Lecture 5.6: The Sylow theorems

Matthew Macauley

Department of Mathematical Sciences
Clemson University
http://www.math.clemson.edu/~macaule/

Math 4120, Modern Algebra
Overview

The Sylow theorems are about one question:

What finite groups are there?

Early on, we saw five families of groups: cyclic, dihedral, abelian, symmetric, alternating.

Later, we classified all (finitely generated) abelian groups.

But what other groups are there, and what do they look like? For example, for a fixed order $|G|$, we may ask the following questions about $G$:

1. How big are its subgroups?
2. How are those subgroups related?
3. How many subgroups are there?
4. Are any of them normal?

There is no one general method to answer this for any given order.

However, the Sylow Theorems, developed by Norwegian mathematician Peter Sylow (1832–1918), are powerful tools that help us attack this question.
Recall from last time

**Definition**

A \textit{p-group} is a group whose order is a power of a prime \( p \). A \( p \)-group that is a subgroup of a group \( G \) is a \textit{\( p \)-subgroup} of \( G \).

**Notational convention**

Throughout, \( G \) will be a group of order \( |G| = p^n \cdot m \), with \( p \nmid m \). That is, \( p^n \) is the highest power of \( p \) dividing \( |G| \).

There are three \textbf{Sylow theorems}, and loosely speaking, they describe the following about a group’s \( p \)-subgroups:

1. **Existence**: In every group, \( p \)-subgroups of all possible sizes exist.
2. **Relationship**: All maximal \( p \)-subgroups are conjugate.
3. **Number**: There are strong restrictions on the number of \( p \)-subgroups a group can have.

Together, these place strong restrictions on the structure of a group \( G \) with a fixed order.
Our unknown group of order 200

Throughout our two lectures on the Sylow theorems, we will have a running example, a “mystery group” $M$ of order 200.

Using *only* the fact that $|M| = 200$, we will uncover as much about the structure of $M$ as we can.

We actually already know a little bit. Recall Cauchy’s theorem:

**Cauchy’s theorem**

If $p$ is a prime number dividing $|G|$, then $G$ has an element $g$ of order $p$. 
Our mystery group of order 200

Since our mystery group $M$ has order $|M| = 2^3 \cdot 5^2 = 200$, Cauchy’s theorem tells us that:

- $M$ has an element $a$ of order 2;
- $M$ has an element $b$ of order 5;

Also, by Lagrange’s theorem, $\langle a \rangle \cap \langle b \rangle = \{e\}$. 
The 1st Sylow Theorem: Existence of $p$-subgroups

First Sylow Theorem

$G$ has a subgroup of order $p^k$, for each $p^k$ dividing $|G|$. Also, every $p$-subgroup with fewer than $p^n$ elements sits inside one of the larger $p$-subgroups.

The First Sylow Theorem is in a sense, a generalization of Cauchy’s theorem. Here is a comparison:

<table>
<thead>
<tr>
<th>Cauchy’s Theorem</th>
<th>First Sylow Theorem</th>
</tr>
</thead>
<tbody>
<tr>
<td>If $p$ divides $</td>
<td>G</td>
</tr>
<tr>
<td>There is a subgroup of order $p$</td>
<td>There is a subgroup of order $p^k$</td>
</tr>
<tr>
<td>which is cyclic and has no non-trivial proper subgroups.</td>
<td>which has subgroups of order 1, $p$, $p^2$ . . . $p^k$.</td>
</tr>
<tr>
<td>$G$ contains an element of order $p$</td>
<td>$G$ might not contain an element of order $p^k$.</td>
</tr>
</tbody>
</table>
The 1st Sylow Theorem: Existence of $p$-subgroups

Proof

The trivial subgroup $\{e\}$ has order $p^0 = 1$.

**Big idea:** Suppose we’re given a subgroup $H < G$ of order $p^i < p^n$. We will construct a subgroup $H'$ of order $p^{i+1}$.

By the normalizer lemma, $H \leq N_G(H)$, and the order of the quotient group $N_G(H)/H$ is a multiple of $p$.

By Cauchy’s Theorem, $N_G(H)/H$ contains an element (a coset!) of order $p$. Call this element $aH$. Note that $\langle aH \rangle$ is cyclic of order $p$.

**Claim:** The preimage of $\langle aH \rangle$ under the quotient $q: N_G(H) \to N_G(H)/H$ is the subgroup $H'$ we seek.

The preimages $q^{-1}(H), q^{-1}(aH), q^{-1}(a^2H), \ldots, q^{-1}(a^{p-1}H)$ are all distinct cosets of $H$ in $N_G(H)$, each of size $p^i$.

Thus, the preimage $H' = q^{-1}(\langle aH \rangle)$ contains $p \cdot |H| = p^{i+1}$ elements. □
The 1\textsuperscript{st} Sylow Theorem: Existence of $p$-subgroups

Here is a picture of how we found the group $H' = q^{-1}(<aH>)$.

Since $|H| = p^i$, the subgroup $H' = \bigcup_{k=0}^{p-1} a^k H$ contains $p \cdot |H| = p^{i+1}$ elements.
Our unknown group of order 200

We now know a little bit more about the structure of our mystery group of order $|M| = 2^3 \cdot 5^2$:

- $M$ has a 2-subgroup $P_2$ of order $2^3 = 8$;
- $M$ has a 5-subgroup $P_5$ of order $25 = 5^2$;
- Each of these subgroups contains a nested chain of $p$-subgroups, down to the trivial group, $\{e\}$.

\[|M| = 200\]
The 2nd Sylow Theorem: Relationship among $p$-subgroups

**Definition**

A subgroup $H < G$ of order $p^n$, where $|G| = p^n \cdot m$ with $p \nmid m$ is called a **Sylow $p$-subgroup** of $G$. Let $\text{Syl}_p(G)$ denote the set of Sylow $p$-subgroups of $G$.

**Second Sylow Theorem**

Any two Sylow $p$-subgroups are conjugate (and hence isomorphic).

**Proof**

Let $H < G$ be any Sylow $p$-subgroup of $G$, and let $S = G/H = \{Hg \mid g \in G\}$, the set of right cosets of $H$.

Pick *any other* Sylow $p$-subgroup $K$ of $G$. (If there is none, the result is trivial.)

The group $K$ acts on $S$ by **right-multiplication**, via $\phi: K \to \text{Perm}(S)$, where

$$\phi(k) = \text{the permutation sending each } Hg \text{ to } Hgk.$$
The 2\textsuperscript{nd} Sylow Theorem: All Sylow $p$-subgroups are conjugate

Proof

A fixed point of $\phi$ is a coset $Hg \in S$ such that

\[ Hgk = Hg, \forall k \in K \iff Hgk^{-1} = H, \forall k \in K \]
\[ \iff gkg^{-1} \in H, \forall k \in K \]
\[ \iff gKg^{-1} \subseteq H \]
\[ \iff gKg^{-1} = H. \]

Thus, if $\phi$ has a fixed point $Hg$, then $H$ and $K$ are conjugate by $g$, and we’re done!

All we need to do is show that $|\text{Fix}(\phi)| \neq p\, 0$.

By the $p$-group Lemma, $|\text{Fix}(\phi)| \equiv_p |S|$. Recall that $|S| = [G, H]$.

Since $H$ is a Sylow $p$-subgroup, $|H| = p^n$. By Lagrange’s Theorem,

\[ |S| = [G : H] = \frac{|G|}{|H|} = \frac{p^n m}{p^n} = m, \quad p \nmid m. \]

Therefore, $|\text{Fix}(\phi)| \equiv_p m \neq p\, 0.$
Our unknown group of order 200

We now know even more about the structure of our mystery group $M$, of order $|M| = 2^3 \cdot 5^2$:

- If $M$ has any other Sylow 2-subgroup, it is isomorphic to $P_2$;
- If $M$ has any other Sylow 5-subgroup, it is isomorphic to $P_5$. 

If any other Sylow 2-subgroup exists, it is isomorphic to the first.
The 3rd Sylow Theorem: Number of $p$-subgroups

### Third Sylow Theorem

Let $n_p$ be the number of Sylow $p$-subgroups of $G$. Then

$$n_p \text{ divides } |G| \quad \text{and} \quad n_p \equiv_p 1.$$  

(Note that together, these imply that $n_p \mid m$, where $|G| = p^n \cdot m$.)

---

### Proof

The group $G$ acts on $S = \text{Syl}_p(G)$ by conjugation, via $\phi: G \to \text{Perm}(S)$, where

$$\phi(g) = \text{the permutation sending each } H \text{ to } g^{-1}Hg.$$  

By the Second Sylow Theorem, all Sylow $p$-subgroups are conjugate! Thus there is only one orbit, $\text{Orb}(H)$, of size $n_p = |S|$.

By the Orbit-Stabilizer Theorem,

$$|\text{Orb}(H)| \cdot |\text{Stab}(H)| = |G| \quad \implies \quad n_p \text{ divides } |G|.$$
The 3\textsuperscript{rd} Sylow Theorem: Number of $p$-subgroups

Proof (cont.)

Now, pick any $H \in \text{Syl}_p(G) = S$. The group $H$ acts on $S$ by conjugation, via $\theta: H \to \text{Perm}(S)$, where

$$\theta(h) = \text{the permutation sending each } K \text{ to } h^{-1}Kh.$$ 

Let $K \in \text{Fix}(\theta)$. Then $K \leq G$ is a Sylow $p$-subgroup satisfying

$$h^{-1}Kh = K, \quad \forall h \in H \iff H \leq N_G(K) \leq G.$$ 

We know that:

- $H$ and $K$ are Sylow $p$-subgroups of $G$, but also of $N_G(K)$.
- Thus, $H$ and $K$ are conjugate in $N_G(K)$. (2nd Sylow Thm.)
- $K \trianglelefteq N_G(K)$, thus the only conjugate of $K$ in $N_G(K)$ is itself.

Thus, $K = H$. That is, $\text{Fix}(\theta) = \{H\}$ contains only 1 element.

By the $p$-group Lemma, $n_p := |S| \equiv_p |\text{Fix}(\theta)| = 1$. \qed
Summary of the proofs of the Sylow Theorems

For the 1st Sylow Theorem, we started with $H = \{e\}$, and inductively created larger subgroups of size $p, p^2, \ldots, p^n$.

For the 2nd and 3rd Sylow Theorems, we used a clever group action and then applied one or both of the following:

(i) **Orbit-Stabilizer Theorem.** If $G$ acts on $S$, then $|\text{Orb}(s)| \cdot |\text{Stab}(s)| = |G|$.
(ii) **p-group Lemma.** If a $p$-group acts on $S$, then $|S| \equiv_p |\text{Fix}(\phi)|$.

To summarize, we used:

S2 The action of $K \in \text{Syl}_p(G)$ on $S = G/H$ by right multiplication for some other $H \in \text{Syl}_p(G)$.
S3a The action of $G$ on $S = \text{Syl}_p(G)$, by conjugation.
S3b The action of $H \in \text{Syl}_p(G)$ on $S = \text{Syl}_p(G)$, by conjugation.
Our unknown group of order 200

We now know a little bit more about the structure of our mystery group $M$, of order $|M| = 2^3 \cdot 5^2 = 200$:

- $n_5 \mid 8$, thus $n_5 \in \{1, 2, 4, 8\}$. But $n_5 \equiv 1 \pmod{5}$, so $n_5 = 1$.
- $n_2 \mid 25$ and is odd. Thus $n_2 \in \{1, 5, 25\}$.
- We conclude that $M$ has a unique (and hence normal) Sylow 5-subgroup $P_5$ (of order $5^2 = 25$), and either 1, 5, or 25 Sylow 2-subgroups (of order $2^3 = 8$).
Our unknown group of order 200

\[ |M| = 200 \]

The only Sylow 5-subgroup is normal

There may be other Sylow 2-subgroups

Suppose \( M \) has a subgroup isomorphic to \( D_4 \).

This would be a Sylow 2-subgroup. Since all of them are conjugate, \( M \) cannot contain a subgroup isomorphic to \( Q_4, C_4 \times C_2 \), or \( C_8 \)!

In particular, \( M \) cannot even contain an element of order 8. (Why?)