MAT205: Abstract Algebra II

Ma, Jia-Jun — Xiamen University Malaysia

Textbook: Fraleigh, *A First Course in Abstract Algebra*

Prerequisites: MAT211 (Abstract Algebra I)

Assessment

Component	Weight	Details
Assignments	30%	2 assignments, 15% each
Quizzes	10%	2 quizzes, 5% each
Midterm Exam	20%	Covers Part I (Group Theory)
Final Exam	40%	Cumulative

Course Outline

Part I: Advanced Group Theory

1. Review of basics
2. Subnormal series & solvable groups
3. Sylow theorems
4. Applications of Sylow theorems
5. Free groups & free abelian groups

Part II: Galois Theory

6. Field extensions
7. Algebraic extensions
8. Finite fields
9. Field automorphisms
10. Separable extensions
11. Galois theory I & II
12. Factorization in integral domains

Midterm: after Part I | **Final**: cumulative (Part I + II)

Recall: What is a Group?

A **binary operation** on S is a map $\cdot : S \times S \to S$.

A **group** $(G, \cdot)$ satisfies:

1. **Associativity**: $(ab)c = a(bc)$
2. **Identity**: $\exists\, e$ s.t. $ea = ae = a$
3. **Inverse**: $\forall\, a$, $\exists\, a^{-1}$ s.t. $aa^{-1} = a^{-1}a = e$

Convention: Write ab for $a \cdot b$.

Structure	Axioms
Magma	closure
Semigroup	+ associativity
Monoid	+ identity
Group	+ inverses

Examples of Groups

Group	Operation	Identity	Abelian?
$(\mathbb{Z}, +)$	addition	0	Yes
$(\mathbb{Q}^*, \times)$	multiplication	1	Yes
$(S_n, \circ)$	permutation composition	id	No ($n \geq 3$)
$(\mathbb{Z}/n\mathbb{Z}, +)$	addition mod n	$\bar{0}$	Yes
$(GL_n(\mathbb{R}), \times)$	matrix multiplication	I_n	No ($n \geq 2$)
$SL_n(\mathbb{Z})$	matrix multiplication	I_n	No ($n \geq 2$)

Abelian group: G is **abelian** if $ab = ba$ for all $a, b \in G$.

$SL_n(\mathbb{Z}) = \{A \in M_n(\mathbb{Z}) \mid \det(A) = 1\}$ – the **special linear group** over $\mathbb{Z}$.

Niels Henrik Abel and the Abel Prize


N. H. Abel (1802–1829)

Niels Henrik Abel (1802–1829) proved that the general quintic equation has **no solution by radicals** — one of the founding results of group theory.

He died at age 26 from tuberculosis, before receiving a professorship offer from Berlin.

The **Abel Prize** (est. 2003, ~$700K) is the "Nobel Prize of Mathematics," awarded annually by the Norwegian Academy. Recent laureates:

Year	Laureate	Contribution
2026	**Gerd Faltings**	Arithmetic geometry, Mordell conjecture
2025	**Masaki Kashiwara**	Algebraic analysis, representation theory
2024	**Michel Talagrand**	Probability, stochastic processes

Faltings' proof of the Mordell conjecture uses deep tools from **algebraic geometry** and **Galois representations** — themes we will encounter in Part II.

$SL_n(\mathbb{Z})$ is a Group

Why is $SL_n(\mathbb{Z})$ a group? Under matrix multiplication:

- **Closure**: $\det(AB) = \det(A)\det(B) = 1 \cdot 1 = 1$ ✓
- **Associativity**: matrix multiplication is associative ✓
- **Identity**: $\det(I_n) = 1$ ✓
- **Inverse**: $\det(A) = 1 \implies A^{-1}$ has integer entries (Cramer's rule: $A^{-1} = \mathrm{adj}(A)/\det(A)$) ✓

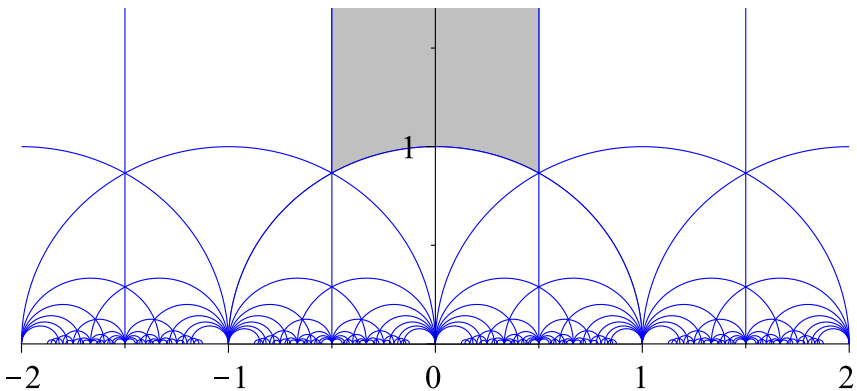
In fact, $SL_n(\mathbb{Z}) = \ker(\det : GL_n(\mathbb{Z}) \to \{\pm 1\})$, where $GL_n(\mathbb{Z}) = \{A \in M_n(\mathbb{Z}) \mid \det(A) = \pm 1\}$.

Exercise. Use the one-step subgroup criterion to prove $SL_n(\mathbb{Z}) \leq GL_n(\mathbb{R})$.

$SL_2(\mathbb{Z})$ and Modular Forms

$SL_2(\mathbb{Z})$ acts on the **upper half-plane** $\mathbb{H}$ by Mobius transformations:

$$\mathbb{H} = \{z \in \mathbb{C} \mid \mathrm{Im}(z) > 0\}, \qquad \begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot z = \frac{az+b}{cz+d}$$



A **modular form** of weight k: holomorphic $f : \mathbb{H} \to \mathbb{C}$ with

$$f\left(\frac{az+b}{cz+d}\right) = (cz+d)^k f(z)$$

Connects to: **number theory** (counting arithmetic objects), **Fermat's Last Theorem** (Wiles 1995), **string theory** (partition functions).

Non-Examples: Which axiom fails?

Which of the following are groups? **Which axiom fails?**

Structure	Operation
$(\mathbb{Z}, \times)$	multiplication
$(\mathbb{N}, +)$	addition
$(M_n(\mathbb{R}), \times)$	matrix multiplication
$(\mathbb{Z}, -)$	subtraction

Non-Examples: Answers

Structure	Fails	Type
$(\mathbb{Z}, \times)$	**no inverses** – $2^{-1} \notin \mathbb{Z}$	monoid
$(\mathbb{N}, +)$	**no inverses** – $-3 \notin \mathbb{N}$	monoid
$(M_n(\mathbb{R}), \times)$	**no inverses** – singular matrices	monoid
$(\mathbb{Z}, -)$	**not associative** – $(1-1)-1 \neq 1-(1-1)$	magma

Monoid = associative + identity, but no inverses. **Magma** = just closure.

Subgroups

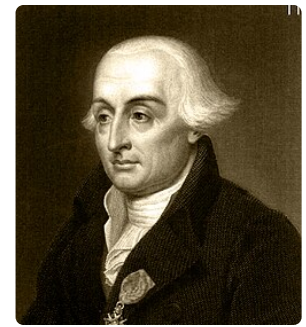
Definition. A nonempty subset $H \subseteq G$ is a **subgroup** of G (written $H \leq G$) if H is itself a group under the same operation.

One-step subgroup criterion. $H \leq G$ if and only if $H \neq \emptyset$ and

$$a, b \in H \implies ab^{-1} \in H$$

Two-step criterion. $H \leq G$ if and only if:

1. $a, b \in H \implies ab \in H$ (closed under multiplication)
2. $a \in H \implies a^{-1} \in H$ (closed under inverse)



Lagrange (1736–1813)

Lagrange's 1770 work on permutations of polynomial roots laid the groundwork for subgroup theory.

Subgroup Examples

Example 1. $k\mathbb{Z} = \{kn \mid n \in \mathbb{Z}\} \leq (\mathbb{Z}, +)$ for any $k \in \mathbb{Z}$.

Proof. If $a = km$ and $b = kn$, then $a - b = k(m - n) \in k\mathbb{Z}$. $\square$

Subgroup inclusion $\leftrightarrow$ divisibility: $m\mathbb{Z} \subseteq k\mathbb{Z} \iff k \mid m$.

$$6\mathbb{Z} \subset 3\mathbb{Z} \subset \mathbb{Z}, \qquad 6\mathbb{Z} \subset 2\mathbb{Z} \subset \mathbb{Z}$$

The **lattice of subgroups** of $(\mathbb{Z}, +)$ is exactly the **divisibility lattice** of $\mathbb{N}$.

A **lattice** is a partially ordered set where every pair has a **join** (least upper bound) and **meet** (greatest lower bound). For subgroups of G: meet = $H \cap K$, join = $\langle H, K \rangle$.

More examples: $A_n \leq S_n$ (alternating group), $SL_n(\mathbb{Z}) \leq GL_n(\mathbb{R})$.

Definition. The **center** of G is $Z(G) = \{g \in G \mid gx = xg \text{ for all } x \in G\} \leq G$.

Exercise. Verify that $Z(G)$ is a subgroup using the two-step criterion.

The Center of a Group

Recall. $Z(G) = \{g \in G \mid gx = xg \text{ for all } x \in G\}$.

Example 1. $Z(GL_n(\mathbb{R})) = \{\lambda I_n \mid \lambda \in \mathbb{R}^*\} \cong \mathbb{R}^*$ (scalar matrices).

Proof sketch. If A commutes with every invertible matrix, take $AE_{ij} = E_{ij}A$ for elementary matrices $\implies$ A is diagonal $\implies$ all diagonal entries equal. $\square$

Example 2. $Z(S_n) = \{e\}$ for $n \geq 3$ (the symmetric group has trivial center).

Example 3. $Z(D_n) = \{e, r^{n/2}\}$ if n even; $Z(D_n) = \{e\}$ if n odd.

Remark. The quotient $G/Z(G)$ is called the **inner automorphism group** $\mathrm{Inn}(G)$. Note $PGL_n(\mathbb{R}) = GL_n(\mathbb{R})/Z(GL_n(\mathbb{R}))$ – the **projective linear group**.

Homework. Write a complete proof that $Z(GL_n(\mathbb{R})) = \{\lambda I_n\}$. You may use ChatGPT/Gemini to help you understand the argument, but you must write the final proof **in your own words** and verify each step.

The Derived (Commutator) Subgroup

Definition. The **commutator** of $a, b \in G$ is $[a, b] = aba^{-1}b^{-1}$.

The **derived subgroup** (or commutator subgroup) is:

$$[G, G] = \langle [a, b] \mid a, b \in G \rangle$$

Key properties:

- $[G, G] \trianglelefteq G$ (it is a normal subgroup)
- $G/[G, G]$ is the largest **abelian quotient** of G (the abelianization G^{ab})
- G is abelian $\iff [G, G] = \{e\}$

Example: The Structure of $GL_n(\mathbb{R})$

Theorem. $[GL_n(\mathbb{R}), GL_n(\mathbb{R})] = SL_n(\mathbb{R})$ for $n \geq 2$.

Proof idea. $\det[A, B] = \det(ABA^{-1}B^{-1}) = 1$, so $[GL_n, GL_n] \subseteq SL_n$. Conversely, every matrix of determinant 1 is a product of commutators. $\square$

The abelianization: $GL_n(\mathbb{R})^{\text{ab}} = GL_n/SL_n \cong \mathbb{R}^*$ via $\det$.

Summary of $GL_n(\mathbb{R})$:

Subgroup	Description	Quotient
Center $Z(GL_n)$	$\{\lambda I_n \mid \lambda \in \mathbb{R}^*\}$	$PGL_n(\mathbb{R})$
Derived $[GL_n, GL_n]$	$SL_n(\mathbb{R})$	$\mathbb{R}^*$

$$1 \to SL_n(\mathbb{R}) \to GL_n(\mathbb{R}) \xrightarrow{\det} \mathbb{R}^* \to 1$$

Classification of Subgroups of $\mathbb{Z}$

Theorem. Every subgroup of $(\mathbb{Z}, +)$ is of the form $k\mathbb{Z}$ for some $k \in \mathbb{N}$.

Proof sketch. Let $H \leq \mathbb{Z}$. If $H = \{0\}$, then $H = 0\mathbb{Z}$. Otherwise, H contains a smallest positive element k (well-ordering). Then $H = k\mathbb{Z}$.

This gives a **bijection**:

$$\{\text{subgroups of } \mathbb{Z}\} \xleftrightarrow{1:1} \mathbb{N}, \qquad k\mathbb{Z} \longleftrightarrow k$$

Under this correspondence:

- $k\mathbb{Z} \subseteq m\mathbb{Z} \iff m \mid k$ (inclusion $\leftrightarrow$ divisibility)
- $k\mathbb{Z} \cap m\mathbb{Z} = \operatorname{lcm}(k, m)\mathbb{Z}$
- $k\mathbb{Z} + m\mathbb{Z} = \gcd(k, m)\mathbb{Z}$
- $\mathbb{Z}/k\mathbb{Z} \cong \mathbb{Z}_k$ (quotient $\leftrightarrow$ modular arithmetic)

Cosets

Definition. Let $H \leq G$ and $g \in G$. The **left coset** of H by g is:

$$gH = \{gh \mid h \in H\}$$

Key properties:

1. $g \in gH$ (since $e \in H$)
2. $gH = kH \iff k^{-1}g \in H$
3. Two cosets are either **equal** or **disjoint**
4. $|gH| = |H|$ for any $g \in G$

The coset relation $a \sim b \iff a^{-1}b \in H$ is an **equivalence relation** on G. Cosets are the equivalence classes of this relation.

The Coset Space and Lagrange's Theorem

Definition. The set of all left cosets is the **coset space**:

$$G/H = \{gH \mid g \in G\}$$

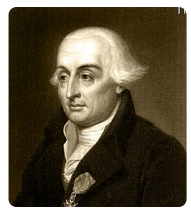
The number of cosets is the **index**: $[G : H] = |G/H|$.

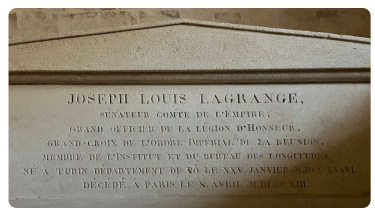
Lagrange's Theorem. If G is a finite group and $H \leq G$, then

$$|G| = [G : H] \cdot |H|$$

In particular, $|H|$ divides $|G|$.

Corollary. The order of any element divides $|G|$. Hence $g^{|G|} = e$ for all $g \in G$.





Lagrange (1736–1813)
Tomb in the Pantheon, Paris

Example: Cosets in $\mathbb{Z}/6\mathbb{Z}$

Let $G = \mathbb{Z}/6\mathbb{Z} = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}, \bar{5}\}$ and $H = \{\bar{0}, \bar{3}\}$.

The left cosets of H:

Coset	Elements
$\bar{0} + H$	$\{\bar{0}, \bar{3}\}$
$\bar{1} + H$	$\{\bar{1}, \bar{4}\}$
$\bar{2} + H$	$\{\bar{2}, \bar{5}\}$

So $[G : H] = 3$, and indeed $|G| = 6 = 3 \times 2 = [G : H] \cdot |H|$. ✓

Consequences of Lagrange's Theorem

Corollary 1. If $|G| = p$ (prime), then $G \cong \mathbb{Z}/p\mathbb{Z}$.

Proof. Take any $g \neq e$. Then $|\langle g \rangle|$ divides p, so $|\langle g \rangle| = p$, hence $\langle g \rangle = G$. $\square$

Corollary 2. (Fermat) If p prime, $\gcd(a, p) = 1$, then $a^{p-1} \equiv 1 \pmod{p}$.

Proof. Apply Lagrange to $(\mathbb{Z}/p\mathbb{Z})^*$, order $p - 1$. $\square$

Corollary 3. (Euler) If $\gcd(a, n) = 1$, then $a^{\varphi(n)} \equiv 1 \pmod{n}$.

Proof. Apply Lagrange to $(\mathbb{Z}/n\mathbb{Z})^*$, order $\varphi(n)$. $\square$

Fermat (1607–1665)

Euler (1707–1783)

Group Homomorphisms

> *"Rather than analyzing objects, we should concentrate on **morphisms** between them."* – Grothendieck

Definition. A map $f : G \to H$ is a **group homomorphism** if

$$f(ab) = f(a)f(b) \quad \text{for all } a, b \in G$$

Automatic consequences:

- $f(e_G) = e_H$
- $f(a^{-1}) = f(a)^{-1}$

Exercise. Prove these two consequences from the definition.

A. Grothendieck (1928–2014)

Kernel and Image

Definition. For a homomorphism $f : G \to H$:

- **Kernel**: $\ker(f) = \{g \in G \mid f(g) = e_H\}$
- **Image**: $\mathrm{im}(f) = \{f(g) \mid g \in G\}$

Key facts:

1. $\ker(f) \leq G$ and $\mathrm{im}(f) \leq H$
2. f is injective $\iff \ker(f) = \{e\}$
3. $\ker(f)$ is a **normal** subgroup of G

Exercise. Prove fact 3: if $g \in G$ and $n \in \ker(f)$, show $gng^{-1} \in \ker(f)$.

Order of an Element via $\mathbb{Z} \to G$

For any $g \in G$, define $\varphi_g : \mathbb{Z} \to G$ by $\varphi_g(n) = g^n$.

This is a **group homomorphism** $(\mathbb{Z}, +) \to (G, \cdot)$: $\varphi_g(m+n) = g^{m+n} = g^m \cdot g^n$.

By the first isomorphism theorem:

$$\mathbb{Z}/\ker(\varphi_g) \cong \mathrm{im}(\varphi_g) = \langle g \rangle$$

Since every subgroup of $\mathbb{Z}$ is $k\mathbb{Z}$, we have $\ker(\varphi_g) = d\mathbb{Z}$ for some $d \in \mathbb{N}$.

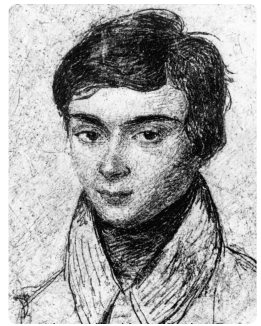
- If $d = 0$: $\langle g \rangle \cong \mathbb{Z}$ – infinite order
- If $d > 0$: $\langle g \rangle \cong \mathbb{Z}/d\mathbb{Z}$ – finite order d

Definition. The **order** of g is $\mathrm{ord}(g) = d = |\langle g \rangle|$.

So $\mathrm{ord}(g) = d \iff g^d = e$ and $g^k \neq e$ for $0 < k < d$, i.e., d is the smallest positive integer with $g^d = e$.

Normal Subgroups

Definition. $N \leq G$ is **normal** ($N \trianglelefteq G$) if $gNg^{-1} = N$ for all $g \in G$.



Galois (1811–1832)

Equivalent conditions:

1. $gNg^{-1} \subseteq N$ for all $g \in G$
2. $gN = Ng$ for all $g \in G$ (left cosets = right cosets)
3. $N = \ker(f)$ for some homomorphism f

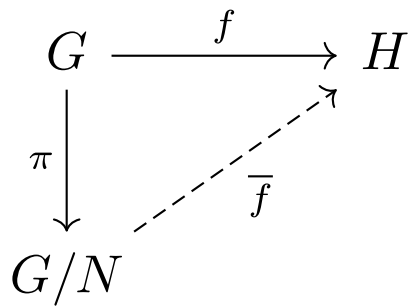
Why normal? Coset multiplication becomes well-defined: $(gN)(hN) = (gh)N$. This makes G/N a group – the **quotient group**.

Galois introduced normal subgroups in 1832, connecting them to solvability of polynomials.

Universal Property of the Quotient Group

Given $N \trianglelefteq G$, the **projection** $\pi : G \to G/N$, $g \mapsto gN$, satisfies:

Universal Property. For every homomorphism $f : G \to H$ with $N \subseteq \ker(f)$, there exists a **unique** homomorphism $\bar{f} : G/N \to H$ such that $f = \bar{f} \circ \pi$.



$$\bar{f}(gN) = f(g)$$

Why it matters:

- **Well-definedness** of $\bar{f}$ uses $N \subseteq \ker(f)$: if $gN = g'N$ then $g^{-1}g' \in N \subseteq \ker(f)$, so $f(g) = f(g')$
- $\bar{f}$ is injective $\iff$ $\ker(f) = N$ (this gives the First Isomorphism Theorem!)

The Isomorphism Theorems

First Isomorphism Theorem. If $f : G \to H$ is a homomorphism, then

$$G/\ker(f) \cong \mathrm{im}(f)$$

$$\begin{array}{ccc} G & \xrightarrow{\quad f \quad} & H \\ {\scriptstyle \pi}\downarrow & & \uparrow \\ G/\ker(f) & \xrightarrow[\overline{f}]{\cong} & \mathrm{im}(f) \end{array}$$

Second Isomorphism Theorem. If $A \leq G$ and $B \trianglelefteq G$, then

$$A/(A \cap B) \cong AB/B$$

Third Isomorphism Theorem. If $N \subseteq M$ are both normal in G, then

Emmy Noether (1882–1935)

Simple Groups

Definition. A group G is **simple** if its only normal subgroups are $\{e\}$ and G.

Examples:

- $\mathbb{Z}/p\mathbb{Z}$ for p prime (abelian simple groups)
- A_n for $n \geq 5$ (non-abelian simple groups)

Theorem. The only finite abelian simple groups are $\mathbb{Z}/p\mathbb{Z}$ for p prime.

Proof. If G is abelian, every subgroup is normal. If G is simple, it has no proper nontrivial subgroups. Take $g \neq e$; then $\langle g \rangle = G$. If $|G| = mn$ with $1 < m, n$, then $\langle g^m \rangle$ is a proper subgroup – contradiction. So $|G|$ is prime. $\square$

Classification of Finite Simple Groups

The **CFSG** (completed ~2004, tens of thousands of pages) states:

Every finite simple group is one of:

1. $\mathbb{Z}/p\mathbb{Z}$ (cyclic of prime order)
2. A_n for $n \geq 5$ (alternating groups)
3. A group of **Lie type** (e.g., $PSL_n(\mathbb{F}_q)$)
4. One of **26 sporadic groups** (e.g., the Monster group, $|M| \approx 8 \times 10^{53}$)

The Monster group has dimension 196,883 in its smallest faithful representation — its connections to modular functions are known as **"monstrous moonshine"** (proved by Borcherds, 1992).

This course: We will use simple groups as building blocks via **composition series** (next lecture).

Homework (Lecture 1)

Problem 1. From groups to simple groups

a. Prove that if $H \leq G$ and $[G : H] = 2$, then $H \trianglelefteq G$.

b. Let $|G| = p$, where p is prime. Prove that G is cyclic.

c. Prove that every finite abelian simple group is isomorphic to $\mathbb{Z}_p$ for some prime p.

d. Explain why part © does not say that every finite simple group is abelian.

Problem 2. How homomorphisms compress structure

a. Let $f : G \to H$ be a group homomorphism. Prove that $\ker(f) \trianglelefteq G$.

b. If $f : G \to H$ is surjective and G is abelian, prove that H is abelian.

c. Show by example that the converse is false.

d. Find a non-abelian group with an abelian quotient, and explain what structure is being forgotten in the quotient.

Looking Ahead

In this course, we will study:

1. **Subnormal series** – decomposing groups into simple factors
2. **Sylow theorems** – existence and structure of p-subgroups
3. **Free groups** – universal constructions
4. **Field extensions** – moving from groups to fields
5. **Galois theory** – connecting field extensions to group theory

Next lecture: Subnormal series and solvable groups.

Questions?