Ex: Let G be a non-abelian group of order p^3, p is a prime. Prove that $|Z(G)| = p$.

Since $|G| = p^3$, $|Z| > 1$.

Also since $Z(G) \leq G$, $|Z(G)| = p$, or p^2, or p^3.

If $|Z(G)| = p^3$, then $G = Z(G) \Rightarrow G$ is abelian, contradiction.

So $|Z(G)| \neq p^3$.

If $|Z(G)| = p^2$, then $|G/Z(G)| = \frac{|G|}{|Z(G)|} = \frac{p^3}{p^2} = p$.

$\Rightarrow \{G/Z(G)\}$ is cyclic $\Rightarrow G$ is abelian, a contradiction.

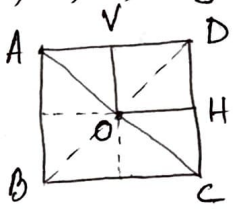
$\therefore |Z(G)| \neq p^2$.

Thus $|Z(G)| = p$. (proved)

Ex: Find the conjugacy classes in D_4 and write down the class equation for D_4.

Dihedral group $D_4 = \{R_0, R_{90}, R_{180}, R_{270}, H, V, D, D'\}$.

Symmetries of a square.



$O(D_4) = 8$.

$cl(R_0) = \{x R_0 x^{-1} : x \in D_4\} = \{R_0\} = Z(D_4)$.

R_0 is self-conjugate element.

We have, $O(R_{90}) = O(R_{270}) = 4$; $O(R_{180}) = 2 = O(H) = O(V) = O(D) = O(D')$.

$\therefore cl(R_{90}) = \{R_{90}, R_{270}\} = cl(R_{270})$; since R_{90} is conjugate to R_{270}, because

$$H R_{90} H^{-1} = \begin{pmatrix} A & B & C & D \\ B & A & D & C \end{pmatrix} \begin{pmatrix} A & B & C & D \\ B & C & D & A \end{pmatrix} \begin{pmatrix} A & B & C & D \\ B & A & D & C \end{pmatrix}^{-1}$$

$$= \begin{pmatrix} A & B & C & D \\ D & A & B & C \end{pmatrix} = R_{270}$$

$\Rightarrow R_{270}$ is conjugate to R_{90}.

Again, R_{180}, H, V, D, D' cannot be conjugate to R_{90} & R_{270}.

One may verify that —

$cl(R_{180}) = \{R_{180}\}$; $cl(H) = \{H, V\} = cl(V)$; $cl(D) = \{D, D'\} = cl(D')$.

Here, R_{180} is self-conjugate element.

And H is conjugate to V and D is conjugate to D'.

$\therefore D_4 = cl(R_0) \cup cl(R_{90}) \cup cl(R_{180}) \cup cl(H) \cup cl(D)$

The class equation of D_4 is given by

$$O(D_4) = |cl(R_0)| + |cl(R_{180})| + |cl(R_{90})| + |cl(H)| + |cl(D)|$$

$$\text{i.e., } 8 = \underbrace{(1 + 1)}_{O(Z)} + 2 + 2 + 2.$$

NOTE: According to Lagrange's theorem, the order of any subgroup of a finite group G divides $O(G)$.

Now the question naturally arises whether the converse of Lagrange's theorem holds, i.e., given a factor d of $O(G)$, does there exist a subgroup of G of order d?

The answer is "NO" in general.

For example, the alternating group A_4 has no subgroup of order 6.

$O(A_4) = \frac{1}{2} \times 4! = 12$.

Let $H \leq A_4$ and $[A_4 : H] = 2$. Then for every $x \in A_4$, $x^2 \in H$.

The elements of A_4 are: (1), $(12)(34)$, $(13)(24)$, $(14)(23)$, (123), (132), (124), (142), (134), (143), (234), (243).

Denoting these all elements by f_i, $i = 1, 2, \cdots, 12$,

we have $f_i^2 = (1) = f_1$, $\forall\, i = 1, 2, 3, 4$.

and $f_i^2 = f_{i+1}$, $\forall\, i = 5, 7, 9, 11$.

and $f_i^2 = f_{i-1}$, $\forall\, i = 6, 8, 10, 12$.

} There are more than 6 squares in A_4 and each of them must belong to H of order 6, which is not possible.

However, There are important special cases when the converse of Lagrange's theorem is TRUE:

(i) when G is an abelian group.

(ii) if p is a prime and $p \mid O(G)$, then G has a subgroup of order p → Known as CAUCHY'S THEOREM.

(iii) More generally (than (ii)), if $q = p^r$ (p is a prime), r is a +ve integer, and $q \mid O(G)$, then G has a subgroup of order $q (= p^r)$ → SYLOW'S FIRST THEOREM.

(iv) As a particular case of (iii), if G is a p-group for some prime p, then for any factor d of $O(G)$, there exists a subgroup of order d in G.

Cauchy's Theorem & Sylow's Theorems :-

- We know that the converse of Lagrange's theorem does not hold.
  i.e., if G is a finite group of order $n > 1$ and m is a +ve divisor of n, then G may not have a subgroup of order m.
- However, Cauchy's theorem and Sylow's theorems provide some information regarding partial converse of Lagrange's theorem.
- Lagrange's theorem gives a necessary condition for the existence of subgroups.
- Sylow's theorem give a sufficient condition for the existence of subgroups.

Cauchy's Theorem →

Let G be a finite group and p be a prime divisor of $O(G)$, then G has an element of order p and hence a subgroup of order p.

With the help of Cauchy's theorem, one may prove that the converse of Lagrange's theorem holds for finite Abelian groups.

Th. i.e., if G be a finite Abelian group and d be a +ve divisor of $O(G)$, then G has a subgroup of order d.

Proof: If $d = 1$, then the subgroup is $\{e\}$ of order 1.
If $O(G) = n = 1$, then $d = 1$, the result follows.
Let us assume that $d > 1$, $n > 1$.
We prove the result by induction on n.
If $n = 2$, then $d = 2 = n$ and G is the subgroup itself of order 2.
Let us suppose the result is true for all finite Abelian groups of order m s.t. $2 \leq m < n$.

Let p be a prime s.t. $p|d$. Then $\exists$ an integer k_1 s.t. $d = p \cdot k_1$. By Cauchy's theorem, G has a subgroup H of order p. Since G is abelian, H is normal and the quotient group G/H exists.

Now $1 \leq |G/H| = \frac{|G|}{|H|} < |G|$, and $\frac{|G|}{|H|} = \frac{n}{p}$.

Again, $d|n$, so $\exists$ an integer k_2 s.t. $n = d \cdot k_2$.

$\therefore \frac{|G|}{|H|} = \frac{n}{p} = \frac{d \cdot k_2}{p} = \frac{p \cdot k_1 \cdot k_2}{p} = k_1 k_2$

$\Rightarrow k_1$ divides $\frac{|G|}{|H|} = |G/H|$.

Hence, from the induction hypothesis, G/H has a subgroup, say K/H s.t. $|K/H| = k_1$, where $K \leq G$. Now $|K| = |K/H| \cdot |H| = k_1 \cdot p = d$.

$\Rightarrow \exists$ a subgroup K of G s.t. $|K| = d$. (proved)

Some important definitions:-

Definition 1: Let p be a prime. A group G is said to be a p-group if the order of each element of G is a power of p.

Definition 2: A subgroup H of a group G is called a p-subgroup if H is a p-group.

Examples:

1. Klein 4-group is a p-group, where $p=2$
2. The group of symmetries of a square is also a p-group, where $p=2$
3. In fact, any group of order p^n is a p-group, since the order of each element must divide the $O(G)$.

Definition 3: A subgroup P of G is called a Sylow p-subgroup of G, if P is a p-subgroup and is not properly contained in any other p-subgroup of G, i.e., P is a maximal p-subgroup of G.

Alternative definition 3: Sylow p-subgroup $\longrightarrow$ Let G be a finite group and p be a prime divisor of $|G|$. If $p^k \mid |G|$ and $p^{k+1} \nmid |G|$, then any subgroup of G of order p^k is called a Sylow p-subgroup of G.

Conjugate Subgroups $\longrightarrow$ Let H and K be subgroups of G. If there exists an element $g \in G$ s.t. $H = gKg^{-1}$, then we say that H and K are conjugate in G.

A unique Sylow p-subgroup is normal.

i.e., A Sylow p-subgroup of a finite group G is a normal subgroup of G iff it is the only Sylow p-subgroup of G.

Necessary and sufficient condition for a finite group G to be a p-group.

Statement → Let G be a non-trivial group. Then G is a finite p-group if and only if $|G| = p^K$, $K \in Z^+$.

Proof → Let G be a finite p-group. Also let q be a prime s.t. $q \neq p$ and $q \mid |G|$.
Then by Cauchy's theorem G has an element of order q, which contradicts the fact that G is a p-group.
$\therefore$ p is the only prime divisor of $|G|$.
$\Rightarrow |G| = p^K$, for some $K \in Z^+$.
Conversely, let $|G| = p^K$. Then by Lagrange's theorem, the order of each element of G is a power of p. $\Rightarrow$ G is a p-group.

Theorem: If G be a non-trivial finite p-group, then $|Z(G)| > 1$.
i.e. the centre of a p-group is non-trivial.

Proof → Trivial Case: if G be abelian, then $Z(G) = G$.
$\Rightarrow |Z(G)| > 1$. [$\because |G| = p^K$, $K \geq 1$, $K \in Z^+$].
$\therefore$ Z(G) is non-trivial.
Let us consider the class equation:

$$|G| = |Z(G)| + \sum_{a \notin Z(G)} [G : C(a)].$$

Let $a \in G$ s.t. $a \notin Z(G)$. Now C(a) is a proper subgroup of G where $|G| = p^K$, $K \geq 1$, $K \in Z^+$.
Then $p \mid [G : C(a)]$ $\forall$ $a \notin Z(G)$.

$$\Rightarrow p \mid \sum_{a \notin Z(G)} [G : C(a)].$$

Since $p \mid |G|$ also, we have from the class eqn,

$$p \mid Z(G) \Rightarrow |Z(G)| > 1. \quad \text{(proved)}.$$

Sylow's Theorems:

1. Sylow's First Theorem → [Existence of subgroups of prime-power order]

Let G be a finite group of order $p^r m$, where p is a prime, $r, m \in \mathbb{Z}^+$, and $\gcd(p, m) = 1$. Then G has a subgroup of order p^k for $0 \le k \le r$.

2. Sylow's Second Theorem →

Let G be a finite group of order $p^r m$, where p is a prime, $r, m \in \mathbb{Z}^+$ and $\gcd(p, m) = 1$. Then any two Sylow p-subgroups of G are conjugate, and therefore isomorphic.

3. Sylow's Third Theorem →

Let G be a finite group of order $p^r m$, where p is a prime, $r, m \in \mathbb{Z}^+$, and $\gcd(p, m) = 1$. Then the number n_p of Sylow p-subgroups of G is $1 + kp$ for some $k \ge 0$, $k \in \mathbb{Z}$ and $n_p \mid |G|$.

Applications of Sylow's theorems :—

① Let G be a finite group and H be a Sylow p-subgroup of G. Then H is a unique Sylow p-subgroup of G if and only if H is normal in G.

Proof: Let $|G| = p^r m$, where p is prime, $r, m \in \mathbb{Z}^+$, $\gcd(p, m) = 1$.
Let $g \in G$, then $gHg^{-1} \le G$ and $|gHg^{-1}| = |H| = p^r$.
$\Rightarrow gHg^{-1}$ is also a Sylow p-subgroup of G.
Since G contains only one Sylow p-subgroup H, then $gHg^{-1} = H$, $\forall g \in G$. $\Rightarrow H \triangleright G$.
The converse follows from the Sylow's 2nd theorem i.e., any two Sylow p-subgroups of G are conjugate, i.e., $gHg^{-1} = H (\forall g \in G) \Rightarrow H$ is a unique Sylow p-subgroup.

② If G be a group of order $p \cdot q$, where p, q are primes such that $p > q$ and $q \nmid p-1$, then G is a cyclic group.

Example: Show that every group of order 35 is cyclic.

Here let G be a group s.t. $|G| = 35 = 7 \cdot 5 \equiv p \cdot q$ where $7 > 5$ $(p > q)$ and $5 \nmid (7-1)$.
$\Rightarrow$ G is a cyclic group.

③ Show that every group of order 14 has six elements of order 7.

Let G be a group s.t. $|G| = 14 = 2 \cdot 7$
Since $7 \mid |G|$, by Cauchy's theorem G has a subgroup H of order 7.
Let us suppose there exist two distinct subgroups H & K of order 7.
then $|H \cap K| = 1$ and $|HK| = \frac{|H||K|}{|H \cap K|} = \frac{7 \cdot 7}{1} = 49 > 14 = |G|$.
$\Rightarrow$ G has only one subgroup of order 7.
Let $a \in G$ s.t. $o(a) = 7$. Then $o(\langle a \rangle) = 7 = |H|$
$\therefore H = \langle a \rangle \Rightarrow a \in H$. $\Rightarrow$ H contains all elements of order 7 except the identity element.
$\therefore$ H has 6 elements of order 7
$\Rightarrow$ G " 6 " " " 7.

④ Find all sylow 3-subgroups of S_4.

$|S_4| = 4! = 24 = 2^3 \cdot 3$.
By the sylow theorem, S_4 has sylow 3-subgroups of order 3 each.
Now any subgroup of order 3 is a cyclic subgroup generated by an element of order 3 in S_4. If $a \in S_4$ & $o(a) = 3$, then $H = \langle a \rangle$ is a subgroup of order 3. In S_4, an element α is of order 3 iff α is a 3-cycle.
Hence the subgroups of order 3 in S_4 are:
$\{e, (123), (132)\}$, $\{e, (124), (142)\}$, $\{e, (134), (143)\}$, and $\{e, (234), (243)\}$.

(5) Show that every group of order 45 has a normal subgroup of order 9.

Solution: Let G be a group s.t. $|G| = 45 = 3^2 \cdot 5$.
Let n_3 denote the number of Sylow 3-subgroups of G. Then $n_3 = 3K+1$ for some integer $K \geq 0$, and $n_3 \mid 45$.
If $K=0$, $n_3 = 1$ which divides $45 (= |G|)$.
For any $K \geq 1$, $n_3 \nmid |G|$. Hence G contains a unique Sylow 3-subgroup H of order 9.
Consequently G has a normal subgroup of order 9.

(6) If a group G of order 52 contains a normal subgroup of order 4, show that G is a commutative group.

Let G contain a normal subgroup H of order 4.
Then H is a commutative group.
Now $|G| = 52 = 13 \cdot 2^2$.
Let n_{13} denote the number of Sylow 13-subgroups of G. Then $n_{13} = 13K+1$, for some integer $K \geq 0$, and $n_{13} \mid |G|$.
If $K=0$, $n_{13} = 1$ which divides $52 (= |G|)$.
For any $K \geq 1$, $n_3 \nmid |G|$. Hence G contains a unique Sylow 13-subgroup, say K.
Then $K \triangleright G$ and $|K| = 13$ and $K \cap H = \{e\}$.
Since $|KH| = \dfrac{|K||H|}{|K \cap H|} = \dfrac{13 \cdot 4}{1} = 52 = |G|$

$\Rightarrow G = K \times H$. Both K and H are commutative.
$\therefore$ G is also commutative.