Math 210A Lecture 16 Notes

Daniel Raban

November 2, 2018

1 Sylow Theorems

1.1 Sylow p-subgroups

For this lecture, we will assume that a p-group is finite and of order p^k. Let G be a finite group. Take $p \mid |G|$ and say that $p^n \mid\mid |G|$ if $p^n \mid |G|$ but $p^{n+1} \nmid |G|$.

Definition 1.1. A **p-subgroup** of G is a subgroup of order p^k for some $k \leq n$.

Definition 1.2. A **Sylow p-subgroup** of G is a p-subgroup of G which is not properly contained in any other p-subgroup.

Example 1.1. The symmetric group S_5 has order $120 = 2^3 \cdot 3 \cdot 5$. For $p = 5$, a Sylow 5-subgroup will look like $\langle \begin{pmatrix} a_1 & a_2 & a_3 & a_4 & a_5 \end{pmatrix} \rangle$. There are $6 = 4!/4$ of these, For $p = 3$, a Sylow 3-subgroup will look like $\langle \begin{pmatrix} a_1 & a_2 & a_3 \end{pmatrix} \rangle$. There are 10 of these. For $p = 2$, a Sylow 2-subgroup will look like $\langle \begin{pmatrix} a_1 & a_2 & a_3 & a_4 \end{pmatrix}, \begin{pmatrix} a_1 & a_3 \end{pmatrix} \rangle$. There are 15 of these.

Observe that the number of each type of Sylow p-subgroup divides the order of the group. In general, this is unusual.

1.2 Sylow theorems

Let $n_p(G)$ be the number of p-Sylow subgroups of G, and let $\mathrm{Syl}_p(G)$ be the set of Sylow p-subgroups of G. Our goal will be to prove the following.

Theorem 1.1 (Sylow theorems)**.** *Let G be a finite group.*

1. *Every Sylow p-subgroup of G has order p^n, where $p^n \mid\mid |G|$.*
2. *Any two Sylow p-subgroups are conjugate.*
3. *$n_p(G) \mid |G|$, and $n_p(G) \equiv 1 \pmod{p}$.*

Recall that if P is a p-group, X is a finite set, and $P \circlearrowright X$, then $|X| \equiv |X^p| \pmod{p}$.

Lemma 1.1. *Let G be finite, and let H be a p-subgroup of G. Then*

$$[G : H] \equiv [N_G(H) : H] \pmod p.$$

Proof. Let $L = G/H$ be the set of right cosets of H. Then $|L| = [G : H]$. $H \circlearrowright L$ by $h \cdot (aH) = (ha)H$. If $aH \in L^H$, then for all $h \in H$, $haH = aH$, which means that $a^{-1}haH = H$, which is the same thing as $a^{-1}ha \in H$ for all $h \in H$. □

Theorem 1.2. *If $H \leq G$, and $|H| = p^k$ for $k < n$, then there is some $P \leq G$ with $H \trianglelefteq P$ and $|P| = p^{k+1}$.*

Proof. If $|H| \neq p^n$, then $p \mid [G : H]$, so $p \mid [N_G(H) : H] = |N_G(H)/H|$. So $N_G(H)/H$ has a subgroup P/H of order p. Then $P \leq N_G(H)$, and $|P| = p^{k+1} = |P/H||H|$. So $H \trianglelefteq P$. □

This proves the first Sylow theorem. Let's prove the second theorem.

Proof. Take $P, Q \in \mathrm{Sly}_p(G)$. We know that $|P| = |Q| = p^n$. Let $Q \circlearrowright G/P$. Since $p \nmid |G/P|$, $p \nmid |(G/P)^Q|$. So $(G/P)^Q \neq \varnothing$, and we get some xP such that $qxP = xP$ for all $q \in Q$. This means that $(x^{-1}qx)P = P$, so $x^{-1}qx \in P$ for all $q \in Q$. So $x^{-1}Qx \subseteq P$. Since P and $x^{-1}Qx$ have the same order, $x^{-1}Qx = P$. □

Now let's prove the third Sylow theorem.

Proof. Let $G \circlearrowright \mathrm{Syl}_p(G)$ by conjugation. By the second Sylow theorem, this action is transitive. Let P be a Sylow p-subgroup of G. By orbit-stabilizer,

$$n_p(G) = |\mathrm{Syl}_p(G)| = [G : \mathrm{Stab}(P)] = [G : N_G(P)].$$

We have that

$$[G : P] = [G : N_G(P)][N_P(G) : P]$$

and

$$[G : P] \equiv [N_G(P) : P] \not\equiv 0 \pmod p,$$

so

$$[G : N_G(P)] \equiv 1 \pmod p.$$ □

Example 1.2. Let $|G| = 42$. We will show that G has a nontrivial normal subgroup. $n_7(G) \mid 42$ and $7 \nmid n_7(G)$, so $n_7(G) \mid 6$. So $n_7(G) = 1$. So if $|H| = 7$, then $H \trianglelefteq G$.

Example 1.3. Let $|G| = 30$. We show that G has a nontrivial normal subgroup. Then G has 9 nontrivial normal subgroups. $n_5(G) \mid 30$, so $n_5(G) \mid 6$. Then $n_5(G) = 1$ or 6. Similarly, $n_3(G) \mid 10$, so $n_3(G) = 1$ or 10. Assume that $n_5(G), n_3(G) > 1$. Then we have 6 5-subgroups. Each one has 4 elements of order 5. So there are 24 elements of order 5. If $n_3(G) = 10$, there are 20 different elements of order 3. This is impossible because $24 + 20 > 30$.