p-Group:

A p-Group is a group in which every non-identity element has order p^r, p is prime and $r \in \mathbb{N}$.

Ex: (1) K_4, $|K_4| = 4 = 2^2$

$o(a) = 2$, $\forall\ e \neq a \in K_4$.

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

$o(a) = 2$ or 2^2, $\forall\ e \neq a \in Q_8$.

(3) $(P(N), \Delta)$, $|P(N)| = 2^x$

$o(a) = 2$, $\forall\ e \neq a \in P(N)$

(4) $G = \left\{ \mathbb{Z} + \frac{m}{p^n} : m, n \in \mathbb{Z}^+ \text{ \& p is a fixed prime} \right\}$.

G is a subgroup of $\frac{\mathbb{Q}}{\mathbb{Z}}$.

Now $p^n\left(\mathbb{Z} + \frac{m}{p^n}\right) = \mathbb{Z} + m = \mathbb{Z}$

$\Rightarrow o\left(\mathbb{Z} + \frac{m}{p^n}\right) \Big| p^n$

$\Rightarrow o\left(\mathbb{Z} + \frac{m}{p^n}\right) = p^r$, $0 < r < n$

Remarks:

(1) A finite p-group has non-trivial centre.

(2) A p-group may or may not be abelian.

Scanned with CamScanner

Theorem: Let G be a finite group, then G is a p-group iff $o(G) = p^n$, where p is a prime and $n \in \mathbb{N}$.

Proof: Let G be a finite p-group. so by definition, every non-identity element has order p^r, $r \in \mathbb{N}$

i.e $o(x) = p^r$, $1 \leq r < n$, $e \neq x \in G$.

Suppose q is another prime such that $q \mid o(G)$.

So by Cauchy's theorem, there exists $e \neq y \in G$ such that $o(y) = q$

$$\Rightarrow q = p^r, \text{ for some } r \in \mathbb{N}.$$

$$\Rightarrow p \mid q$$

$$\Rightarrow p = q.$$

So p is the only prime which divides $o(G)$.

Thus $o(G) = p^n$, $n \in \mathbb{N}$.

Conversely, let $o(G) = p^n$; $n \in \mathbb{N}$

Since, for all $x \in G$,

$$o(x) \mid o(G) = p^n$$

$$\therefore o(x) = p^r, 1 \leq r \leq n.$$

So G is a p-group.

Result: Let G be a finite group with the property that if H, K are two subgroups of G then either $H \subseteq K$ or $K \subseteq H$. Show that G is a cyclic p-group.

Solution: let H, K be two subgroups of a finite group G such that either $H \subseteq K$ or $K \subseteq H$.

Case I: If G has no proper subgroups, then G is a cyclic group of prime order. Thus we have done.

Case II: Suppose that G has a proper Subgroup H
To show G is cyclic p-group.
Suppose G is not cyclic.
Since $H \subset G$, So there exists $x \in G$ s.t. $x \notin H$
Now, let $K = \langle x \rangle$, then $K \nsubseteq H$ and $K \neq G$.
But given hypothesis, $H \subseteq K$ or $K \subseteq H$
So we get a contradiction, Hence G is cyclic.

Next, let p and q be two distinct primes such that $p \mid o(G)$ and $q \mid o(G)$.

Since G is cyclic, there exists two subgroups H and K of G such that
$o(H) = p$ and $o(K) = q$.
$\Rightarrow$ Neither $o(H) \nmid o(K)$ nor $o(K) \nmid o(H)$
$\Rightarrow$ Neither $H \nsubseteq K$ nor $K \nsubseteq H$
Thus We get a contradiction. So $p = q$
Hence there is only one prime which divides $o(G)$ i.e G is a p-group.

Result: Converse of the above result holds, i.e. Let G be a finite cyclic p-group. Show that if H and K are any two subgroups of G then either $H \subseteq K$ or $K \subseteq H$.

Solution: Let $G = \langle a \rangle$
Then $o(G) = o(a) = p^n$ (say), for some prime p.

Let H be a subgroup of G, hence H is cyclic.
Suppose $H = \langle a^m \rangle$.
Let $d = \gcd(m, p^n)$. Then there exist integers x, y s.t. $d = mx + p^n y$

$$\Rightarrow a^d = a^{mx + p^n y}$$
$$= a^{mx} \cdot a^{p^n y}$$
$$= (a^m)^x \cdot e \qquad \{\because o(a) = p^n\}$$
$$\Rightarrow a^d = (a^m)^x \in H$$
$$\therefore \langle a^d \rangle \subseteq H \quad \text{——— (1)}$$

Since $d \mid m \Rightarrow m = dq$
$$\Rightarrow a^m = (a^d)^q \in \langle a^d \rangle$$
$$\Rightarrow \langle a^m \rangle \subseteq \langle a^d \rangle$$
$$\therefore H \subseteq \langle a^d \rangle. \quad \text{——— (2)}$$

From (1) & (2) $H = \langle a^d \rangle$,

Also $d \mid p^n$. So $d = p^i$, $1 \leq i < n$
So $H = \langle a^{p^i} \rangle$

Let K be ~~another~~ a subgroup of G s.t. $H \neq K$.
$K = \langle a^{p^k} \rangle$, $1 \leq k < n$
Then either $k \leq i$ or $k \geq i$.
Suppose $i \geq k$. So let $i = k + t$, $0 \leq t \in \mathbb{Z}$.
Now $a^{p^i} = a^{p^{k+t}} = (a^{p^k})^{p^t} \in K$
$$\therefore \langle a^{p^i} \rangle \subseteq K$$
$$\Rightarrow H \subseteq K.$$

Similarly $K \subseteq H$ if $k \geq i$.

-

Result: Show that every proper subgroup of a finite p-group G is a proper subgroup of its normalizer in G.

Solution:- Let $o(G) = p^n$ and $H \subsetneq G$.

To show, $H \subsetneq N(H)$ i.e. there exists $g \in G$, $g \notin H$ such that $g \in N(H) \Rightarrow gHg^{-1} = H$.

To prove this, we use the method of induction on n.

Let $n=1$, $o(G) = p$. So G is cyclic group.

Since $H \neq G$. So $o(H) = 1$. So $H = \{e\}$

Now, for all $e \neq g \in G$,

$$gHg^{-1} = g\{e\}g^{-1} = \{e\} = H$$

$$\Rightarrow g \in N(H) \text{ and } g \notin H$$

$$\therefore H < N(H)$$

Thus the result is true for $n=1$.

Now, suppose the true for all groups having order less than p^n.

Let $H = N(H)$

We know that $Z(G) \subseteq N(H)$

So $Z(G) \subseteq H$, $H \neq G$.

$\therefore \frac{H}{Z(G)}$ is a proper subgroup of $\frac{G}{Z(G)}$

Since $o(Z(G)) > 1$ as G is a p-group.

So $\left(\frac{G}{Z(G)}\right) = p^m$, $m < n$

We write $Z = Z(G)$,

Now, by induction hypothesis, there exists

$Zg \in \frac{G}{Z}$ and $Zg \notin \frac{H}{Z}$ s.t.

$$Zg \frac{H}{Z} (Zg)^{-1} = \frac{H}{Z}$$

$\Rightarrow Zg\,Zh\,Zg^{-1} \in \frac{H}{Z}$, $\forall\, h \in H$

$\Rightarrow Zghg^{-1} \in \frac{H}{Z}$

$\Rightarrow Zghg^{-1} = Zh_1$, for some $h_1 \in H$

$\Rightarrow ghg^{-1}h_1^{-1} \in Z = Z(G) \subseteq H$

$\Rightarrow ghg^{-1} \in H$, $\forall\, h \in H$

$\Rightarrow gHg^{-1} \subseteq H$

$\Rightarrow gHg^{-1} = H$ $\{\because o(gHg^{-1}) = o(H)\}$

$\Rightarrow g \in N(H)$

But $g \notin H$ as $Zg \notin \frac{H}{Z}$.

So $H \subset N(H)$.

Thus by induction, the result is true for all $n \geq 1$.

<u>Result</u>: Let $o(G) = p^n$, p, a prime and H be a subgroup of order p^{n-1}. Show that H is normal in G.

<u>Solution</u>: We know that $N(H)$ is the largest subgroup of G such that H is normal in $N(H)$. So

$$H \subseteq N(H) \subseteq G \Rightarrow o(H) \mid o(N(H)) \mid o(G)$$
$$\Rightarrow p^{n-1} \mid o(N(H)) \mid p^n$$
$$\Rightarrow o(N(H)) = p^{n-1} \text{ or } p^n.$$

If $o(N(H)) = p^n$. Then $N(H) = G$

$\therefore$ H is normal in G.

If $o(N(H)) = p^{n-1}$. Then $N(H) = H$.

Also $Z = Z(G) \subseteq N(H) = H$ and $o(Z) = p^m$ (say), $m > 0$.

So $\frac{H}{Z}$ is a subgroup of $\frac{G}{Z}$.

And $o\left(\frac{H}{Z}\right) = p^{n-1-m}$

$o\left(\frac{G}{Z}\right) = p^{n-m}$.

Now, we prove the result by induction on n.

If $n=1$, $H = \{e\}$ and so H is normal in G.

Assume that the result is true for all p-groups having order less than $o(G)$.

So by induction $\frac{H}{Z}$ is normal in $\frac{G}{Z}$ $\{\because o(\frac{G}{Z}) < n\}$

This implies that H is normal in G.

So $N(H) = G \Rightarrow H = G$, a contradiction.

Thus $o(N(H)) \neq p^{n-1}$.

<u>Result</u>: If G is a finite non-abelian p-group, then show that $p^2 \mid o(\text{Aut}\, G)$.

<u>Solution</u>: Let $o(G) = p^n$ and G is non-abelian.

Then $Z(G) > 1$, {by class equation}

Also $Z(G) < o(G)$. So let $o(Z(G)) = p^m$, $1 \leq m < n$.

Thus $o\left(\frac{G}{Z(G)}\right) = p^{n-m}$, $n-m \geq 1$.

If $n-m = 1$, then $o\left(\frac{G}{Z(G)}\right) = p \Rightarrow \frac{G}{Z(G)}$ is cyclic

$\Rightarrow G$ is abelian,

But G is non-abelian.

So $n-m \geq 2$.

Now $\frac{G}{Z(G)} \cong I(G) \Rightarrow o\left(\frac{G}{Z(G)}\right) = o(I(G))$

$\Rightarrow p^2 \mid o(I(G))$

$\Rightarrow p^2 \mid o(\text{Aut}\, G)$ $\{\because I(G) \leq \text{Aut}\, G\}$

<u>Proved</u>.

Theorem: Let G be an abelian group of order n. Then for every divisor m of n, G has a subgroup of order m.

Proof: Let $o(G) = n$, G be abelian group.

Let $m|n$. Then to show that G has at least one subgroup of order m.

For this, we use the method of induction on n.

If $n=1$, $G=\{e\}$. The result is obviously true.

Now we assume that the result is true for all groups having order less than $o(G)$.

Let $m>1$ and p be a prime s.t. $p|m$. So $p|n$

Then by Cauchy's theorem, there exists an element $x \in G$ s.t. $o(x) = p$.

Let $K = \langle x \rangle$. So $o(K) = o(x) = p$.

Since G is abelian, so K is normal in G.

Now $o\left(\frac{G}{K}\right) = \frac{n}{p} < n$ and $\frac{G}{K}$ is an abelian group.

Since $p|m$. So $m = pm_1$ for some $m_1 \in \mathbb{N}$.

Also $pm_1 \mid o(G) = o\left(\frac{G}{K}\right) . o(K)$

$$\Rightarrow m_1 \mid o\left(\frac{G}{K}\right) \quad ; \text{ as } o(K) = p.$$

By induction hypothesis, there exist a subgroup $\frac{H}{K}$ of $\frac{G}{K}$ s.t. $o\left(\frac{H}{K}\right) = m_1$.

$$\therefore \quad o(H) = o(K) . m_1 = pm_1 = m.$$

So the result is true for all groups having order less than $n = o(G)$.

Hence by induction, the result is true is true for all n.