Department of Mathematics

SEM - 6

Course - BMH6DSE33

Group Theory - II

Notes given by Rima Dutta.

Solution :- Let H be any subgroup of order p^{n-1} of a group G of order p^n.

Now by lemma 2, we have,

$$[G:H] \equiv [N(H):H] \pmod{p}.$$

ie. $p \equiv [N(H):H] \pmod{p}$

~~Since~~ $\cancel{[N(H):H]}$ $\therefore p \mid p - [N(H):H]$

Since $[N(H):H] > 1$, so $[N(H):H] = p$.

Now, $[G:H] = [G:N(H)] \times [N(H):H]$

ie. $p = [G:N(H)] \times p$

ie. $[G:N(H)] = 1$.

$\therefore |G| = |N(H)|$

Also, $N(H) \subseteq G$

Thus, $N(H) = G$. and hence H is normal in G.

Theorem (Sylow's first theorem) :-

Let G be a finite group of order $p^r m$ where p is prime, $r \geq 0$ and ~~g~~ m is a positive integer such that $\gcd(p,m) = 1$. Then G has a subgroup of order p^k for all k such that $0 \leq k \leq r$.

Scanned with CamScanner

Proof:- We prove the theorem by mathematical induction on K.

For $K = 0$, G has a subgroup $\{e\}$ of order $1 = p^0 = p^K$

So the result is true for $K = 0$.

For $K = 1$, $p \mid |G|$, where p is prime.

So by Cauchy's theorem, G has an element $a \in G$ s.t. $o(a) = p$. and hence G has a subgroup $H = \langle a \rangle$ of order $p = p^K$.

So the theorem is true for $K = 1$.

Let us assume that, the theorem is true for $K = i$, where $0 \leq i < r$.

So G has a subgroup H of order p^i.

Hence by Lemma 2, we have, $[G:H] \equiv [N(H):H] \pmod{p}$. — (1)

Since $i < r$, so H is a proper subgroup of G.

So, $[G:H] = \frac{|G|}{|H|} = p^{r-i}m$ and hence $p \mid [G:H]$

Thus, from (1), we have,

$$p \mid [N(H):H]$$

Since H is normal in $N(H)$, so $N(H)/H$ exists, and $p \mid |N(H)/H|$.

Hence by Cauchy's theorem, $N(H)/H$ has a subgroup K/H of order p where K is a subgroup of $N(H)$

containing H.

Now, $|K| = \frac{|K|}{|H|} \cdot |H| = [K:H] \times |H|$

$$= p \times p^i$$

$$= p^{i+1}.$$

Thus, ~~the~~ ~~sub~~ G has a subgroup of order p^{i+1}.

Thus, the result is true for $k = i+1$.

Hence by mathematical induction, the theorem is true ~~for~~ for a group of order $p^r m$ i.e. the group G of order $p^r m$ has a subgroup of order p^k, where $1 \le k \le r$.

<u>Definition</u> (<u>Sylow - p - subgroup</u>) :- Let G be a finite group of order $p^r m$ where p is prime, r, m are positive integer and $\gcd(p, m) = 1$. Then any subgroup of G of order p^r is called Sylow p-subgroup of G.

<u>Theorem</u> :- (<u>Sylow's 2nd theorem</u>) :- Let G be a finite group of order $p^r m$, where p is prime, r, m are positive integers and $\gcd(p, m) = 1$. Then any two Sylow-p-subgroups are conjugate.

Proof:- Let H and K be two Sylow p-subgroups of G.

Then $|H| = |K| = p^r$.

Let $S = \{aH : a \in G\}$.

We define an action of K on S by $k \cdot (aH) = (ka)H$

$\forall\ k \in K$, $aH \in S$.

Then S is a K-set.

Also let $S_0 = \{aH \in S : k \cdot (aH) = aH\ \forall\ k \in K\}$.

Then $|S| \equiv |S_0| \pmod p$

i.e. $m \equiv |S_0| \pmod p$

Since $\gcd(m, p) = 1$, so, $|S_0| \neq 0$.

Hence, $\exists$ at least one element $aH \in S_0$.

Then $k \cdot (aH) = aH\ \forall\ k \in K$.

i.e. $a^{-1}ka \in H\ \forall\ k \in K$.

i.e. $a^{-1}Ka \subseteq H$.

Also, $|K| = |a^{-1}Ka| = |H|$.

Thus, $a^{-1}Ka = H$.

Thus, H and K are conjugate to each other.

Hence, any two ~~s~~ Sylow p-subgroups are conjugate to each other.

Notes by Rima Dutta.

Theorem (Sylow's third theorem) :-

Let G be a finite group of order $p^r m$, where p is prime, r, m are positive integer and $\gcd(m, p) = 1$. Then the number n_p of Sylow-p-subgroups of G is $1 + kp$ for some non-negative integer k and $n_p \mid |G|$

Proof:- Let S be the set of all Sylow p-subgroups of G.

Let P be a Sylow p-subgroup of G.

$\therefore P \in S$.

and, $|P| = p^r$

Now, we define a group action $\bullet : P \times S \to S$ by

$$g \bullet H = gHg^{-1} \; \forall g \in P, \; \forall H \in S.$$

Since H is a subgroup of G, so gHg^{-1} is also subgroup of G.

Also, $|gHg^{-1}| = |H| = p^r$

$\therefore gHg^{-1} \in S$.

Also, S is a P-set.

Again let $S_0 = \{H \in S : g \bullet H = H \; \forall g \in P\}$.

$$= \{H \in S : gHg^{-1} = H \; \forall g \in P\}$$

Therefore, $|S| \equiv |S_0| \pmod{p}$. — (1)

Let $H \in S_0$.

Then $g \cdot H = H \ \forall g \in P$.

ie. $gHg^{-1} = H \ \forall g \in P$

ie. $g \in N(H) \ \forall g \in P$.

$\therefore P \subseteq N(H)$

Thus, P and H are Sylow p-subgroups of $N(H)$.

Then by Sylow's 2nd theorem, H and P are conjugate to each other.

$\therefore P = aHa^{-1}$ for some $a \in N(H)$.

But $a \in N(H)$ implies $aHa^{-1} = H$.

$\therefore H = P$.

$\therefore S_0$ contains only one element ~~the~~ P.

$\therefore |S_0| = 1$.

$\therefore$ From (1), we have, $|S| \equiv 1 \pmod{p}$

ie. $n_p \equiv 1 \pmod{p}$.

ie. $n_p = 1 + kp$ for some $k \geq 0$

Again, we define $* : G \times S \to S$ by

$$g * H = gHg^{-1} \;\forall\; g \in G \text{ and } \forall\; H \in S.$$

Then S is a G-set.

$\therefore$ By Sylow's second theorem, any two Sylow p-subgroups are conjugate to each other.

$\therefore$ There is only one orbit in S.

Let $H \in S$.

Then $[G : G_H] = |[H]|$

ie. $\dfrac{|G|}{|G_H|} = |S|$. [$\because$ No. of orbit ~~of~~ in S is 1]

ie. $\dfrac{|G|}{|G_H|} = n_p$.

$\therefore n_p \,\Big|\, |G|$.

Exercise :- Prove that no group of order 8 is simple.

Solution :- Let G be a any group of order 8.

If G is commutative, then G has a subgroup H of order 4.

Since G is commutative and hence H is normal in G.

Also if G is non-commutative, then $|G| = 2^3$.

$\therefore$ G is a 2-group.

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

Also, $Z(G) \neq G$ ($\because$ G is non-commutative).

Also, $Z(G)$ is a normal subgroup of G.

Hence, no group of order 8 is simple. (Proved)

Exercise :- Prove that, no group of order 56 is simple.

Solution :- Let G be a group of order $56 = 2^3 \times 7$.

Then G has Sylow 7-subgroups.

Let n_7 be the number of Sylow 7-subgroups of G.

Then $n_7 \mid 56$ and $n_7 = 7K + 1$, K is non-negetive integers.

$\therefore$ $n_7 = 1$ or 8.

If $n_7 = 1$ then Sylow 7-subgroup is ~~simple~~. unique and hence Sylow 7-subgroup is normal in G.

Hence in this case, G is not simple.

If $n_7 = 8$, then G has 8 Sylow 7-subgroups.

Let $A_1, A_2, \ldots, A_8$ be Sylow 7-subgroups of G.

Then $\bigcup_{n=1}^{8} A_n$ contains 48 elements of order 7.

Again, G has Sylow 2-subgroups.

Let n_2 be the number of Sylow 2-subgroups.

Then $n_2 \mid 56$ and $n_2 = 2k+1$, where k is non-negative integers.

$\therefore n_2 = 1$ or 7.

If $n_2 = 1$, then Sylow 2-subgroup is unique and hence normal in G.

Hence in this case G is not simple.

If $n_2 = 7$, then G has 7 Sylow 2-subgroups.

Let B_1, B_2 be two Sylow 2-subgroups.

Then $B_1 \cup B_2$ contains at least 11 non-identity elements of order other 7.

Hence G contains atleast $59 (= 48 + 11)$ ~~ele~~ non-identity elements, ~~of~~ which is a contradiction.

$\therefore$ if $n_7 = 8$ then $n_2 \neq 7$.

Hence G is not simple.

Exercise :- Prove that no group of order pq, is simple, where p and q are distinct primes.

Solution :- Let G be a group of order $pq = p \times q$.

Since p and q are distinct primes, so without loss of any generality, we may assume that $p > q$.

Now, G has Sylow p-subgroups.

Let n_p be the number of Sylow p-subgroups.

Then $n_p \mid |G|$ and $n_p = kp + 1$, where k is non-negative integer.

Then, $n_p = 1, p, q, pq$.

Since $n_p = kp + 1$, so $p \nmid n_p$.

$\therefore n_p \neq p, pq$.

If $n_p = q$, then $kp + 1 = q$.

$\therefore p \mid (q-1)$ — which is a contradiction ($\because p > q$)

$\therefore n_p = 1$.

Thus, Sylow p-subgroup is unique and hence normal in G.

Thus, G is not simple.

Exercise :- Prove that any group of order 15 is cyclic.

Solution :- Let G be a group of order $15 = 3 \times 5$.

Now, G has Sylow 3-subgroups. and Sylow 5-subgroups

Let n_3 be the number of ~~sylow~~ Sylow 3-subgroup. of G.

Then $n_3 = 3K+1$, and $n_3 \mid |G|$, where k is non-negetive integer.

Therefore $n_3 = 1$.

So, Sylow 3-subgroup H is unique and hence it is normal in G.

Also let n_5 be the number of Sylow 5-subgroup of G.

Then $n_5 \mid |G|$ and $n_5 = 5K+1$, where k is non-negetive integer.

$\therefore n_5 = 1$.

Hence, Sylow 5-subgroup K is unique and hence it is normal in G.

Also, $H \cap K = \{e\}$ [$\because |H| = 3$, $|K| = 5$ and 3 and 5 are prime to each other].

$$\therefore |HK| = \frac{|H||K|}{|H \cap K|} = 3 \times 5 = 15.$$

Thus, $HK = G$

Hence, G is an internal direct product of H and K.

$\therefore \; G \cong H \times K.$

Since H and K are of prime order, so H and K are cyclic groups of order 3 and 5 respectively.

Also, $\gcd(3,5) = 1$.

Also, $|H \times K| = 3 \times 5 = 15$.

$\therefore$ $H \times K$ is cyclic, and hence G is cyclic.