MAT205: Abstract Algebra II

4. Applications of the Sylow Theorems

Ma, Jia-Jun – Xiamen University Malaysia

From Existence to Structure

In Lecture 3, Sylow theory told us:

- when p-subgroups **exist**
- how many Sylow p-subgroups there can be
- when a Sylow subgroup must be **normal**

Today we use Sylow theory in the most important way:

$$\boxed{\text{to determine the structure of a finite group}}$$

Our main example:

$$|G| = 21 = 3 \cdot 7$$

Appetizer: Groups of Order pq are Not Simple

Theorem. Let $p < q$ be primes. Any group G with $|G| = pq$ has a normal Sylow q-subgroup. In particular, G is **not simple**.

Proof. By Sylow III: $n_q \mid p$ and $n_q \equiv 1 \pmod{q}$.

Since p is prime, $n_q \in \{1, p\}$.

If $n_q = p$, then $p \equiv 1 \pmod{q}$, i.e., $q \mid (p-1)$, so $p \geq q + 1 > q$ – contradicting $p < q$.

Hence $n_q = 1$, and the unique Sylow q-subgroup is normal. $\square$

Examples:

- $|G| = 15 = 3 \cdot 5$: $n_5 = 1$, in fact $G \cong \mathbb{Z}_{15}$ (unique up to iso).
- $|G| = 21 = 3 \cdot 7$: $n_7 = 1$, but there are **two** groups (see below!).
- $|G| = 35 = 5 \cdot 7$: $n_7 = 1$, $G \cong \mathbb{Z}_{35}$.

Going deeper: what is the full classification? This is what we'll do for $|G| = 21$.

Sylow Analysis of $|G| = 21$

Let G be a group of order $21 = 3 \cdot 7$. Apply Sylow III to both primes:

Sylow 7-subgroup P: $n_7 \mid 3$ and $n_7 \equiv 1 \pmod 7$.

Only $n_7 = 1$ works, so $P \trianglelefteq G$ and $P \cong \mathbb{Z}_7$.

Sylow 3-subgroup Q: $n_3 \mid 7$ and $n_3 \equiv 1 \pmod 3$.

Both $n_3 = 1$ and $n_3 = 7$ satisfy these, so $n_3 \in \{1, 7\}$. Either way, $Q \cong \mathbb{Z}_3$.

Two cases to analyze:

Case	n_3	Is Q normal?
1	1	yes $\Rightarrow$ G is a direct product
2	7	no $\Rightarrow$ need a new construction

Interlude: The Product Set PQ

Definition. For subgroups $P, Q \leq G$:

$$PQ = \{pq \mid p \in P,\ q \in Q\} \subseteq G$$

Warning: PQ is a **subset**, not always a subgroup!

Lemma. PQ is a subgroup $\iff$ $PQ = QP$.

Sufficient condition: If $P \subseteq N_G(Q)$ or $Q \subseteq N_G(P)$, then $PQ = QP$ (hence $PQ \leq G$).

Proof of sufficient condition. If $P \subseteq N_G(Q)$, then $pQp^{-1} = Q$, so $pQ = Qp$ for every $p \in P$. Hence $PQ = \bigcup_p pQ = \bigcup_p Qp = QP$. $\square$

The Size Formula for PQ

Theorem. For any subgroups $P, Q \leq G$ (even if PQ is not a subgroup):

$$|PQ| = \frac{|P| \cdot |Q|}{|P \cap Q|}$$

Proof via group action. Let $P \times Q$ act on G by $(p, q) \cdot g = p\, g\, q^{-1}$.

Orbit of e: $(P \times Q) \cdot e = \{pq^{-1} \mid p \in P, q \in Q\} = PQ$ (using $Q^{-1} = Q$).

Stabilizer of e: $(p, q) \in \mathrm{Stab}(e) \iff peq^{-1} = e \iff p = q \in P \cap Q$. So

$$\mathrm{Stab}(e) = \{(x, x) \mid x \in P \cap Q\} \cong P \cap Q$$

Orbit-stabilizer:

$$|PQ| = |(P \times Q) \cdot e| = \frac{|P \times Q|}{|\mathrm{Stab}(e)|} = \frac{|P| \cdot |Q|}{|P \cap Q|} \qquad \square$$

When is $PQ \cong P \times Q$?

Proposition. Let $P, Q \leq G$. If:

- $P \subseteq N_G(Q)$ and $Q \subseteq N_G(P)$ (each normalizes the other),
- $P \cap Q = \{e\}$,

then PQ is a subgroup and $PQ \cong P \times Q$.

Proof. Both normalizers $\Rightarrow PQ$ is a subgroup (by previous lemma).

For any $p \in P, q \in Q$: the commutator $[p, q] = pqp^{-1}q^{-1}$ lies in $P \cap Q$:

- $pqp^{-1} \in Q$ since $P \subseteq N_G(Q)$, so $[p, q] = (pqp^{-1})q^{-1} \in Q$
- $qp^{-1}q^{-1} \in P$ since $Q \subseteq N_G(P)$, so $[p, q] = p(qp^{-1}q^{-1}) \in P$

Hence $[p, q] \in P \cap Q = \{e\}$, i.e., $pq = qp$ – elements of P and Q commute.

The map $P \times Q \to PQ$, $(p, q) \mapsto pq$, is a homomorphism, surjective, with trivial kernel. $\square$

Case 1: $n_3 = 1$ – Both Sylow Subgroups Normal

Both $P, Q \trianglelefteq G$, $P \cap Q = \{e\}$ (coprime orders). Applying the proposition:

- $P \trianglelefteq G \Rightarrow Q \subseteq G = N_G(P)$ ✓
- $Q \trianglelefteq G \Rightarrow P \subseteq G = N_G(Q)$ ✓

So $PQ \cong P \times Q$, and $|PQ| = 21 = |G|$, hence $G = PQ$:

$$G \cong \mathbb{Z}_7 \times \mathbb{Z}_3 \cong \mathbb{Z}_{21}$$

Case 2 ($n_3 = 7$): Q is not normal – G is **not** a direct product. But $P \trianglelefteq G$ still means Q acts on P by conjugation:

$$G = \text{“}\mathbb{Z}_7 \text{ with a } \mathbb{Z}_3\text{-action”} \quad \longrightarrow \quad \text{semidirect product}$$

To handle this case we first develop the theory of semidirect products.

A Motivating Example: S_3

Consider the smallest non-abelian group S_3 (order 6).

Inside S_3:

- $N = A_3 = \langle (123) \rangle \cong \mathbb{Z}_3$, with $N \trianglelefteq S_3$
- $H = \langle (12) \rangle \cong \mathbb{Z}_2$, a subgroup (not normal!)

Observation: $N \cap H = \{e\}$ and $|N| \cdot |H| = 6 = |S_3|$, so $S_3 = NH$ (every element $\sigma = \nu h$ uniquely).

This looks just like a direct product! But $S_3 \ncong \mathbb{Z}_3 \times \mathbb{Z}_2 = \mathbb{Z}_6$ – S_3 is non-abelian.

Something subtle is happening.

Why S_3 Is Not $\mathbb{Z}_6$

Both S_3 and $\mathbb{Z}_6$ contain a subgroup $\mathbb{Z}_3$ and a subgroup $\mathbb{Z}_2$, both with trivial intersection. The **multiplication rule differs**:

In $\mathbb{Z}_6 = \mathbb{Z}_3 \times \mathbb{Z}_2$: elements of $\mathbb{Z}_3$ and $\mathbb{Z}_2$ **commute**.

In S_3: let $r = (123) \in N$, $s = (12) \in H$. Compute:

$$srs^{-1} = (12)(123)(12) = (132) = r^{-1}$$

So s **conjugates** r to r^{-1} – H acts **nontrivially** on N by automorphisms.

Key insight: S_3 is not just N and H sitting side by side – H **acts on** N by conjugation, twisting the multiplication.

This twisting is exactly what a **semidirect product** captures – we make this precise next.

Group Extensions: Building Bigger Groups

A **short exact sequence** of groups:

$$1 \to K \xrightarrow{\iota} G \xrightarrow{\pi} H \to 1$$

means ι injective, π surjective, and $\mathrm{im}(\iota) = \ker(\pi)$ – equivalently:

$$K \trianglelefteq G \quad \text{and} \quad G/K \cong H$$

We say G is an **extension** of H by K.

Structural interpretation:

- K is a **normal subgroup** of G (the "kernel piece")
- $H \cong G/K$ is the **quotient** (the "external piece")
- $|G| = |K| \cdot |H|$

Extension problem: given K and H, classify all G fitting into such a sequence – inverse of forming quotients, **has many solutions** in general.

Not Every Extension Splits

Simplest example: $1 \to \mathbb{Z}_2 \to \mathbb{Z}_4 \to \mathbb{Z}_2 \to 1$

- $\mathbb{Z}_2 \cong \{0, 2\} \trianglelefteq \mathbb{Z}_4$ (the unique order-2 subgroup)
- $\mathbb{Z}_4/\{0, 2\} \cong \mathbb{Z}_2$
- So $\mathbb{Z}_4$ is an extension of $\mathbb{Z}_2$ by $\mathbb{Z}_2$.

Does it split? We'd need a subgroup $H \leq \mathbb{Z}_4$ with $|H| = 2$ and $H \cap \{0, 2\} = \{0\}$. But $\{0, 2\}$ is the **only** order-2 subgroup of $\mathbb{Z}_4$! So no complement exists.

Consequence: $\mathbb{Z}_4 \ncong \mathbb{Z}_2 \rtimes \mathbb{Z}_2$. In fact the only order-4 semidirect products are $\mathbb{Z}_2 \times \mathbb{Z}_2$ (trivial action, since $\mathrm{Aut}(\mathbb{Z}_2) = 1$).

The cyclic group $\mathbb{Z}_4$ is **genuinely a non-trivial extension** – it doesn't factor as a semidirect product.

Moral: extensions are more general than semidirect products. The classification of non-split extensions leads to **group cohomology** $H^2(H; K)$ – a topic for later.

Semidirect Product: Definition

Data: groups K, H and a homomorphism $\varphi : H \to \mathrm{Aut}(K)$ – an **action of H on K by automorphisms**.

Definition. $K \rtimes_\varphi H$ is the set $K \times H$ with multiplication

$$(k_1, h_1)(k_2, h_2) = \big(k_1 \cdot \varphi(h_1)(k_2),\ h_1 h_2\big)$$

The second factor multiplies as usual; $\varphi(h_1)$ **twists** the first factor.

Special case. If φ is trivial: $K \rtimes_\varphi H = K \times H$ (direct product).

As an extension: $K \rtimes_\varphi H$ fits into the split exact sequence

$$1 \to K \to K \rtimes_\varphi H \to H \to 1$$

with splitting $h \mapsto (e_K, h)$.

Internal vs External

External: start with $\varphi : H \to \mathrm{Aut}(K)$, build $K \rtimes_\varphi H$ on $K \times H$.

Internal: inside a group G, if $N \trianglelefteq G$, $H \leq G$, $N \cap H = \{e\}$, $NH = G$, then

$$G \cong N \rtimes_\varphi H, \qquad \varphi(h)(n) = hnh^{-1}$$

These are the same thing:

- Internal $\Rightarrow$ External: conjugation gives the action φ.
- External $\Rightarrow$ Internal: the copies $K \times \{e\}$ and $\{e\} \times H$ satisfy the internal conditions.

Three equivalent viewpoints:

$$\underbrace{\text{split exact sequence}}_{\text{extension}} \iff \underbrace{N \trianglelefteq G,\ N \cap H = 1,\ NH = G}_{\text{subgroup}} \iff \underbrace{\varphi : H \to \mathrm{Aut}(N)}_{\text{action}}$$

Discrete Example: The Dihedral Group

The dihedral group D_n (symmetry group of regular n-gon) has presentation

$$D_n = \langle r, s \mid r^n = e,\ s^2 = e,\ srs^{-1} = r^{-1} \rangle$$

- $\langle r \rangle \cong \mathbb{Z}_n$ is the rotation subgroup (normal)
- $\langle s \rangle \cong \mathbb{Z}_2$ is generated by a reflection

Conjugation by s acts on $\langle r \rangle$ by $r \mapsto r^{-1}$, so:

$$\boxed{D_n \cong \mathbb{Z}_n \rtimes \mathbb{Z}_2}$$

where $\mathbb{Z}_2$ acts on $\mathbb{Z}_n$ by **inversion**.

Continuous Example: Rigid Motions of $\mathbb{R}^3$

$SO(3)$ acts on $(\mathbb{R}^3, +)$ by rotations ($A \cdot v = Av$), giving a homomorphism $SO(3) \to \mathbf{Aut}(\mathbb{R}^3, +)$.

The semidirect product

$$\boxed{\mathbb{R}^3 \rtimes SO(3)}$$

is the group of **orientation-preserving rigid motions** of Euclidean 3-space (rotations + translations).

An element (v, A) means: first rotate by A, then translate by v. Multiplication:

$$(v, A)(w, B) = (v + Aw,\ AB)$$

Physics: this is the special Euclidean group $SE(3)$ – describes rigid body motion, used in robotics, mechanics, and computer graphics.

Automorphisms of Cyclic Groups

Theorem. $\mathrm{Aut}(\mathbb{Z}_n) \cong (\mathbb{Z}/n\mathbb{Z})^\times$, the group of units mod n.

Proof. Every $\sigma \in \mathrm{Aut}(\mathbb{Z}_n)$ is determined by $\sigma(1) \in \mathbb{Z}_n$. For σ to be an automorphism, $\sigma(1)$ must generate $\mathbb{Z}_n$, i.e., $\gcd(\sigma(1), n) = 1$.

The map $\sigma \mapsto \sigma(1)$ gives an isomorphism $\mathrm{Aut}(\mathbb{Z}_n) \cong (\mathbb{Z}/n\mathbb{Z})^\times$. $\square$

Corollary. $|\mathrm{Aut}(\mathbb{Z}_n)| = \#\{k \in \{1, \ldots, n\} \mid \gcd(k, n) = 1\}$ (Euler's totient).

Special case. For prime p: $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ is a field, and

$$\mathrm{Aut}(\mathbb{Z}_p) \cong \mathbb{F}_p^\times \cong \mathbb{Z}_{p-1}$$

Theorem *(to be proved in Part II)*. Any finite subgroup of the multiplicative group of a field is **cyclic**.

Back to $|G| = 21$: Compute $\mathrm{Aut}(\mathbb{Z}_7)$

Apply the theorem with $p = 7$: $\mathrm{Aut}(\mathbb{Z}_7) \cong (\mathbb{Z}/7\mathbb{Z})^\times$, cyclic of order 6.

The isomorphism $(\mathbb{Z}/7\mathbb{Z})^\times \cong \mathbb{Z}_6$ **depends on a choice of generator**.

Orders in $(\mathbb{Z}/7\mathbb{Z})^\times$:

k	1	2	3	4	5	6
$\mathrm{ord}(k)$	1	3	**6**	3	**6**	2

$2^3 = 8 \equiv 1 \pmod 7$, so $\mathrm{ord}(2) = 3$ – **2 is not a generator**.

Verify 3 is a generator:

$$3^1 \equiv 3,\ \ 3^2 \equiv 2,\ \ 3^3 \equiv 6,\ \ 3^4 \equiv 4,\ \ 3^5 \equiv 5,\ \ 3^6 \equiv 1 \pmod 7$$

Hence $(\mathbb{Z}/7\mathbb{Z})^\times = \langle 3 \rangle$, and we seek $\varphi : \mathbb{Z}_3 \to \mathrm{Aut}(\mathbb{Z}_7) \cong \mathbb{Z}_6$.

Classification: Two Groups of Order 21

Homomorphisms $\varphi : \mathbb{Z}_3 \to \mathbb{Z}_6$ are determined by where the generator goes, and $\mathbb{Z}_6$ has exactly $\gcd(3,6) = 3$ solutions, giving **two isomorphism classes** of φ: trivial or nontrivial.

Case 1 (trivial φ): $G \cong \mathbb{Z}_7 \times \mathbb{Z}_3 \cong \mathbb{Z}_{21}$ – the cyclic group.

Case 2 (nontrivial φ): $\mathbb{Z}_3$ acts via an order-3 automorphism of $\mathbb{Z}_7$. Since $\mathrm{ord}(2) = 3$ in $(\mathbb{Z}/7\mathbb{Z})^\times$, we can take $\varphi(1) : a \mapsto a^2$. This gives the non-abelian group with presentation:

$$G = \langle a, b \mid a^7 = e,\ b^3 = e,\ bab^{-1} = a^2 \rangle \ \cong\ \mathbb{Z}_7 \rtimes \mathbb{Z}_3$$

$$\boxed{\text{Up to isomorphism, there are exactly two groups of order 21.}}$$

The Sylow workflow:

1. Sylow III forces a normal subgroup P
2. P gives a decomposition $G \cong P \rtimes_\varphi H$
3. Automorphisms $H \to \mathrm{Aut}(P)$ classify the possibilities

Example: $|G| = 36$ is Not Simple

Theorem. No group of order 36 is simple.

$|G| = 36 = 2^2 \cdot 3^2$. By Sylow III: $n_3 \mid 4$ and $n_3 \equiv 1 \pmod 3$, so $n_3 \in \{1, 4\}$.

Case 1 ($n_3 = 1$): the unique Sylow 3-subgroup is normal – done. ✓

Case 2 ($n_3 = 4$): Let G act on $\mathrm{Syl}_3(G) = \{P_1, P_2, P_3, P_4\}$ by conjugation, giving $\varphi : G \to S_4$.

- By Sylow II the action is **transitive**, so φ is nontrivial.
- But $|G| = 36 > 24 = |S_4|$ forces φ **not injective**.

So $\ker(\varphi)$ is a proper nontrivial normal subgroup of G. $\square$

Concrete model for Case 2: $G = A_4 \times \mathbb{Z}_3$ has order 36 with $n_3 = 4$.

Here $A_4 \hookrightarrow S_4$ gives φ, and $\ker(\varphi) = \{e\} \times \mathbb{Z}_3 \cong \mathbb{Z}_3$.

Technique (pigeonhole): if $|G| > n_p!$, then the conjugation action on $\mathrm{Syl}_p(G)$ gives a nontrivial kernel, so G is not simple.

Example: $|G| = 48$ is Not Simple (Fraleigh 37.13)

Theorem. G has a normal subgroup of order 8 or 16.

$|G| = 48 = 2^4 \cdot 3$. Sylow III: $n_2 \in \{1, 3\}$. **Case 1** ($n_2 = 1$): Sylow 2-subgroup is normal. ✓

Case 2 ($n_2 = 3$): let H, K be two distinct Sylow 2-subgroups ($|H| = |K| = 16$). If $|H \cap K| \leq 4$, the size formula gives

$$|HK| = \frac{|H||K|}{|H \cap K|} \geq \frac{256}{4} = 64 > 48$$

– contradiction. So $|H \cap K| = 8$.

$[H : H \cap K] = 2 \Rightarrow H \cap K \trianglelefteq H$; similarly $\trianglelefteq K$. So $N_G(H \cap K) \supseteq H \cup K$, hence

$$|N_G(H \cap K)| \geq |HK| = \tfrac{16 \cdot 16}{8} = 32.$$

$|N_G(H \cap K)|$ divides 48 and is ≥ 32 – the only such value is **48**. Hence $H \cap K \trianglelefteq G$, with $|H \cap K| = 8$. $\square$

Faster (pigeonhole): act on $\mathrm{Syl}_2(G)$ gives $\varphi : G \to S_3$; $|G| > |S_3|$ forces $|\ker \varphi| \geq 8$. – Weaker but quicker.

How Small Can a Non-Abelian Simple Group Be?

We have seen that many small orders force a normal subgroup (by Sylow + counting). It is natural to ask:

> What is the smallest non-abelian simple group?

Theorem. A_5 is simple, with $|A_5| = 60$.

No non-abelian simple group has order < 60 – this can be shown by Sylow case-by-case (see Fraleigh).

$A_5 \cong$ rotation group of the icosahedron/dodecahedron – will reappear in Part II for the **insolvability of the quintic**.

Why A_5 is Simple: Proof Sketch

Strategy: Any $N \trianglelefteq A_5$ is a union of conjugacy classes, contains e, and $|N| \mid 60$.

Conjugacy classes of A_5: e (1), 3-cycles (20), double transpositions (15), 5-cycles (12 + 12).

$$1 + 20 + 15 + 12 + 12 = 60 \checkmark$$

(In S_5 the 5-cycles form **one** class of size 24; in A_5 it **splits** into two of size 12.)

Check divisibility: $|N| = 1 + (\text{subset of } \{20, 15, 12, 12\})$.

Possible sums: $1,\ 13,\ 16,\ 21,\ 25,\ 28,\ 33,\ 36,\ 40,\ 45,\ 48,\ 60$.

Divisors of 60 in this list: only $\boxed{1 \text{ and } 60}$.

Hence $N = \{e\}$ or $N = A_5$. $\square$

General Case: A_n is Simple for $n \geq 5$

Theorem. A_n is simple for all $n \geq 5$.

Proof sketch – three key facts:

(1) A_n is generated by 3-cycles. Every even permutation is a product of an even number of transpositions, and $(ab)(cd) = (acb)(acd)$, $(ab)(ac) = (acb)$.

(2) All 3-cycles are conjugate in A_n (for $n \geq 5$). In S_n they're always conjugate via some π. If $\pi \notin A_n$, multiply by a transposition of two elements **not** moved by σ – this requires $n \geq 5$.

(3) Any nontrivial $N \trianglelefteq A_n$ contains a 3-cycle. Take $\sigma \in N \setminus \{e\}$ with fewest moved points. The commutator $\tau\sigma\tau^{-1}\sigma^{-1} \in N$ (for a well-chosen 3-cycle τ) has strictly fewer moved points – unless σ is already a 3-cycle.

Combining (2) + (3): N contains one 3-cycle $\Rightarrow$ all 3-cycles $\Rightarrow N = A_n$. $\square$

Remark. Fails for $n \leq 4$: $A_3 \cong \mathbb{Z}_3$ is abelian simple; A_4 has a normal Klein 4-subgroup – see next page for the geometric picture.

Geometric View: Klein 4-Group in A_4

$A_4 \cong$ rotation group of the regular tetrahedron ($12 =$ identity $+$ 8 vertex rotations $+$ 3 edge rotations).

The 6 edges form **3 pairs of opposite edges**; each pair determines an axis through the edge midpoints. The 180° rotations about these 3 axes give:

Edge axis	180° rotation
$\overline{12} \leftrightarrow \overline{34}$	$(12)(34)$
$\overline{13} \leftrightarrow \overline{24}$	$(13)(24)$
$\overline{14} \leftrightarrow \overline{23}$	$(14)(23)$

These 3 rotations $+$ identity $= V_4 \trianglelefteq A_4$.

Cube picture. Inscribe the tetrahedron in a cube. The 3 edge-midpoint axes become the cube's 3 **coordinate axes** through opposite face centers.

Why normal? Conjugation permutes the 3 edge-axes (but preserves the set), so V_4 is invariant.

Summary

For groups of order 21:

- Sylow forces the subgroup of order 7 to be normal
- this gives a decomposition

$$G \cong \mathbb{Z}_7 \rtimes \mathbb{Z}_3$$

- the action is either trivial or nontrivial
- therefore there are exactly two groups of order 21

And among all finite groups, the smallest non-abelian simple group is

$$A_5 \quad \text{of order} \quad 60.$$

Homework (Lecture 4)

Fraleigh-inspired practice on applications of Sylow theory and semidirect products.

Exercise 1. Classify all groups of order 21 up to isomorphism.

Exercise 2. Show that no group of order 20 is simple.

Exercise 3. Show that no group of order 30 is simple.

Exercise 4. Show that

$$S_3 \cong \mathbb{Z}_3 \rtimes \mathbb{Z}_2,$$

and identify explicitly the homomorphism

$$\mathbb{Z}_2 \to \mathrm{Aut}(\mathbb{Z}_3).$$