Notes of Abstract Algebra

Yuang Lu

2025 Fall

Chapter 1

2025/9/8

Some goals of this course.

- What is Abstract Algebra?

  Goal: study algebraic operations, namely $+, -, \times, \div$.

- Group Theory, Ring Theory and Field Theory, ordered in the complexity of operations endowed with.

- In group theory, we will spend some time on groups and maps between them. Subsequently, the subgroups of a group, group action[1] and group classification.

- In ring theory, we will similarly spend time on rings and maps between them. Afterwards ideals of rings, example of rings and perhaps modules. More advanced topics of ring theory will be discussed in the course Commutative Algebra.

- In field theory, we will start by field extensions, automorphisms and finally Galois Theory.

1.1 Groups

Definition 1.1. If a set G is endowed with a binary operation

$$\begin{aligned} * : G \times G &\to G \\ (x, y) &\mapsto x * y, \end{aligned}$$

then we call G

1. a *semigroup* if $*$ satisfies the condition

$$(x * y) * z = x * (y * z) = x * y * z.$$

2. a *monoid* if it is a semigroup and it has an identity element e_G satisfying

$$x * e_G = e_G * x = x, \quad \forall x \in G.$$

[1] In this course, we only care 2 group actions.

3. a *group* if it is a monoid and for all $g \in G$ there exists $g^{-1} \in G$ such that

$$g * g^{-1} = g^{-1} * g = e_G.$$

Some conventions for simplicity.

- $(G, *) = G$, e.g. $\mathbb{Z}$ is a group under addition. Note that $\mathbb{Z}$ is not a group under multiplication, as 0 does not have an inverse.
- $x * y = xy$.
- The operation $*$ is often called *group law* or *group multiplication* despite the fact that $*$ might not be an actual multiplication.

Example. Some examples of groups.

1. $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ are groups under additions with 0 as the identity element.
2. Matrices. $M_n(\mathbb{R}) = \{A = (a_{ij}) : n \times n \text{ matrix}, a_{ij} \in \mathbb{R}\}$ is a group under addition.
3. Polynomials. $\mathbb{R}[x] = \{\text{polynomials with coefficients in } \mathbb{R}\}$ is a group under addition.

Definition 1.2. A group $G = (G, *)$ is *abelian* or *commutative* if

$$\forall x, y \in G, \quad x * y = y * x.$$

The reason why we call $*$ multiplication rather than addition is that addition always implies the commutative law.

Example. Matrix multiplication. For any $A, B \in M_n(\mathbb{R})$, we have $AB \in M_n(\mathbb{R})$. The identity $e = I_n$. Yet $M_n(\mathbb{R})$ is but a monoid as there exists A without an inverse. Also note that $AB \neq BA$ for some $A, B \in M_n(\mathbb{R})$.

1.2 Subgroups

For a subset H of a group G, the question rises "when does H have a group struction inherited from G".

Definition 1.3. If $H \subset G = (G, *)$ is a subset, we say H is a subgroup of G if $(H, *)$ is a group. And we write $H \leq G$.

The above statement implies the following.

1. $*$ is a binary operation. (Fails for $G = \mathbb{Z}$ and $H = 2\mathbb{Z} + 1$.)
2. H contains an identity.
3. $\forall g \in H, g^{-1} \in H$.

Proposition 1.1. Nonempty subset $H \subset G$ is a subgroup if it is closed under division, i.e. $\forall x, y \in H$, we have $xy^{-1} \in H$.

Proof. First $e = xx^{-1} \in H$ for some x, so H must contain identity. Then $\forall x \in H$, $x^{-1} = ex^{-1} \in H$. Finally, $\forall x, y \in H$, $y^{-1} \in H$ and $xy = x\left(y^{-1}\right)^{-1} \in H$. □

Example. $\mathbb{Z}$ has subgroups $k\mathbb{Z} = \{kn : n \in \mathbb{Z}\}$, which are closed under subtraction for each $k \in \mathbb{Z}$. In fact, these are all the subgroups of $\mathbb{Z}$.

Definition 1.4. Suppose G a group, $a \in G$ an element. We define

$$\langle a \rangle \triangleq \{a^n : n \in \mathbb{Z}\}.$$

Lemma 1.2. $\langle a \rangle$ is a subgroup of G.

Proof. For all $a^n, a^m \in \langle a \rangle$, $a^n (a^m)^{-1} = a^{n-m} \in \langle a \rangle$. □

Lemma 1.3. $\langle a \rangle$ is abelian.

Hence $\langle a \rangle$ is called a *cyclic* subgroup of G.

Definition 1.5. G is called a cyclic group if $G = \langle a \rangle$ for some $a \in G$.

Example.
1. $G = \mathbb{Z}/n\mathbb{Z} = \left\{\overline{0}, \overline{1}, \ldots, \overline{n-1}\right\}$, with $\overline{a} + \overline{b} = \overline{a + b \pmod{n}}$, is a group (and cyclic) for prime n.
2. $\mathbb{Z} = \langle 1 \rangle$ is an infinite cyclic group.

Definition 1.6. Let the *order of a group* G be its cardinality as a set: $|G| = \operatorname{card} G$. For $a \in G$, let the *order of* a be $\operatorname{ord}(a) \triangleq |\langle a \rangle|$.

Example. If $G = \mathbb{Z}$, $|G| = \infty$, $\forall k \in \mathbb{Z} \setminus \{0\}$, $\operatorname{ord}(k) = \infty$.
Any $a \in G$, $\operatorname{ord}(a) = 1 \iff a = e$.

Now we have enough tools to prove that each subgroup of $\mathbb{Z}$ is equal to some $\langle k \rangle$.

Lemma 1.4. The subgroup of a cyclic group remains cyclic.

We consider the case $G = \mathbb{Z} = \langle 1 \rangle$: $\forall H \leq \mathbb{Z}$, $H = \langle k \rangle$ for some $k \in \mathbb{Z}$.

Proof. Take k as the smallest positive integer in H, then $\langle k \rangle = H$. Since

$$a \in H \leq G \implies \langle a \rangle \leq H$$

Now if $H \neq \langle k \rangle$, $\exists 0 \neq k' \in H$, k' is not a multiple of k, but $\gcd(k, k') < k$ is contained in H. □

Another question is how to classify all the cyclic groups. Suppose $G = \langle a \rangle$ for some a.

- $\operatorname{ord}(a) = |G| = \infty$ implies $G = \left\{\ldots, a^{-1}, a^0 = e, a^1 = a, a^2, \ldots\right\}$ and $a^n \neq a^m$ if $n \neq m$.
- $\operatorname{ord}(a) = |G| = n$ implies $G = \{a^0 = e, a^1, a^2, \ldots, a^{n-1}\}$.

Proof. If $|G| = \infty$, $a^k \neq a^m$ once $k \neq m$. This is because $a^k = a^m$ and $k \neq m$ implies $a^{k-m} = a^k a^{-m} = e$ and hence $k = m$, which provides a contradiction. The rest follows suit. □

Chapter 2

2025/9/10

2.1 Subgroups & Presentations of Groups

For a group G, it is a set G plus the group law $*$. H is subgroup $\iff$ $H \subseteq G$ and $(H, *)$ is a group. Given G, there are

- the trivial subgroups: $\{e\}$ and G.
- non-trivial subgroups, e.g.

$$a \in G \rightsquigarrow \langle a \rangle \leq G$$
$$\{a\} \subseteq G \rightsquigarrow \langle \{a\} \rangle \leq G,$$

  with the former a cyclic subgroup, and the latter a subgroup generated by a subset $\{a\}$.

Definition 2.1. Define $\langle S \rangle$ as the *subgroup generated by* S.

$$\langle S \rangle \triangleq \bigcap_{H \leq G, S \subseteq H} H.$$

Here we use the simple fact: If we have $H_1 \leq G$ and $H_2 \leq G$, then $H_1 \cap H_2 \leq G$.

Remark. $H_1 \cup H_2 \not\leq G$.

Proposition 2.1.

$$\langle S \rangle = \left\{ \prod_{\text{finite}} a_i : a_i \in S \text{ or } a_i^{-1} \in S \right\}.$$

Proof. We prove the following three steps.

1. RHS is a subgroup.
2. $S \subseteq$ RHS.
3. $\langle S \rangle =$ RHS by showing that RHS is the smallest one.

For 2, $S = \{a : a \in S\} \subseteq$ RHS. For 3, we shoulde prove $\forall H \leq G (H \supseteq S \implies H \supseteq \text{RHS})$. This is because if $H \supseteq S$, since H is closed under division, $\prod_{\text{finite}} a_i \in H, a_i$ or $a_i^{-1} \in S$. These two are almost free.

For 1, we claim that for any $\prod a_i, \prod b_i \in \text{RHS}$, $\left(\prod a_i\right)\left(\prod b_i\right)^{-1} \in H$. Given the fact that

$$\left(\prod_{i=1}^{n} b_i\right)^{-1} = b_n b_{n-1} \cdots b_1$$

we can write

$$\left(\prod_{i=1}^{m} a_i\right)\left(\prod_{i=1}^{n} b_i\right)^{-1} = \prod_{i=1}^{m} a_i \prod_{i=1}^{n} b_{n+1-i}^{-1} \in \text{RHS}. \qquad \square$$

If $H \leq G$ and $H = \langle S \rangle$, then we call S the *generators* of H or H is *generated by* S.

Example. $G = \mathbb{Z}$, and $\mathbb{Z} = \langle 1 \rangle$.

Example. We have $GL_n(\mathbb{R}) = \{A \in M_n(\mathbb{R}) : \det(A) \neq 0\}$ generated by diagnoal and elementary matrices.

Example (Why?)**.** We have $SL_2(\mathbb{Z}) = \{A \in M_2(\mathbb{Z}) : \det(A) = 1\}$ generated by

$$\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \quad \& \quad \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}.$$

Example. $H = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} = \{(0,0), (1,0), (0,1), (1,1)\}$. $(H, +)$ is a group under the natural addition $(a, b) + (c, d) = (a + c, b + d)$, which is generated by $(1, 0)$ and . Note that H is none cyclic because there is not an element of order 4 in H.

Remark. G is a cyclic group iff there exists $a \in G$ such that $\text{ord}(a) = |G|$.

If we have $G = \langle S \rangle$ for some $S \subseteq G$, we know very little from the definition of $\langle S \rangle$.

Definition 2.2. For any set S, we define a *free group* generated by S. $\langle S \rangle_{\text{free}}$ contains all the words composed of letters in S.

$$\langle S \rangle_{\text{free}} \triangleq \left\{a_1 \cdots a_n : a_i \in S \text{ or } S^{-1}\right\},$$

with S^{-1} defined formally as $\left\{a_i^{-1} : a_i \in S\right\}$. The group law of $\langle S \rangle_{\text{free}}$ is the juxtaposition of word. Note that the identity is the empty word.

Example. For $S = \{a\}$, $\langle S \rangle_{\text{free}} = \langle a \rangle = \mathbb{Z}$.

Example. For $S = \{a, b\}$, $S^{-1} = \{a^{-1}, b^{-1}\}$. The structure of $\langle S \rangle_{\text{free}}$ is very complex and very far from $\mathbb{Z} \times \mathbb{Z}$.

The reason we call the group defined above "free group", is that from any set we obatin a group, with no extra relations. And any group G can be obtained by adding more relations to a free group.

Example.

- $\mathbb{Z}/2\mathbb{Z}$ comes from a cyclic free group as it is generated by a single element.

$$\mathbb{Z}/2\mathbb{Z} = \langle a \mid aa = e \rangle_{\text{free}} = \{e, a\}.$$

- $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ comes from the free group with relations

$$\langle a, b \mid aa = e, bb = e, ab = ba \rangle_{\text{free}} = \{e, a, b, ab = ba\}.$$

- $SL_2(\mathbb{Z})$, recall the previous example, comes from the free group with relations

$$\langle a, b \mid aaaa = e, ab = b^? a^? \rangle_{\text{free}}.$$

Definition 2.3. If G a group, the *center* of G

$$C(G) \triangleq \{g \in G : gh = hg, \forall h \in G\}.$$

Note that $C(G)$ is an abelien subgroup of G.

Definition 2.4. For $g \in G$, the centralizer of g

$$C_g(G) \triangleq \{h \in G : hg = gh\}.$$

$C_g(G)$ is also a subgroup.

2.2 Symmetric Group

This is an important example in group theory.

Definition 2.5. Let Σ be a set, then

$$S_\Sigma \triangleq \{f : \Sigma \to \Sigma : f \text{ is bijective}\}.$$

$(S_\Sigma, \circ)$ is a group under composition. If Σ is a finite set, namely, $|\Sigma| = n$, we can use S_n to denote S_Σ.

We are concerned with the following topics.

- Order of elements in S_n.
- Subgroups of S_n.
- Normal subgroups. (Next Week)

We mainly consider finite symmetric groups.

Proposition 2.2. 1. S_n is abelien iff $n \leq 2$.

2. S_3 is the smallest non-abelien finite group.

In order to better describe elements in S_3, we need the definition below.

Definition 2.6. A m-cycle $(a_1\ a_2\ \dots\ a_m)$, $a_i \in \Sigma$ is a map

$$\begin{aligned} f : \Sigma &\to \Sigma \\ a_i &\mapsto a_{i+1}, \quad a_{m+1} = a_1 \\ b &\mapsto b, \quad b \neq a_i \end{aligned}$$

Proposition 2.3. For any $\sigma \in S_n$, there exists a unique decomposition

$$\sigma = \tau_1 \cdots \tau_k,$$

where τ_i are disjoint cycles. Here, Σ_i and Σ_j are disjoint if $|\Sigma_i| \cap |\Sigma_j| = \varnothing$ and $|(a_1\ \cdots\ a_m)| = \{a_1, \dots, a_m\}$.

The proof is trivial.

Sketchy Proof of Proposition 2.2. 1. $(1\ 2)(2\ 3) = (1\ 2\ 3) \neq (1\ 3\ 2) = (2\ 3)(1\ 2)$.

2. For groups of order 1,2,3,5, they must be cyclic. For groups of order 4, there are two possibilities $\mathbb{Z}/4\mathbb{Z}$ and $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. □

Chapter 3

2025/9/15

3.1 Symmetric Group

Recall that

$$S_n = \{\text{permutation of the set } \{1, 2, \ldots, n\}\}.$$

It is a group under composition. We kwow the following facts.

- $|S_n| = n!$.
- For any $a \in S_n$, according to cycle decomposition, we have the unique formula up to a permutation of cycles

  $$a = \prod_{\text{disjoint}} \tau_i,$$

  where τ_i are cycles. Since τ_i, τ_j commute for each pair (i, j), $\text{ord}(a) = \text{lcm}(\text{ord}(\tau_i)) = \text{lcm}(|\tau_i|)$.
- S_n is generated by cycles. Further, by 2-cycles or *transportations*. And even further, either by $(1\ i), 2 \leq i \leq n$ or by $(1\ 2)$ and $(1\ 2\ 3\ \cdots\ n)$.

Definition 3.1 (Alternating group)**.**

$$A_n = \{\text{even permutations in } S_n\}.$$

Some well-known facts.

- $|A_n| = \frac{|S_n|}{2} = \frac{n!}{2}$.
- $A_n \leq S_n$.
- A_n is generated by 3-cycles.

3.2 Coset of subgroups & Quotient Groups

Definition 3.2. For $H \leq G$ a subgroup, $\forall a \in G$, we define

$$aH \triangleq \{ah : h \in H\} \subseteq G,$$

called a *left coset* of H. Similarly we can define the *right cosets*.

We have some easy properties.

- $|H| = |aH| = |Ha|$, $\forall a \in G$.
- aH, or Ha, is a subgroup iff $a \in H$.

We can now consider new players: aH. Consider, what is the relation between aH, bH and abH, i.e. do we have

$$(aH)(bH) = (ab)H?$$

We hope that there is an algebraic relation on cosets. But unfortunately, this idea does not hold in general.

Definition 3.3. If $H \leq G$, we say H is a normal subgroup of G if the following equivalent conditions hold

1. $(aH)(bH) = (ab)H, \quad \forall a, b \in G$.
2. $aH = Ha, \forall a \in G$.
3. $H = aHa^{-1}, \forall a \in G$.

Example. 1. If G is an abelian group, then $\forall H \leq G$ is a normal group.

2. If $G = S_3$, we have subgroups $H_1 = \langle (1\ 2) \rangle$ and $H_2 = \langle (1\ 2\ 3) \rangle$.

Proposition 3.1. If $H \leq G$, we have

$$G = \coprod_{a \in G} aH = \coprod_{a \in G} Ha.$$

And $aH \cap bH = \varnothing$ if $aH \neq bH$.

Example. $H \leq G$, $|H| = \frac{1}{2}|G|$, then H is a normal subgroup. Especially, A_n is a normal subgroup of S_n.

Chapter 4

2025/09/17

4.1 Cosets & Quotient groups

Theorem 4.1 (Lagrange's Theorem)**.** If $H \leq G$, then if $|G| < +\infty$, the number of cosets is

$$\frac{|G|}{|H|},$$

such number is denoted by $[G : H]$, called the *index* of H in G.

Corollary. If $H \leq G$, and $|G| < +\infty$, then $|H| \mid |G|$. In particular, $\forall a \in G$, $H = \langle a \rangle$, $\mathrm{ord}(a) || G|$.

Corollary. If $|G| = p$ is a prime number, then $G = \langle a \rangle$ is a cyclic group and hance abelian.

Proof. Take $a \neq e \in G$, $\mathrm{ord}(a) \neq 1$ and $\mathrm{ord}(a) \mid |G| = p$, so $\mathrm{ord}(a) = p$. It follows that $|\langle a \rangle| = p$ and $\langle a \rangle = G$. □

Proposition 4.2. If $|G| = p^2$, where p prime, then G is also abelian but not necessarily cyclic.

Part of Proof. Consider $C(G) \leq G$. By Lagrange's Theorem, $|C(G)| \mid p^2$. $|C(G)| = 1$, p or p^2.

1. If $|C(G)| = p^2$, $C(G) = G$, we obtain the desired result.
2. If $|C(G)| = p$, $[G : C(G)] = \frac{|G|}{|C(G)|} = p$. The cosets of $C(G)$ are $aC(G), a^2C(G), a^{p-1}C(G)$ for some $a \in G$. For any $g \in G$, g can be written as $a^k h$, $h \in C(G)$. Then any two elements $a^k h, a^l h$ in G have
$$\left(a^k h\right)\left(a^l h'\right) = a^{l+k} hh' = a^{l+k} h' h,$$
because $h, h' \in C(G)$ can commute with elements in G. G is thus abelian.
3. If $|C(G)| = 1$, this is also impossible. See 8. □

Definition 4.1. If H is a normal subgroup of G, denoted by $H \lhd G$. We can define the *quotient group*

$$G/H \triangleq \{aH\},$$

with $(aH)(bH) = (ab)H$ as the group law.

We have some easy properties.

- G/H is a group, with identity $\overline{e} = eH = H$.
- $\overline{g} = gH$ has an inverse $\overline{g^{-1}} = g^{-1}H$.
- $|G/H| = [G : H]$.

Back to the case $|G| = p^2$, $|C(G)| = p$. then $|G/C(G)| = p$ and $G/C(G)$ is a cyclic group. There exists $a \in G$ such that $G/C(G) = \langle aC(G)\rangle = \{a^k C(G)\}$.

Recall one of the goals in group theory: to classify some finite groups. We need the following definition.

Definition 4.2. G is a *simple group* if every normal subgroup of G is trivial, i.e. $\{e\}$ and G.

The ultimate goal in finite group theory is to classify all the finite groups, which has been realized. A way to simplify this monstrous task is to consider the normal subgroups and quotient groups of finite groups[1]. This process terminates at simple groups. Hence to classify finite groups is to classify simple finite groups.

Theorem 4.3. 1. A_n is simple when $n \geq 5$.

2. A_5 is the smallest non-abelian simple group.

Remark. 1. If $G = \mathbb{Z}/p\mathbb{Z}$, p is a prime, then G is an abelian simple group.

2. If G is a simple abelian group, then G is a cyclic group of prime order.

Example.
- $A_n \lhd S_n$.
- $SL_n(\mathbb{R}) \lhd GL_n(\mathbb{R})$.
- $H \leq G$ not necessarily normal, we can define a new group

$$N_G(H) = \{g \in G : g^{-1}Hg = H\}$$

called the *normalizer* of H in G, then $H \lhd N_G(H)$ and $H \lhd G \iff N_G(H) = G$.

[1] We can recover G from H and G/H from direct products and semidirect products.

Chapter 5

2025/9/22

5.1 Normal subgroup & Simple group

For G a group and $H \leq G$ a subgroup, our question is how to show H is a normal subgroup?

1. Verify that $aH = Ha$, for all $a \in G$. *Application*: $[G : H] = 2 \implies H \lhd G$.
2. Verify that aHa^{-1}, for all $a \in G$. A simple observation is that aHa^{-1} is a subgroup of G, so it suffices to check the generators are the same, i.e.

$$H = \langle S \rangle, \quad \forall g \in S, aga^{-1} \in H.$$

   This makes things much easier as S is usually a very small set.

Example. If G a group, define the *commutator* of G.

$$[G, G] \triangleq \langle aba^{-1}b^{-1} \mid a, b \in G \rangle \leq G.$$

We claim $[G, G] \lhd G$.

Proof. For each generator $aba^{-1}b^{-1} \in [G, G]$, and $g \in G$, then

$$g(aba^{-1}b^{-1})g^{-1} = (gag^{-1})(gbg^{-1})(ga^{-1}g^{-1})(gb^{-1}g^{-1}) \in [G, G]. \qquad \square$$

Remark. $G/[G, G] = G^{\text{ab}}$ is an abelian group, called the *abelianization* of G. [1]

For simple groups, we have an analogous question: "how to determine whether G is a simple group?"

Example. If $|G| < +\infty$,

1. $|G| = 4 \implies G$ is not a simple group as G is abelian.
2. $|G| = 6$, if $G = S_3$ then G is not simple since $C_3 \cong A_3 \lhd S_3$.

Recall the following theorem about the smallest non-abelian simple finite group.

[1] For example, for a topological space X which is simplicial,

$$\pi_1(X)^{\text{ab}} = H_1(X, \mathbb{Z}).$$

Theorem 5.1. The smallest non-abelian simple finite group is A_5.

There are two steps of difficulty.

1. A_5 is simple.
2. A_5 is the smallest among such. Or more explicitly,
   (a) $|G| < 60$ and non-abelian, then G is non-abelian.
   (b) $|G| = 60$ and simple, then $G = A_5$.

Today we shall deal with the first step. We need a tool beforehand.

Definition 5.1. $a \in G$, its *conjugacy class* $[a] = \{gag^{-1} : g \in G\}$.

Then $H \leq G$ is normal iff H is a union of conjugacy classes.

Lemma 5.2. $\tau \in S_n$, and $(a_1 \ \cdots \ a_k)$ is a k-cycle, then

$$\tau(a_1 \ \cdots a_k)\tau^{-1} = (\tau(a_1) \ \tau(a_2) \ \cdots \ \tau(a_k)).$$

It follows naturally that conjugacy classes in S_n are indentical to types of cycle decomposition. However, for $\sigma \in A_n$, $[\sigma]_{A_n} \subseteq [\sigma]_{S_n}$ and the equivalence often fails. In fact, $[\sigma]_{A_n} = [\sigma]_{S_n}$ iff σ commutes with some 2-cycle.

Theorem 5.3. A_n is a non-abelian simple group iff $n \geq 5$.

Sketch of Proof. When $n < 5$,

1. $n = 2, 3$, abelian.
2. $n = 4$, non-abelian, as $V = e \cup [(1\ 2)(3\ 4)]$ the Klein 4-group is a normal subgroup.

When $n \geq 5$, given $H \lhd A_n$, $H \neq \{e\}$, we need to show $H = A_n$. That is to say, H contains a subset that generates A_n. If H contains a 3-cycle, then H contains all $(1\ 2\ k)$. And H must contain a 3-cycle, so $H = A_n$. □

Chapter 6

2025/9/24

Recall that in the previous leture, we began the proof of A_n being simple when $n \geq 5$.

6.1 Group homomorphism

Definition 6.1. If G, G' are groups, then a *group homomorphism* $f : G \to G'$ is a map, such that it preserves the group law, i.e.

$$f(ab) = f(a)f(b), \quad \forall a, b \in G.$$

Proposition 6.1. $f(e_G) = e_{G'}$, $f(a^{-1}) = f(a)^{-1}$.

Proof. Since $f(ab) = f(a)f(b)$ for any $a, b \in G$, take $a = b = e_G$, $f(e_G) = f(e_G)f(e_G)$, and by cancelling out one $f(e_G)$, we get $f(e_G) = e_{G'}$. Similarly,

$$e_{G'} = f(aa^{-1}) = f(a)f(a^{-1}) \quad \Longrightarrow \quad f(a^{-1}) = f(a)^{-1}. \qquad \square$$

Example. 1. Integers modulo n.

$$\begin{aligned} f : \mathbb{Z} &\to \mathbb{Z}/n\mathbb{Z} \\ k &\mapsto k \pmod{n}. \end{aligned}$$

2. The exponential map.

$$\begin{aligned} \mathbb{R} &\to \mathbb{C}^* \\ a &\mapsto \exp(ia). \end{aligned}$$

3. The determinant,

$$\begin{aligned} \det : GL_n(\mathbb{R}) &\to \mathbb{R}^* \\ A &\mapsto \det A. \end{aligned}$$

Definition 6.2. A group homomorphism $f : G \to G'$ is an *isomorphism* if there is also another homomorphism $g : G' \to G$ such that $f \circ g = \mathrm{id}_{G'}$ and $g \circ f = \mathrm{id}_G$.

Definition 6.3. If f is a group homomorphism, the *kernel* of f is

$$\mathrm{Ker}(f) \triangleq \{a \in G : f(a) = e\},$$

and the *image* of f

$$\mathrm{Im}(f) \triangleq \{f(a) : a \in G\}.$$

Theorem 6.2 (Fundamental Theorem for group homomorphism)**.** 1. $\mathrm{Ker}(f) \lhd G$; $\mathrm{Im}(f) \leq G'$.

2. f induces an isomorphism

$$f : G/\mathrm{Ker}(f) \cong \mathrm{Im}(f) \leq G'.$$

Proof. 1. Omitted.

2. Consider the map

$$\begin{aligned} \overline{f} : G/\mathrm{Ker}(f) &\to G' \\ \overline{a} &\mapsto f(a). \end{aligned}$$

We need to verify that $\overline{f}$ is well-defined, is a group homomorphism and is bijective. All of them are easy to see. □

Remark. f is injective iff $\mathrm{Ker}(f) = \{e\}$.

Since $Ker(f) \lhd G$, we have the following corollary.

Corollary. If there exists a non-trivial group homomorphism $G \to G'$, then G is not simple.

For any $N \lhd G$, then we have $f : G \to G/N, a \mapsto \overline{a}$ a quotient map, which is group homomorphism and $\mathrm{Ker}(f) = N$.

Example (Another definition of A_n)**.** A_n is the kernel of the sign of permutations.

$$\begin{aligned} \mathrm{sgn} : S_n &\to \mathbb{Z}/2\mathbb{Z} \\ \sigma &\mapsto \mathrm{sgn}(\sigma) \end{aligned}$$

Also we have $SL_n(\mathbb{R}) = \mathrm{Ker}(\det)$.

The consequences of Theorem (6.2) is the followings.

Theorem 6.3. G is a group, $H \leq N \leq G$ and $H \lhd G, N \lhd G$, then

$$G/N \cong (G/H)\Big/(N/H)$$

Proof. 1. $H \lhd N$ as $gHg^{-1} = H$ for any $g \in N \subseteq G$, so RHS is well-defined.

2. Construct a group homomorphism:

$$\begin{aligned} \varphi : G/H &\to G/N \\ aH &\mapsto aN. \end{aligned}$$

This is obviously surjective, and well-defined. Its kernel

$$\mathrm{Ker}(\varphi) = \{aH : aN = N\} = \{aH : a \in N\} = N/H.$$ □

Theorem 6.4. $H \lhd G$, $K \leq G$, then $KH = HK$ and

$$K/(K \cap H) \cong HK/H.$$

Proof. Just prove that $HK \leq G$ and consider the homomorphism $K \to HK/H$. □

Chapter 7

2025/9/29

Some interesting questions of group homomorphism.

1. Given two groups, G and G', how to tell the difference between two groups, e.g. $G \cong G'$?
   (a) $G \ncong G'$ if $|G| \neq |G'|$, e.g. $\mathbb{Q}/\mathbb{Z} \ncong \mathbb{R}/\mathbb{Q}$.
   (b) If $G \cong G'$, for $a \in G$, there must exist some $a' \in G'$ s.t. $\operatorname{ord}(a) = \operatorname{ord}(a')$.
2. How to find group homomorphisms between different groups? For instance, given G and G', find out all the group homomorphisms $\varphi : G \to G'$.
   (a) For $G = \langle a \rangle$ a cyclic group, consider
   $$\operatorname{Aut}(G) = \left\{ \varphi : \langle a \rangle \xrightarrow{\cong} \langle a \rangle \right\}.$$
   Note that $\operatorname{Im}(\varphi) = \langle \varphi(a) \rangle = \langle a \rangle$ iff $\operatorname{ord}(\varphi(a)) = \operatorname{ord}(a)$, when $\operatorname{ord}(a) < +\infty$. Hence
   $$\operatorname{Aut}(G) \xleftrightarrow{1:1} \{ b \in G : \operatorname{ord}(b) = \operatorname{ord}(a) \}.$$
   (b) For general $G = \langle S \rangle$, we only need to consider the image of generators. In other words, we only need to define
   $$\begin{aligned} &\varphi : G \to G' \\ &a \in S \mapsto \varphi(a) \end{aligned}$$
   and check $\varphi(a), a \in S$ satisfy the group law in G'.

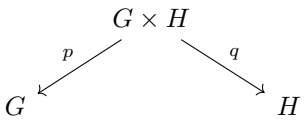
7.1 Direct Product of Groups

Idea. In set theory, if we have X, Y as sets, we can define their direct product $X \times Y$.

Definition 7.1. If G and H are groups, we define
$$G \times H \triangleq \{(g, h) : g \in G, h \in H\}$$
and $(G \times H) \times (G \times H) \to (G \times H), (g_1, h_1)(g_2, h_2) \to (g_1 g_2, h_1 h_2)$.

Proposition 7.1. 1. $G \times H$ is a group.

2. $G \times H$ carries projections.



3. There exists inclusions $G \overset{i}{\hookrightarrow} G \times H$ and $H \overset{j}{\hookrightarrow} G \times H$ s.t.

$$p \circ i = \mathrm{id}_G, \quad q \circ j = \mathrm{id}_H.$$

Remark. The properties in Proposition 7.1 is in fact the universal property of dirct product.

Theorem 7.2. We can write $G \cong G_1 \times G_2$ iff $\exists H, K \lhd G$, $H \cap K = \{e\}$ and $HK = G$.

Proof. It suffices to verify that the map

$$\begin{aligned} \varphi : H_1 \times H_2 &\to H_1 H_2 \\ (g_1, g_2) &\mapsto g_1 g_2 \end{aligned}$$

is a group isomorphism. □

Chapter 8

2025/10/13

Recall. The direct product of groups.

Applications of Direct Products.

1. Fundamental Theorem for abelian groups.

   Fact. If G, G' are abelian groups, then $G \times G'$ remains abelian. Especially, the product of cyclic groups are abelian.

   Hence it is natural to propose the converse: "any finitely generately abelian group is isomorphic to the products of some cyclic groups."

   Remark. When $|G| = 6$, there is only one such abelian group, $\mathbb{Z}/6\mathbb{Z}$. When $|G| = 4$, there are two, $\mathbb{Z}/4\mathbb{Z} \ncong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

2. Understand the structure of finite groups. For instance, given a group G of order 6, not necessarily abelian. The idea is to consider elements in G. If $g \in G$, $\mathrm{ord}(g) \mid G$, so $\mathrm{ord}(g) = 1, 2, 3$ or 6. If $\mathrm{ord}(g) = 1$, $g = e$; if $\mathrm{ord}(g) = 6$, G is cyclic. If $\mathrm{ord}(g) = 2$ for all $g \in G$, then G is abelian, but this is absurd. Hence we can suppose there exists g s.t. $\mathrm{ord}(g) = 3$. $H = \langle g \rangle \lhd G$, as $[G : H] = 2$, so there exists g' s.t. $\mathrm{ord}(g') = 2$ and $H' = \langle g' \rangle$. So
$$G = HH\text{"} = \begin{cases} H \times H', & H' \lhd G \\ H \rtimes H', & \text{otherwise.} \end{cases}$$

8.1 Actions of Groups

Definition 8.1. For G a group and X a set, an action of group G on X is a map
$$\begin{aligned} \cdot : G \times X &\to X \\ (g, x) &\mapsto g \cdot x. \end{aligned}$$
satisfying

1. $e \cdot x = x$.
2. $g_1 \cdot (g_2 \cdot x) = (g_1 g_2) \cdot x$.

Example. 1. S_n acts on $\{1, 2, \ldots, n\}$.

2. Let V be a vector space over $\mathbb{F}$. $GL(V)$ acts on V.
3. *Left/Right multiplication.* Let G be a group, and X be a collection of certain subsets of G. Then $G \times X \to X, (g, H) \mapsto gH$ can be a group action. For X, possible selections include $\{H \subseteq G \mid |H| = n\}$, {cosets of $H \leq G$}.
4. *Adjoint action/Conjugation.* $G \times X \to X, (g, H) \mapsto g^{-1}Hg$. Some possible X's include G, {subgroups of G, with fixed order n}.

Remark. The first example is called a symmetric representation because of the following observation.

$$\{G\text{-actions on } X\} \leftrightsquigarrow \left\{G \xrightarrow{\rho} S_X \mid \rho \text{ is a homomorphism}\right\}.$$

Example (Good properties)**.** If G is a simple group and admits a group action $\rho : G \to S_X$, then ρ must be

1. injective, where $\mathrm{Ker}(\rho) = \{e\}$.
2. trivial, where $\mathrm{Ker}(\rho) = G$.

Assume G acts on a set X.

Definition 8.2. If $x \in X$, then

1. the *stablizer* of x is
$$G_x := \{g \in G \mid g \cdot x = x\}.$$
2. the *orbit* of x is
$$G \cdot x = \{g \cdot x \mid g \in G\}.$$

Remark. The orbits of elements of X, $G \cdot x$ form a set of equivalence classes.

Proposition 8.1. 1. $G_x \leq G$.

2. $|G \cdot x| = [G : G_x]$.
3. Since $X = \bigsqcup G \cdot x$, when $|X| < +\infty$, $|G| < +\infty$,
$$|X| = \sum |G \cdot x| = \sum \frac{|G|}{|G_x|}.$$

Example. 1. *Left/Right multiplication.* Consider $G \curvearrowright X = G$. For any $x \in G$, $G_x = \{e\}$, $G \cdot x = X = G$.[1]

2. *Adjoint action.* Consider $G \curvearrowright X = G$. For $x \in G$, $G_x = C_G(x)$ is the centralizer of x, and $G \cdot x = \{g^{-1}xg \mid g \in G\}$ is the conjugacy class of x. When $|G| < +\infty$, we can write
$$|X| = |G| = \sum_{G \cdot x} \frac{|G|}{C_G(X)}$$
and hence
$$|G| = |C(G)| + \sum_{|G \cdot x| > 1} \frac{|G|}{|C_G(x)|}$$

[1] When $G \cdot x = X$ for some action $G \curvearrowright X$, we call such action *transitive*.

Corollary. By the above formula, when $|G| = p^n$, p prime, the center of G is never trivial, i.e. $|C(G)| > 1$.

Theorem 8.2. Any group is a subgroup of some symmetric group.

Proof. Let G be a group. Consider the left multiplication action $G \curvearrowright G$, which yields a group homomorphism $G \xrightarrow{\rho} S_G$. This map is injective as

$$\mathrm{Ker}(\rho) = \bigcup_{x \in G} G_x = \{e\}. \qquad \square$$

8.2 Sylow's Theorem

By Lagrange's theorem, a subgroup H of group G satisfies $|H| \mid |G|$. Sylow's theorem is about the converse problem. For what divisors of $|G|$ does there exist a subgroup H such that $|H| = n$?

If no additional assumptions, this fails, since we can let $G = A_n, n \geq 5$ and $m = \frac{|G|}{2}$, then there is no such subgroup H as to satisfy $|H| = m$.

Theorem 8.3. The answer is positive if $m = p^n$.

Chapter 9

2025/10/15

9.1 Sylow's Theorem

Theorem 9.1. If $m = p^r$, where p is a prime, such subgroup will exist. Moreover, the number of such groups is congruent to 1 modulo p.

There are two strategies. First is to consider the cases where $m = p^r \mid n$, and r is maximal. Such groups are called Sylow p-subgroups. And we have the following theorems.

Theorem 9.2. 1. The number of Sylow p-groups is congruent to 1 modulo p.

2. If $|G| = p^k$, $\forall r < k$, $\exists H \leq G$, s.t. $|H| = p^r$.

The technique involved in the first part is also valid in the previous theorem.

Proof of the second part. Inducion on k. If $|G| = p^k$, $|G/C(G)| < p^k$, as $|C(G)| \neq 1$. Consider the quotient map $\pi : G \to G/C(G)$. For any $H \leq G/C(G)$, $\pi^{-1}(H) \leq G$ and $\pi^{-1}(H) \supseteq C(G)$.

- If $p^r \leq |C(G)| < |G|$, this is okay by the induction hypothesis, as we can find $H' \leq C(G), |H| = p^r$.
- $|G| = |C_(G)|$, decompose G as product of cyclic groups.
- $|C(G)| < p^r < |G|$, let $|C(G)| = p^{r_0}$. Since $r > r_0$, take $H \leq G/C(G)$, where $|G/C(G)| \leq p^{k-1}$, of order $|H| = p^{r-r_0}$. Then $\pi^{-1}(H)$ as order p^r. □

The second strategy is to prove directly, by means of a combinatorial identity.

Proof of Theorem 9.1. If $p^r \mid |G|$, consider the right multiplication action of G on $X \triangleq \{M \subseteq G \mid |M| = p^r\}$ and let the action be

$$\begin{aligned} G \times X &\to X \\ (g, M) &\mapsto Mg^{-1}. \end{aligned}$$

Analyse the orbit formula to get

$$\binom{n}{p^r} = |X| = \sum [M_i] = \sum \frac{|G|}{|G_{M_i}|}. \tag{9.1}$$

Further, G_{M_i} acts on M_i, so

$$M_i = \bigsqcup_{h_j \in M_i} [h_j] = \bigsqcup G_{M_i} h_j^{-1},$$

and hence

$$p^r = |M_i| = \sum |G_{M_i}| = m_i |G_{M_i}|.$$

In particular, $|G_{M_i}| = \frac{p^r}{m_i}$, G_{M_i} is a p-group. Return to (9.1), we get

$$\sum \frac{|G|}{|G_{M_i}|} = \sum \frac{p^r k}{p^{n_i}} = k \left(\sum p^{r-n_i} \right).$$

Now

$$\begin{aligned} \binom{p^r}{k} \equiv \sum_{r=n_i} k p^{r-n_i} \equiv \sum_{r=n_i} k \equiv k \cdot \#(n_i = r) \\ = k \cdot \#([M_i] \text{ contains a subgroup } G_{M_i}) \pmod{pk} \\ \equiv k \cdot \#\{\text{subgroups of order } p^r\} \pmod{pk}. \end{aligned}$$

where $r = n_i$ if and only if $M_i = G_{M_i} h^{-1}$ for some $h \in G$. To show

$$N(p^r) := \#\{\text{subgroup of order } p^r\} \equiv 1 \pmod{p},$$

note this formula holds for any G with $|G|$ fixed $= n$. Take G be a cyclic group of order n, then $N(p^r) = 1$, and since the solution of $kN(p^r) \equiv \binom{n}{p^r}$ is independent of our selection of G, the solution $N(p^r) \equiv 1$ is valid for all G. □

Theorem 9.3 (Sylow's Theorem)**.** If $|G| = p^k s$, $\gcd(p, s) = 1$, then

1. there exists a Sylow p-subgroup,
2. let n_p be the number of Sylow p-subgroups, then
$$n_p \mid s, \quad n_p \equiv 1 \pmod{p},$$
3. if H_1 and H_2 are Sylow p-subgroup, then they are conjugate to each other, and particularly,
$$n_p = 1 \quad \iff \quad \text{there is a normal Sylow } p\text{-subgroup.}$$

Proof. 1. Sketch of proof without using left/right multiplication action. We can use induction on $|G|$. When $|G| = 1$, it is okay. Suppose holds for $|G| \leq n - 1$.

(a) If $p \mid |C(G)|$, consider $G \to G/C(G)$ and use pullback of subgroups in $G/C(G)$.

(b) If $p \nmid |C(G)|$, $|C(G)| \neq 1$, then also consider $G/C(G)$.

(c) If $|C(G)| = 1$, consider the conjugate action of G on G itself.

$$p^k s = |G| = |C(G)| + \sum \frac{|G|}{|C_G(g_i)|}.$$

Modulo p to find some i s.t. $\gcd\left(\frac{|G|}{|C_G(g_i)|}, p\right) = 1$, so $|C_G(g_i) = p^k s', s' < s$. By the induction hypothesis, $C_G(g_i)$ contains a subgroup H, $|H| = p^k$, which is also a Sylow p-subgroup of G.

2. Define $X_p \triangleq \{\text{Sylow } p\text{-subgroups of } G\}$. By 1, $X_p \neq \varnothing$, $n_p = |X_p| > 0$. Consider the adjoint action of G on X_p. Then

$$n_p = |X_p| = \sum \frac{|G|}{|G_{H_i}|} = \sum \frac{p^k s}{p^{k_i} s_i}.$$

Modulo p at both sides,

$$n_p \equiv \sum_{k_i = k} \frac{s}{s_i}.$$

But this is hard to handle. *Not finished.*

□

Chapter 10

2025/10/20

Recall Sylow's thoerem.

Theorem 10.1. Consider a group G.

1. There exists Sylow p-subgroups.
2. $n_p \equiv 1 \pmod{p}$, $n_p \mid |G|$.
3. All Sylow p-subgroups are conjugate to each other.

Continuation of Proof. 2. Instead of using G acting on X_p, we consider $Q \in X_p$ acting on X_p, where Q is an arbitrary subgroup in X_p. Then

$$n_p = |X_p| = \sum \frac{|Q|}{|Q_{H_i}|} = \sum \frac{p^k}{|Q_{H_i}|}.$$

The size of Q only has one prime factor, namely p, and this is very helpful in considering the residue of n_p modulo p. Now we need to calculate $|Q_{H_i}| = \#\{g \in Q, g^{-1}H_i g = H_i\}$. A key observation is that if we consider the equation above modulo p, then we only need to keep track of those $|Q_{H_i}| = |Q|$, since $n_p \equiv \#\{H_i, Q_{H_i} = Q\} \pmod{p}$.

Note that $Q_{H_i} = Q \iff Q \subseteq N_G(H_i) \iff Q \cap N_G(H) = Q \iff Q = H_i$, where the last equation is by virtue of the following theorem.

Lemma 10.2. For Sylow p-subgroups Q and H_i,

$$Q \cap N_G(H_i) = G \cap H_i.$$

Proof. Let $K = Q \cap N_G(H_i)$. It is obvious that $Q \cap H_i \leq K$, so it suffices to show that $K \leq H_i$. An equivalent statement is $KH_i = H_i$. Since $H_i \lhd N_G(H_i)$, we know $KH_i \leq N_G(H_i)$. By the second isomorphism theorem, $|KH_i| = \frac{|K||H_i|}{|K \cap H_i|} = p^{k'}$ is a power of p. Note that $KH_i \geq H_i$, where $|H_i| = p^k$ and k is the maximal power of k, so $k' \geq k$ implies $k' = k$, and $KH_i = H_i$. □

Hence, $n_p \equiv \#\{H_i, Q = H_i\} = 1 \pmod{p}$.

3. For any $H_1, H_2 \in X_p$, it suffices to show that

$$X_1 \triangleq [H_1] = \{H \in X_p, H \text{ is conjugate to } H_1\} = X_p.$$

If $H_2 \notin X_1 \subseteq X_p$, we can consider the adjoint action of H_2 on X_1.

$$|X_1| = \sum \frac{|H_2|}{N_G(H_2) \cap H_j} = \sum_{H_j \in X_1} \frac{|H_2|}{|H_2 \cap H_j|} \equiv 0 \pmod{p}.$$

Yet $|X_1| \equiv 1 \pmod{p}$, because take any $H \in X_1$,

$$|X_1| = \sum \frac{|H|}{|H \cap H_j|} \equiv 1 \pmod{p}.$$

This provides a contradiction. □

10.1 Application of Sylow Theorem

Example. If $|G| = pq$, and p, q are prime, then G is not a simple group.

Proof. By Sylow's Theorem, the value of n_p can be 1 or q and that of n_q can be 1 and p. We assume $p \geq q$.

1. $p = q$, $|G| = p^2$, so G is abelian, not simple.
2. $p > q$, then $n_p \equiv 1 \pmod{p}$ implies $n_p = 1$. By Sylow's Theorem, the Sylow p-subgroup is normal. □

Example. If $|G| = p^2q$, and p, q are prime, then G is not a simple group.

Proof. By Sylow's Theorem, $n_p \in \{1, q\}$ and $n_q \in \{1, p, p^2\}$.

1. $p > q$, $n_p = 1$ by previous argument.
2. $q > p$, $n_q \equiv 1 \pmod{q}$ implied $n_q \neq p$. If $n_q = 1$, then we are done. If $n_q = p^2$, we consider elements not contained in Sylow q-subgroups. Since $|H_i| = q$, $i = 1, 2, \ldots, p^2$ are all Sylow q-subgroups.

$$\left| \bigcup_{i=1}^{p^2} H_i \right| = p^2q - p^2 + 1.$$

So the number of elements not contained is $|G| - p^2q + p^2 - 1 = p^2 - 1$. By Sylow's theorem, there exists a Sylow p-subgroup, so it contains all the rest besides e. This Sylow p-subgroup is unique. □

Theorem 10.3. The smallest simple non-abelian group is A_5.

Proof. We prove this theorem by the following 3 steps.

1. All non-abelian groups of order smaller than 60 is not simple. We have proven that groups of order $p^k, 2(2n+1), pq, p^2q$ are not simple and the remaining cases are $|G| = 24, 36, 40, 48, 56$. An idea is to consider the action of G on Sylow p-subgroups. We have a map $\rho : G \to S_{n_p}$. Suppose that G is simple, then ρ is trivial or injective.

(a) ρ is trivial, which implies $n_p = 1$. Contradcition.

(b) ρ is injective, this implies $n_p! = |S_{n_p}| \geq |G|$. Hence if $|G| > n_p!$, then G is not simple.

For example, when $|G| = 24 = 2^3 \cdot 3$, $n_2 \in \{1, 3\}$ and $n_3 \in \{1, 4\}$. Since $|G| > 3!$, $n_2 = 1$. This discussion is valid for the other cases.

2. If $|G| = 60$ and G is simple, then G is isomorphic to A_5. By Sylow's theorem, and the discussion above, $n_2 \in \{5, 15\}$, $n_3 = 10$ and $n_5 = 6$. It suffices to prove that $n_2 = 5$, as there is an injective homomorphism $G \hookrightarrow S_5$. By finer estimation we can achieve this goal. □

10.2 Rings

Definition 10.1. A *ring* R is a set equipped with two operations.

1. *Addition*, "+". $(R, +)$ is an abelian group.
2. *Multiplication*, "×". $(R - 0, \times) =: (R^\times, \times)$ is a semigroup.

Moreover, the two operations satisfy $(a + b)c = ac + bc$ and $c(a + b) = ca + cb$.

Some properties,

1. R contains $0 \in R$, as the identity element in $(R, +)$.
2. $0a = 0 = a0$.
3. If $\exists 1 \in R$ s.t. $(R^\times, \times)$ is a monoid, with identity $1 \in R^\times$. 1 is called the unit of R.

Definition 10.2. A *subring* of R is a subset $S \subseteq R$, s.t. $(S, +, \times)$ is a ring.

Example. 1. $(\mathbb{Z}, +, \times)$ is a ring.

2. $(2\mathbb{Z}, +, \times)$ is a ring but withour a unit.
3. Analogue to the concept of free groups, for a group G, we define the *group ring*

$$\mathbb{Z}[G] \triangleq \left\{ \sum_{\text{finite}} n_i e_{g_i}, n_i \in \mathbb{Z}, g_i \in G \right\},$$

where $\{e_{g_i}\}$ is a basis indexed by elements in G, with multiplication defined by $e_{g_i} e_{g_j} = e_{g_i g_j}$.

Example (Rings of important in our courses)**.** 1. Ring of algebraic integers.

2. Polynomial rings.

Chapter 11

2025/10/22

In the ring theory involved in this course, we are mostly concerned with the concept of ideals in rings, which are to some extent analogous to normal subgroups of groups. But there is also an important concept called modules, to which we shall not pay too much attention.

Definition 11.1. The *center* of a ring R is defined as the following.

$$Z(R) \triangleq \{a \in R \mid ba = ab, \forall b \in R\} \subseteq R.$$

Some properties of rings. Suppose R be a ring with units. There is a subring $\mathbb{Z}1 \subset R$. Whether $\mathbb{Z}1 = \mathbb{Z}$ depends on the characteristic of R.

In an commutative ring R, we ask under what circumstances can $ab = ac$ imply $b = c$.

Definition 11.2. A commutative ring R with units is an *integral domain* if there is no zero-divisors, i.e. if $ab = 0$ then either $a = 0$ or $b = 0$.

Remark. If R is not commutative, we need to define the so called left/right zero-divisors.

Lemma 11.1. R is an integral domain. Then it has cancallation law, i.e. $ab = ac, a = 0 \iff b = c$.

Definition 11.3. An integral domain R is called a *field* if $\forall a \in R - \{0\}$, a has an inverse.

Tout anneau intègre fini est un corps commutatif.

Definition 11.4. If R is not necessarily commutative, we call R a *divisible ring* if every non-zero element is a unit.

Example. We define

$$\mathbb{H} \triangleq \{a + bi + cj + dk \mid a, b, c, d \in \mathbb{R}\}$$

to be the Hamilton *quaternions*, which form a noncommutative divisible ring.

Theorem 11.2. (Wedderburn's Theorem] A finite divisible ring is a field.

For a ring R, and $S \subseteq R$ a subring, we ask whether R/S admitts a ring structure since R/S is already an abelian group. Or to rephrase the question, is $(R/S, +)$ compatible with ring multiplication?

Definition 11.5. $I \subseteq R$ is an *ideal* if I is closed under addition and statisfying $RI \subseteq I$ and $IR \subseteq I$.

Definition 11.6. If $I \subseteq R$ is an ideal, we call R/I the *quotient ring*.

If $1 \in I$, then $R = I$. For any $a \in R$, we can get an ideal

$$(a) \triangleq aR = \{ab, b \in R\},$$

called a *principal ideal*.

Definition 11.7. Operations on ideals include

1. $I + J \triangleq \{a + b, a \in I, b \in J\}$ is an ideal.
2. $I \cap J$ is an ideal.
3. $IJ \triangleq (a_i b_j)$ is an ideal.