date: monday, february 5, 2024

Second Sylow Theorem

Def$^{\underline{n}}$: A Sylow p-subgroup P of G is a subgroup that is a maximal p-group in G. Ie. if $|G| = p^r m$ with $\gcd(p,m)=1$, then any subgroup of order p^r is a Sylow p-subgroup.

Note: The First Sylow Theorem implies there always exists at least one Sylow p-group.

The proof of the First Sylow Theorem used the group action:

$$G \times G \to G$$
$$(g,h) \mapsto ghg^{-1}$$

The proof of the Second and Third Sylow Theorem use a different action.

Let $S = \{\text{all subgroups of } G\}$. We define a G-action on S by

$$G \times S \to S$$
$$(g,K) \to gKg^{-1} = g \cdot K.$$

Def$^{\underline{n}}$: Say subgroups L and K are congruent if there exists $g \in G$ such that $L = gKg^{-1}$. If H is a subgroup of G, we say L and K are H-congruent if exists $h \in H$ such that $L = hKh^{-1}$.

Def$^{\underline{n}}$: $N(H) = \{g \in G \mid gHg^{-1} = H\}$ is the normalizer of H.

this plays the "role" of $C(x)$

Proposition: $N(H)$ is a subgroup of G (and $H \subseteq N(H)$)
H is normal in $N(H)$
$N(H)$ is the largest subgroup of G such that H is normal in it.

Second Sylow Theorem: Let G be a finite group and $p \| |G|$ with p prime. If P_1, P_2 are two sylow p-subgroups of G, then they are conjugates, ie. exists $g \in G$ such that $P_2 = gP_1g^{-1}$.

Lemma ①: Let P be a sylow p-subgroup and suppose $x \in G$ with $|x| = p^m$. If $xPx^{-1} = P$, then $x \in P$.

Note: $x \in N(P)$, and since P is normal in $N(P)$, $\langle xP \rangle$ is a cyclic subgroup of $N(P)/P$.

Note: $|xP| = p^{\ell}$ for some ℓ, since $(xP)^{p^m} = x^{p^m}P = eP = P$. So $|xP| \mid P^m$.

Proof

By the Correspondance Theorem, there exists a subgroup H such that $P \subseteq H \subseteq N(P)$ and $H/P = \langle xP \rangle$. So $|H| = |\langle xP \rangle||P|$. Ie. $|H|$ is a power of p. But P is the largest subgroup that is a power of $P \Rightarrow H = P$. So $xP = P \Rightarrow x \in P$.

$\square$

Lemma ②: Let H and K be subgroups of G. The number of distinct H-conjugates of K is $[H : N(K) \cap H]$.

Proof (different from the book, uses group actions)

$|\{hKh^{-1} \mid h \in H\}| = |\mathcal{O}_K|$ ← number of orbits of K under the action $H \times S \to S$, $(h, K) \mapsto hKh^{-1}$

$= [H : H_K]$ where $H_K = \{h \in H \mid h \cdot K = K \Leftrightarrow hKh^{-1} = K\}$

$= [H : N(K) \cap H]$ $\qquad = N(K) \cap H$

$\square$

Proof (second Sylow)

Suppose $|G| = p^r m$ with $\gcd(p, m) = 1$. And let P by a Sylow p-subgroup with $|P| = p^r$.

Let $S = \{gPg^{-1} \mid g \in G\}$. By the previous result, the number of distinct conjugates given by

$$|S| = [G : N(P) \cap G] = [G : N(P)].$$

We have $|G| = [G : N(P)]|N(P)|$. Since $P \subseteq N(P)$, $p^r \mid |N(P)|$. This forces $p \nmid [G : N(P)] = |S|$.

Let Q be any other Sylow p-subgroup. Want to show $Q \in S$. For each $P_i \in S$, consider the Q-conjugates of P_i, ie. $\{qP_iq^{-1} | q \in Q\}$. This is a subset of S.
Also, $|\{qPq^{-1}|q \in Q\}| = [Q:N(P_i) \cap Q] = p^r$, we have $p^\ell | [Q:N(P_i) \cap Q]$ for some ℓ. The sets

$$A_1 = \{qP_1q^{-1} | q \in Q\}$$
$$A_2 = \{qP_2q^{-1} | q \in Q\}$$
$$\vdots$$

partition the set S, ie. $S = A_1 \cup A_2 \cup \cdots \cup A_t$ for some t.
Note $|A_i| = [Q:N(P_i) \cap Q] = p^{\ell_i}$ with $\ell_i \geq 0$.
If each $|A_i| \geq p$, this forces $p \,|\, |S|$. But $p \nmid |S|$. So some

$$|A_i| = 1 \iff \{qPq^{-1} | q \in Q\} = \{P_i\}.$$

But, $|q| = p^m$ for some m and $qP_iq^{-1} = P_i$. But by Lemma 1, this says $q \in P_i$. So for all $q \in Q$, $q \in P_i$. Ie. $Q \subseteq P_i$. But $|Q| = |P_i|$, so $Q = P_i$.

$\square$

IMPORTANT COROLLARY A Sylow p-subgroup is normal if and only if there is exactly one Sylow p-subgroup.

<u>Proof</u>

"$\Rightarrow$" Suppose P and Q are sylow p-subgroups. So they are conjugates, ie. $gPg^{-1} = Q$ for all $g \in G$. But P is normal, so $P = gPg^{-1} = Q$.

"$\Leftarrow$" Suppose P is the only Sylow p-subgroup. Then for any $g \in G$. $gPg^{-1} = P$ since $|gPg^{-1}| = |P|$, ie. gPg^{-1} is also a Sylow p-subgroup. So P is normal since true for all $g \in G$.

$\square$