MAT205: Abstract Algebra II

3. Cauchy's Theorem and the Sylow Theorems

Ma, Jia-Jun – Xiamen University Malaysia

Recap: Tools from Lectures 1–2

We have built the following toolkit:

- **Orbit-Stabilizer**: $|G \cdot x| = [G : G_x]$
- **Class Equation**: $|G| = |Z(G)| + \sum_i [G : C_G(x_i)]$
- **p-groups**: If $|G| = p^n$, then $Z(G) \neq \{e\}$

Today: use group actions to prove the **three Sylow theorems** – the most powerful structure results for finite groups.

Counting Principle for p-Group Actions

Proposition. If a p-group P acts on a finite set X, then

$$|X| \equiv |X^P| \pmod{p}$$

where $X^P = \{x \in X \mid g \cdot x = x \text{ for all } g \in P\}$ is the set of **fixed points**.

Proof. Decompose X into orbits: $X = X^P \sqcup O_1 \sqcup \cdots \sqcup O_k$ where each O_i has $|O_i| > 1$.

By orbit-stabilizer, $|O_i| = [P : P_{x_i}]$ divides $|P| = p^n$, so $|O_i|$ is a power of p.

Since $|O_i| > 1$, we have $p \mid |O_i|$. Hence $|X| = |X^P| + \sum |O_i| \equiv |X^P| \pmod{p}$. $\square$

This is the key technique behind all Sylow proofs: let a p-group act, then count fixed points mod p.

Augustin-Louis Cauchy (1789–1857)

Cauchy was one of the founders of **rigorous analysis** and a pioneer of **group theory**. He introduced the concept of permutation groups and proved that every finite group whose order is divisible by a prime p contains an element of order p.

His 1845 *Mémoire sur les arrangements* laid the groundwork for the study of permutation groups, directly influencing Sylow's later work.

Cauchy was extraordinarily prolific – he published over **800 papers**, second only to Euler in volume. His contributions span complex analysis (Cauchy integral formula), elasticity theory, and number theory.

A.-L. Cauchy (1789–1857)

Cauchy's Theorem

Theorem (Cauchy, 1845). If G is a finite group and p is a prime dividing $|G|$, then G has an element of order p.

Proof. Let $\mathbb{Z}/p\mathbb{Z}$ act on $X = \{(g_1, \ldots, g_p) \in G^p \mid g_1 g_2 \cdots g_p = e\}$ by cyclic shift.

- **Well-defined:** $g_1 \cdots g_p = e \implies g_2 \cdots g_p \cdot g_1 = g_1^{-1}(g_1 \cdots g_p)g_1 = e$. ✓
- **Size:** $|X| = |G|^{p-1}$ (choose $g_1, \ldots, g_{p-1}$ freely; g_p is determined).
- **Orbits** have size 1 or p (since $|\mathbb{Z}/p\mathbb{Z}| = p$ is prime).

Key step – identify the fixed points:

$$\boxed{X^{\mathbb{Z}/p\mathbb{Z}} = \{(g, g, \ldots, g) \mid g^p = e\}}$$

By the counting principle: $|X^{\mathbb{Z}/p\mathbb{Z}}| \equiv |X| = |G|^{p-1} \equiv 0 \pmod{p}$.

Since $(e, \ldots, e)$ is one fixed point, we have $|X^{\mathbb{Z}/p\mathbb{Z}}| \geq p$. Hence $\exists\, g \neq e$ with $g^p = e$. $\square$

The Normalizer

Definition. For $H \leq G$, the **normalizer** of H in G is:

$$N_G(H) = \{g \in G \mid gHg^{-1} = H\}$$

Key properties:

- $H \leq N_G(H) \leq G$
- $H \trianglelefteq N_G(H)$ (and $N_G(H)$ is the **largest** subgroup in which H is normal)
- $H \trianglelefteq G \iff N_G(H) = G$

Example: Computing the Normalizer

Example. In S_4, let $H = \langle (12)(34) \rangle = \{e,\ (12)(34)\}$.

Question: Which $\sigma \in S_4$ satisfy $\sigma H \sigma^{-1} = H$, i.e., $\sigma(12)(34)\sigma^{-1} \in H$?

$$N_{S_4}(H) = \{e,\ (12)(34),\ (12),\ (34),\ (13)(24),\ (14)(23),\ (1324),\ (1423)\}$$

This is a group of order 8, isomorphic to D_4.

Observations:

- $H \trianglelefteq D_4$ (since $H \leq N_{S_4}(H) = D_4$)
- $H \not\trianglelefteq S_4$ (since $N_{S_4}(H) = D_4 \neq S_4$)
- $[S_4 : N_{S_4}(H)] = 24/8 = 3$ – so H has **3 conjugates** in S_4

The conjugates: $\{e, (12)(34)\}$, $\{e, (13)(24)\}$, $\{e, (14)(23)\}$ – the three "double transposition" subgroups.

Try it in Sage: CoCalc Notebook

p-Groups

Definition. A group G is a **p-group** if every element has order a power of p.

For finite groups, there is a cleaner characterization:

Proposition. A finite group G is a p-group $\iff$ $|G| = p^k$ for some $k \geq 0$.

Proof. ($\Leftarrow$) Lagrange: $\mathrm{ord}(g) \mid |G| = p^k$, so every element has p-power order. ✓

($\Rightarrow$) If a prime $q \neq p$ divides $|G|$, then by **Cauchy's theorem**, G has an element of order q – contradicting that every element has p-power order. So $|G| = p^k$. ✓

Key fact (Lecture 2): If $|G| = p^k > 1$, then $Z(G) \neq \{e\}$.

Example: Abelian p-Groups

Example 1. $\mathbb{Z}/p^k\mathbb{Z}$ is a p-group of order p^k. Every element $\bar{a}$ has order dividing p^k.

More generally, $\mathbb{Z}/p^{a_1}\mathbb{Z} \times \cdots \times \mathbb{Z}/p^{a_r}\mathbb{Z}$ is an **abelian** p-group of order $p^{a_1+\cdots+a_r}$.

By the **classification of finite abelian groups**, every finite abelian p-group is of this form.

Example: The abelian 2-groups of order 8:

Group	Type
$\mathbb{Z}/8\mathbb{Z}$	cyclic
$\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$	–
$(\mathbb{Z}/2\mathbb{Z})^3$	elementary abelian

These are the **only** abelian groups of order 8 (up to isomorphism).

Example: Non-Abelian p-Groups

Example 2. The **upper-unitriangular group** $U_n(\mathbb{F}_p)$ consists of matrices in $GL_n(\mathbb{F}_p)$ with 1's on the diagonal and 0's below:

$$U_n(\mathbb{F}_p) = \left\{ \begin{pmatrix} 1 & * & \cdots & * \\ & 1 & \cdots & * \\ & & \ddots & \vdots \\ & & & 1 \end{pmatrix} \right\} \leq GL_n(\mathbb{F}_p)$$

Order: $p^{n(n-1)/2}$ – there are $n(n-1)/2$ free entries above the diagonal, each from $\mathbb{F}_p$.

So $U_n(\mathbb{F}_p)$ is a finite **p-group**.

Non-abelian for $n \geq 3$: e.g., in $U_3(\mathbb{F}_p)$, the matrices $I + E_{12}$ and $I + E_{23}$ do not commute.

For $n = 3, p = 2$: $|U_3(\mathbb{F}_2)| = 2^3 = 8$, isomorphic to D_4.

Fact: $U_n(\mathbb{F}_p)$ is a Sylow p-subgroup of $GL_n(\mathbb{F}_p)$.

Borel Subgroup in $GL_n(\mathbb{F}_p)$

Definition. Let

$$B_n(\mathbb{F}_p) = \left\{ \begin{pmatrix} * & * & \cdots & * \\ & * & \cdots & * \\ & & \ddots & \vdots \\ & & & * \end{pmatrix} \in GL_n(\mathbb{F}_p) \right\}$$

be the group of invertible upper triangular matrices.

This is the **Borel subgroup** of $GL_n(\mathbb{F}_p)$.

Theorem. The Borel subgroup is the normalizer of $U_n(\mathbb{F}_p)$ in $GL_n(\mathbb{F}_p)$. [N_{GL_n(\mathbb{F}_p)} (U_n(\mathbb{F}_p)) = B_n(\mathbb{F}_p).]

Why Is The Normalizer Equal to the Borel?

Proof idea.

First, $U_n(\mathbb{F}_p) \trianglelefteq B_n(\mathbb{F}_p)$, so

$$B_n(\mathbb{F}_p) \subseteq N_{GL_n(\mathbb{F}_p)}(U_n(\mathbb{F}_p)).$$

Key point: $U_n(\mathbb{F}_p)$ fixes the standard complete flag

$$0 < \langle e_1 \rangle < \langle e_1, e_2 \rangle < \cdots < \langle e_1, \ldots, e_n \rangle = \mathbb{F}_p^n,$$

and this is the unique complete flag fixed by $U_n(\mathbb{F}_p)$.

So if $gU_n(\mathbb{F}_p)g^{-1} = U_n(\mathbb{F}_p)$, then g must preserve that flag. But the matrices preserving the standard complete flag are exactly the upper triangular matrices.

Therefore

$$N_{GL_n(\mathbb{F}_p)}(U_n(\mathbb{F}_p)) \subseteq B_n(\mathbb{F}_p).$$

Armand Borel (1923–2003)


A. Borel (1923–2003)

Armand Borel was a Swiss mathematician whose work helped shape the modern theory of **Lie groups**, **algebraic groups**, and their geometry.

He was born on **May 21, 1923** in La Chaux-de-Fonds, Switzerland, studied at ETH Zürich, and received his doctorate from the **University of Paris** in **1952**.

After positions in Paris and Geneva, he joined the **Institute for Advanced Study** in Princeton in **1957**, where he spent most of his career.

His name appears throughout algebra and geometry:

- **Borel subgroup**
- **Borel fixed point theorem**
- **Borel–de Siebenthal theory**
- foundational books on **linear algebraic groups**

In this course, the **Borel subgroup** of $GL_n(\mathbb{F}_p)$ is the subgroup of invertible upper triangular matrices. The theorem is that this subgroup is exactly the normalizer of the standard unitriangular Sylow p-subgroup.

Orders of U_n, B_n, and GL_n

We already know

$$|U_n(\mathbb{F}_p)| = p^{n(n-1)/2}.$$

For $B_n(\mathbb{F}_p)$:

- each diagonal entry can be any element of $\mathbb{F}_p^\times$: $(p-1)^n$ choices
- each entry above the diagonal can be any element of $\mathbb{F}_p$: $p^{n(n-1)/2}$ choices

So

$$\boxed{|B_n(\mathbb{F}_p)| = (p-1)^n p^{n(n-1)/2}.}$$

Most importantly,

$$\boxed{|GL_n(\mathbb{F}_p)| = (p^n-1)(p^n-p)\cdots(p^n-p^{n-1}).}$$

The Normalizer Lemma

Lemma. Let H be a p-group with $H \leq G$. If $p \mid [G : H]$, then $H \subsetneq N_G(H)$ and $p \mid [N_G(H) : H]$.

Proof. Let H act on G/H by left multiplication. Fixed points:

gH is fixed by $H \iff g^{-1}Hg \subseteq H \iff g \in N_G(H)$. So $|(G/H)^H| = [N_G(H) : H]$.

By the counting principle (H is a p-group acting on G/H):

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

Since $p \mid [G : H]$, we get $p \mid [N_G(H) : H] \geq p > 1$, so $H \subsetneq N_G(H)$. $\square$

Remark. A p-subgroup H with $p \mid [G : H]$ always **grows** inside its normalizer. It stops growing only when $p \nmid [G : H]$, i.e., when $|H| = p^a$ is the full p-part of $|G|$.

Peter Ludwig Mejdell Sylow (1832–1918)

L. Sylow (1832–1918)

Sylow was a Norwegian mathematician and high school teacher who proved his famous theorems in a **single 10-page paper** in 1872: *Théorèmes sur les groupes de substitutions*.

He spent most of his career teaching at Fredrikshald (now Halden) — he was not appointed professor at Christiania (Oslo) until **1898**, at age 66, after decades of recognition abroad.

Together with Sophus Lie, Sylow edited the complete works of Abel (1881).

His obituary in *Nature* (G. B. Mathews, 1919) wrote:

> *"[His theorem] has perhaps done more than any other single proposition to advance our knowledge of groups in general."*

Sylow p-Subgroups

Definition. A **Sylow p-subgroup** of G is a maximal p-subgroup, i.e., a p-subgroup not properly contained in any larger p-subgroup.

- For finite G with $|G| = p^a m$, $\gcd(p, m) = 1$: P is Sylow $\iff$ $|P| = p^a$.
- $\mathrm{Syl}_p(G)$: the set of all Sylow p-subgroups; $n_p = |\mathrm{Syl}_p(G)|$.

The three Sylow theorems:

	Statement
I	$\mathrm{Syl}_p(G) \neq \emptyset$ (existence)
II	Any two Sylow p-subgroups are conjugate: $P, Q \in \mathrm{Syl}_p(G) \Rightarrow Q = gPg^{-1}$
III	$n_p \mid m$ and $n_p \equiv 1 \pmod{p}$

Strategy: All three proofs use group actions – the key technique from Lecture 2.

Sylow I: Existence

Theorem. If $p^i \mid |G|$ $(1 \leq i \leq a)$, then G has a subgroup of order p^i.

Proof by induction on i.

Base $(i = 1)$: By Cauchy's theorem, G has an element g of order p, so $\langle g \rangle$ has order p. ✓

Inductive step: Suppose $H \leq G$ with $|H| = p^{i-1}$ exists. Since $p^i \mid |G|$, we have $p \mid [G : H]$.

By the **normalizer lemma**: $p \mid [N_G(H) : H]$.

Since $H \trianglelefteq N_G(H)$, consider $N_G(H)/H$. We have $p \mid |N_G(H)/H|$.

By **Cauchy** applied to $N_G(H)/H$: $\exists\, \bar{a} \in N_G(H)/H$ of order p.

Let $K = \pi^{-1}(\langle \bar{a} \rangle)$. Then $|K| = |\langle \bar{a} \rangle| \cdot |H| = p \cdot p^{i-1} = p^i$. $\square$

Sylow II: Conjugacy

Theorem. All Sylow p-subgroups of G are conjugate.

Proof. Let $P \in \mathrm{Syl}_p(G)$ and Q any p-subgroup of G.

Let Q act on the coset space G/P by left multiplication.

- $|G/P| = [G : P] = m$, and $p \nmid m$ (since P is Sylow).
- Orbits of Q have size dividing $|Q|$ (a power of p).
- Counting principle: $|G/P| \equiv |\text{fixed points}| \pmod{p}$.
- Since $p \nmid m$, there is at least one **fixed point** gP.

A fixed point means: $\forall\, q \in Q,\ qgP = gP$, i.e., $g^{-1}Qg \subseteq P$.

If Q is also Sylow ($|Q| = p^a = |P|$), then $g^{-1}Qg = P$, so $Q = gPg^{-1}$. $\square$

Corollary: Normal $\iff$ Unique

Corollary. Let $P \in \mathrm{Syl}_p(G)$. Then:

$$P \trianglelefteq G \quad \iff \quad n_p = 1$$

Proof. ($\Rightarrow$) If $P \trianglelefteq G$, then $gPg^{-1} = P$ for all g. By Sylow II, every Sylow p-subgroup is a conjugate of P, hence equals P. So $n_p = 1$.

($\Leftarrow$) If $n_p = 1$, then $gPg^{-1} \in \mathrm{Syl}_p(G) = \{P\}$ for all g, so $P \trianglelefteq G$. $\square$

Why this matters: To show a group G is **not simple**, it suffices to find a prime p with $n_p = 1$.

The Sylow III constraints ($n_p \mid m$, $n_p \equiv 1 \bmod p$) often force $n_p = 1$.

Example. $|G| = 15 = 3 \cdot 5$. Then $n_5 \mid 3$ and $n_5 \equiv 1 \pmod 5$, so $n_5 = 1$. The Sylow 5-subgroup is **normal**.

Sylow III: $n_p \mid m$

Theorem. $n_p \mid m$ and $n_p \equiv 1 \pmod{p}$ (where $|G| = p^a m$, $\gcd(p, m) = 1$).

Proof of $n_p \mid m$.

G acts on $\mathrm{Syl}_p(G)$ by conjugation. By Sylow II, this is **transitive**, so:

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

Since $P \leq N_G(P)$, we have $[G : N_G(P)] \mid [G : P] = m$. $\square$

Sylow III: $n_p \equiv 1 \pmod{p}$

Proof. Fix $P \in \mathrm{Syl}_p(G)$ and let P act on $\mathrm{Syl}_p(G)$ by **conjugation**.

Claim: The only fixed point is P itself.

Proof of claim. Suppose Q is a fixed point: $gQg^{-1} = Q$ for all $g \in P$, so $P \leq N_G(Q)$.

Then P and Q are both Sylow p-subgroups of $N_G(Q)$.

Since $Q \trianglelefteq N_G(Q)$, by the corollary (Normal $\iff$ Unique), Q is the **unique** Sylow p-subgroup of $N_G(Q)$. Hence $P = Q$. ✓

By the counting principle, all non-fixed orbits have size divisible by p:

$$n_p = \underbrace{1}_{\text{fixed point } P} + \underbrace{(\text{multiples of } p)}_{\text{other orbits}} \equiv 1 \pmod{p} \qquad \square$$

Example: Sylow Subgroups of S_4

$|S_4| = 24 = 2^3 \cdot 3$.

Sylow 3-subgroups ($p^a = 3$):

- $n_3 \mid 8$ and $n_3 \equiv 1 \pmod 3$, so $n_3 \in \{1, 4\}$.
- S_4 has 8 elements of order 3 (the 3-cycles), each generating a subgroup of order 3.
- Two per subgroup $\implies n_3 = 8/2 = 4$. ✓

Sylow 2-subgroups ($p^a = 8$):

- $n_2 \mid 3$ and $n_2 \equiv 1 \pmod 2$, so $n_2 \in \{1, 3\}$.

Try it in Sage: CoCalc Notebook

Sylow 2-Subgroups of S_4: A Geometric View

S_4 acts on the 3 **pair-partitions** of $\{1,2,3,4\}$:

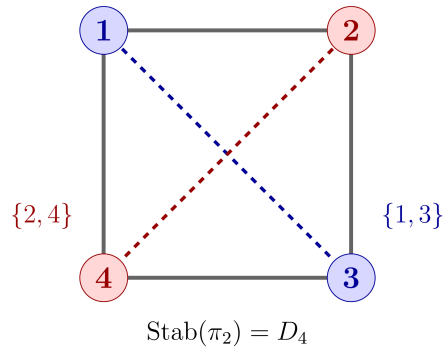
$$\pi_1 = \{\{1,2\},\{3,4\}\}, \quad \pi_2 = \{\{1,3\},\{2,4\}\}, \quad \pi_3 = \{\{1,4\},\{2,3\}\}$$

The **stabilizer** of $\pi_2 = \{\{1,3\},\{2,4\}\}$ is the set of permutations preserving these pairs = **symmetries of the square** 1-2-3-4:

$$\mathrm{Stab}(\pi_2) = D_4 = \{e, (1234), (13)(24), (1432), (13), (24), (12)(34), (14)(23)\}$$

$|D_4| = 8 = 2^3$ – a Sylow 2-subgroup!

The 3 pair-partitions π_1, π_2, π_3 give 3 conjugate copies of D_4, so $n_2 = 3$. ✓



Example: Groups of Order 15

$|G| = 15 = 3 \cdot 5$.

- $n_3 \mid 5$ and $n_3 \equiv 1 \pmod 3$, so $n_3 = 1$.
- $n_5 \mid 3$ and $n_5 \equiv 1 \pmod 5$, so $n_5 = 1$.

So G has a **unique** (hence normal) Sylow 3-subgroup $P \cong \mathbb{Z}/3\mathbb{Z}$ and a unique normal Sylow 5-subgroup $Q \cong \mathbb{Z}/5\mathbb{Z}$.

- $P \cap Q = \{e\}$ (orders coprime) and $|PQ| = |P| \cdot |Q| / |P \cap Q| = 15 = |G|$.
- Both normal $\implies G = P \times Q \cong \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z} \cong \mathbb{Z}/15\mathbb{Z}$.

Conclusion: Every group of order 15 is cyclic!

More generally, if $|G| = pq$ with $p < q$ and $p \nmid q - 1$, then $G \cong \mathbb{Z}/pq\mathbb{Z}$.

Summary: The Sylow Theorems

$|G| = p^a m$, $\gcd(p, m) = 1$.

	Statement	Proof technique
I	$\exists$ subgroup of order p^i, $1 \leq i \leq a$	Cauchy + normalizer lemma
II	All Sylow p-subgroups are conjugate	Q acts on G/P
III	$n_p \mid m$, $n_p \equiv 1 \pmod{p}$	G and P act on $\mathrm{Syl}_p(G)$

Corollary: $P \trianglelefteq G \iff n_p = 1$. To show G is not simple, find p with $n_p = 1$.

Summary: The Proof Strategy

Logical chain: $\text{Counting principle} \to \text{Cauchy} \to \text{Normalizer lemma} \to \text{I} \to \text{II} \to \text{III}$

Common thread: Choose a p-group to act → counting principle ($|X| \equiv |X^P| \bmod p$) → analyze fixed points.

Proof	p-group	Acts on	Fixed points
Cauchy	$\mathbb{Z}/p\mathbb{Z}$	p-tuples, product $= e$	$(g, \ldots, g)$, $g^p = e$
Norm. lemma	H	G/H	cosets in $N_G(H)/H$
Sylow I	use Cauchy on $N_G(H)/H$	quotient by a smaller p-subgroup	element of order p in $N_G(H)/H$
Sylow II	Q	G/P	$\exists$ fixed gP
Sylow III	P	$\text{Syl}_p(G)$	only P itself

Homework (Lecture 3)

Problem 1. The rotation group of the tetrahedron

Let G be the rotation group of a regular tetrahedron.

a. Show that each rotation permutes the four faces, so there is a homomorphism

$$\varphi : G \to S_4.$$

b. Prove that φ is injective.

Hint: if a rotation fixes all four faces, then it fixes the whole tetrahedron.

c. Show that $|G| = 12$.

Hint: count rotations by axis type: identity, 120° and 240° rotations, and 180° rotations.

d. Conclude that $G \cong A_4$.

Hint: an injective homomorphism from a group of order 12 into S_4 must land in the subgroup of even permutations.

Looking Ahead

Lecture 4: Applications of Sylow Theorems

- Use Sylow theory to study the structure of concrete finite groups
- Detect normal subgroups and rule out simplicity in specific examples
- See how semidirect products arise naturally from Sylow subgroups

The Sylow theorems are the **main computational tool** for understanding finite groups.

"To analyze a finite group, first find its Sylow subgroups."

Questions?