MATH 3311, FALL 2025: LECTURE 21, OCTOBER 17

Video: `https://youtu.be/Y6DqUJuViuA`

Again, we will fix a finite group G and a prime p. Let $m \geq 0$ be the integer such that p^m is the largest power of p dividing the order $|G|$.

We have seen the following theorems already:

Theorem 1 (Sylow Theorem A)**.** *There exists a subgroup $Q \leq G$ of order $|Q| = p^m$. That is, $\mathrm{Syl}_p(G)$ is non-empty.*

Theorem 2 (Sylow Theorem B)**.** *The conjugation action of G on $\mathrm{Syl}_p(G)$ is* transitive. *That is, if $P, Q \in \mathrm{Syl}_p(G)$ are two Sylow p-subgroups of G, then there exists $g \in G$ such that $gPg^{-1} = Q$.*

Proof. Let's review the proof. We want to show that, for $P, Q \in \mathrm{Syl}_p(G)$, there exists $g \in G$ such that $Q = gPg^{-1}$.

This in turn is equivalent to knowing

$$Q \leq gPg^{-1}.$$

Indeed, Q and gPg^{-1} both have order p^m by hypothesis.

We now observe that $gPg^{-1} = G_{gP}$ where $G_{gP} \leq G$ is the stabilizer of the coset $gP \in G/P$ for the left multiplication action[1] Therefore, we have to show:

There exists $g \in G$ such that $Q \leq G_{gP}$, which is equivalent to knowing that the action of Q on G/P via left multiplication has a *fixed point*.

That is, we need to know that $(G/P)^Q$ is non-empty, or equivalently that

$$|(G/P)^Q| \neq 0.$$

For this, we will prove something that is a bit stronger. Indeed, since Q is a p-group, we can apply our fundamental congruence for group actions by p-groups on finite sets to deduce that we have

$$|(G/P)^Q| \equiv |G/P| \pmod{p}.$$

Now, we finally use our hypothesis that P is a *Sylow* p-subgroup. This implies that $|G/P| = [G : P]$ is *not* divisible by p. Therefore, we have

$$|(G/P)^Q| \not\equiv 0 \pmod{p}.$$

In particular, $(G/P)^Q$ is *non-empty*, and hence there is $gP \in G/P$ that is fixed by Q. As we established above, this means that $Q = gPg^{-1}$. □

We also saw the following corollaries:

Corollary 1. *If $P, Q \in \mathrm{Syl}_p(G)$ are two Sylow p-subgroups that P is* isomorphic *to Q.*

Corollary 2. *If $P \in \mathrm{Syl}_p(G)$, then the following are equivalence:*

(1) $P \trianglelefteq G$ is normal *in G;*
(2) P is the unique *Sylow p-subgroup.*

Corollary 3. *If G is* abelian, *then G has a unique Sylow p-subgroup.*

Today, we will state and prove the last of the Sylow theorems.

Theorem 3 (Sylow Theorem C)**.** *Let $n_p = |\mathrm{Syl}_p(G)|$ be the number of Sylow p-subgroups of G.*

(1) $n_p = [G : N_G(P)]$ and $n_p \mid [G : P]$ for any $P \in \mathrm{Syl}_p(G)$.
(2) $n_p \equiv 1 \pmod{p}$.

---

[1]Quick proof: $hgP = h(gP) = gP \Leftrightarrow g^{-1}hg \in P \Leftrightarrow h \in gPg^{-1}$.

Proof. The first part is essentially an immediate consequence of orbit-stabilizer, applied to $G \curvearrowright \mathrm{Syl}_p(G)$. The stabilizer of $P \in \mathrm{Syl}_p(G)$ for this (conjugation) action is exactly the normalizer $N_G(P) \leq G$. Moreover, Theorem B tells us that we have exactly one orbit, whose size is n_p. Thus, orbit-stabilizer gives us

$$[G : N_G(P)] = |G|/|N_G(P)| = n_p.$$

Moreover, we have

$$[G : P] = [G : N_G(P)][N_G(P) : P] = n_p[N_G(P) : P].$$

This shows that n_p is a factor of $[G : P]$.

For part (2), we will use the fundamental congruence for the action of p-groups. We will apply it to the action $P \curvearrowright \mathrm{Syl}_p(G)$ to get the congruence

$$|\mathrm{Syl}_p(G)^P| \equiv |\mathrm{Syl}_p(G)| \equiv n_p \pmod{p}. \tag{0.0.0.1}$$

Now, $Q \in \mathrm{Syl}_p(G)^P$ means that P fixes Q under the conjugation action. In other words, for all $x \in P$, we have $xQx^{-1} = Q$. Equivalently, we are saying that every such x is in $N_G(Q)$. Thus we find:

$$\begin{aligned} Q \in \mathrm{Syl}_p(G)^P &\Leftrightarrow P \leq N_G(Q) \\ &\Leftrightarrow P, Q \leq N_G(Q) \qquad \Leftrightarrow P, Q \in \mathrm{Syl}_p(N_G(Q)). \end{aligned}$$

The second line holds because we always have $Q \leq N_G(Q)$, and the last line is because p^m is the largest power of p dividing $|G|$, and is therefore also the largest power of p dividing $|N_G(Q)|$.

Now, we come to the *key* observation: $Q \trianglelefteq N_G(Q)$ is *normal* in $N_G(Q)$ (by the definition of the normalizer). But now Corollary 2 tells us that Q is the *unique* Sylow p-subgroup of $N_G(Q)$. Therefore, we find:

$$P, Q \in \mathrm{Syl}_p(N_G(Q)) \Leftrightarrow Q = P.$$

Putting everything together, we find that

$$\mathrm{Syl}_p(G)^P = \{P\}$$

has exactly one element. So (0.0.0.1) now gives us

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

which gives us assertion (2). □

Example 1. Suppose that $|G| = 48 = 2^4 \cdot 3$. Then $n_2 \equiv 1 \pmod{2}$ is odd and $n_2 \mid 3$. So the only possibilities are $n_2 = 1, 3$. If $n_2 = 1$, then there is exactly one Sylow 2-subgroup (of order 16), which is normal. If $n_2 = 3$, then we have three such subgroups. But we can still obtain some more information about G by now looking at the action $G \curvearrowright \mathrm{Syl}_2(G)$, which gives a *non-trivial* group homomorphism $\rho : G \to S_3$.