m$,
$\Rightarrow p \mid O(Z)$. [This is evident from the class equation]
$\therefore Z$ is a subgroup having at least p elements and therefore non-trivial.
Hence the theorem.

<u>Theorem</u>: If G be a group and $O(G) = p^2$, where p is a prime, then G is abelian.

<u>Proof</u>: Since $O(G) = p^2$, by Lagrange's theorem, $O(Z) \mid p^2$. $\Rightarrow O(Z) = 1$, or p, or p^2. [$\because p$ is a prime].
$O(Z) \neq 1$, since $O(G) = p^2$, G has a non-trivial centre, by the above theorem.
Let $O(Z) = p$. Then $O(G/Z) = \frac{O(G)}{O(Z)} = \frac{p^2}{p} = p$, a prime.
$\Rightarrow G/Z$ is cyclic, which is not TRUE because for any group G, G/Z cannot be non-trivial cyclic.
$\therefore O(Z) = p^2 = O(G) \Rightarrow Z = G$ [$\because Z \leq G$]
$\Rightarrow G$ is abelian, as Z is abelian.