Sylow Second theorem :-

Let G be a finite group and p be a prime number such that $p \mid O(G)$. Then any two sylow-p-subgroups of G are Conjugate.

Proof :- Let $O(G) = p^m q$ with p and q are relatively prime. Then every sylow p-subgroup of G is of order p^m.

Let H be any Sylow p-subgroup of G and M be the set of all subgroups of G which are Conjugate to H.

Now it is sufficient to prove that every Sylow p-subgroup K of G is Conjugate to H, that we show that $K \in M$.

Let us suppose that K is not Conjugate to H i.e. $K \neq x^{-1}Hx$ for all $x \in G$.

Let S be any Sylow p-subgroup such that $S \neq K$, then $K \not\subset S$, therefore there exists an element $x \in K$ but not in S i.e. $x \in K - S$.

Also $x^{-1}Sx = x \Rightarrow x \in N(S)$, the normalizer of S.

Since $x \in K$, which is of order p^m, so $x \in S$ which is a Contradiction. Hence $x^{-1}Sx \neq x$ which means that S has more than one Conjugate in K.

Also the number of Conjugate of S in K is equal to the index of $N_K(S)$ in K and the latter divides $o(K) = p^m$. This shows that number of conjugates of S in K is a multiple of p.

Let us define a relation $\sim$ in M as under :

If $H_1, H_2 \in M$, then $H_1 \sim H_2 \Leftrightarrow$ there exists $x \in K$ such that $H_2 = x^{-1} H_1 x$, clearly this relation is an equivalence on M. therefore this relation partitions M into equivalence classes.

Since we have already proved that the number of Conjugates of S in K is a multiple of p, therefore the equivalence class of S determined by the elements in K Contains n elements where p divides n. Thus $o(M)$ is a multiple of p.

Also $o(M)$ = index of $N(H)$ in G, but the index of H in G is q because $o(H) = p^m$.

Since H is a subgroup of $N(H)$, then by lagrange's theorem we have

$$o(N(H)) = p^m r$$

and $o(H)$. index of $H = o(N(H))$.index$(N(H))$

or
$$o(H) \cdot i(H) = o(N(H)) \cdot i(N(H))$$
$$\Rightarrow o(H) \cdot i(H) = o(N(H)) \cdot o(M)$$

$\Rightarrow o(H) \cdot i(H) = p^m r \cdot o(M)$

$\Rightarrow o(G) = p^m r \cdot o(M) \quad \left[\because i(H) = \frac{o(G)}{o(H)} \right]$

$p^m q = p^m r \cdot o(M) \Rightarrow q = r \cdot o(M)$

Since $p \mid o(M)$, then q is multiple of p. this shows that p and q are not relatively prime which is a contradiction because $(p \cdot q) = 1$. Therefore K is a conjugate of H. Hence the proof of the theorem is complete.

<u>Corollary</u> :- Let $p \mid o(G)$, where G is a finite group and p any prime number. The a Sylow p-subgroup H of G is normal if H is unique Sylow p-subgr of G.

<u>Proof</u> :- Let $o(G) = p^m q$ with $(p, q) = 1$ Then $o(H) = p^m$. By above theorem a Sylow p-subgroup K of G is conju to H i.e. $K = x^{-1} H x$ for some $x \in G$

If H is normal, then $x^{-1} H x \subseteq$

$\Rightarrow K \subseteq H$

since $o(K) = o(H)$, then we obta $H = K$, this shows that H is unique