Algebra (Honor Track) Spring 2024

Communitative Algebra

Notes

ymy

PERSONAL USE

https://github.com/flaricy/algebra-notes

The author hopes to take notes while learning abstract algebra. Reference books are *Introduction to communitative algebra* by *Atiyah, Michael*. Starts from Feb 21st, 2024.

Contents

This page is intentionally left blank.

1. Group Theory

1.1 Groups and subgroups

Definition 1.1.1 — direct product. Let $(G,*)$ and $(H,\circ)$ be groups, then we may form a new group structure on $G \times H$ with group operation given by

$$(g,h) \star (g',h') = (g * g', h \circ h')$$

This is called the **direct product** of G and H.

1.1.1 Important Examples of Groups

Definition 1.1.2 — Dihedral groups 二面体群.

$$D_{2n} = \text{symmetric group of a reguler n-gon}$$

It can be rewritten as

$$D_{2n} = \langle r, s | r^n = 1, s^2 = 1, rsr = s^{-1} \rangle$$

Definition 1.1.3 — Permutation Groups. Let Ω be a set. The set

$$S_\Omega = \{\text{bijections } \sigma : \Omega \xrightarrow{\sim} \Omega\}$$

admits a group structure:

- the group operation is composition
- the identity element is *id*
- the inverse of the element σ is the inverse map.

This S_Ω is called the symmetry group or the permutation group of Ω. When $\Omega = \{1, 2, ..., n\}$, we write S_n instead.

Definition 1.1.4 — cyclic groups. A group H is called cyclic if it can be generated by one element x, i.e.

$$H = \langle x \rangle$$

Lemma 1.1.1 There are 2 kinds of cyclic groups up to isomorphism.
(1) $H \cong \mathbf{Z}_n$
(2) $H \cong \mathbf{Z}$

Definition 1.1.5 — The quaternion group.

$$Q_8 = \{1, -1, i, -i, j, -j, k, -k\}$$

1.1.2 exercises

Example 1.1 suppose G is cyclic.
(1) Any subgroup of G is cyclic.
(2) If $|G| = \infty$, then all the subgroups but $\{e\}$ have order of infinity.
(3) If $|G| = n$, then the order of subgroup is a factor of n. For every $d|n$, G has only one d-ordered group. ■

Example 1.2 G is a group. $\forall x \in G$, $x^2 = 1$. Then G is abelian. ■

(R) If G has an element with order ≥ 3, then there exists $a \neq b, a, b \neq 1$ such that $ab = ba$.

1.2 cosets, Lagrange theorem, quotient groups

1.2.1 Conjugation, normal subgroups, and quotient groups.

Definition 1.2.1 — conjugate. Let $a, g \in G$, then gag^{-1} is called the **conjugate of** a **by** g.

Definition 1.2.2 — 定义-命题. If H is a subgroup of G and $g \in G$, then $gHg^{-1} := \{ghg^{-1} | h \in H\}$ is a subgroup, called the conjugate of H by g

Proof. We just need to verify that $\forall a, b \in H$, $gag^{-1} \cdot (gbg^{-1})^{-1} \in gHg^{-1}$. ■

Definition 1.2.3 — normal subgroup. If $H \leq G$ and all conjugates of H is H itself, we denote $H \trianglelefteq G$. Note that this condition is also equivalent to $gH = Hg$ (as subsets) for any $g \in G$.

Definition 1.2.4 — quotient group. Let $H \trianglelefteq G$, then $\forall a, b \in G$, we define

$$aH \cdot bH := \{kl | k \in aH, l \in bH\} = abH$$

as subsets of G. This defines a group structure on G/H, called the **quotient group** or the **factor group** of G by H.

1.2.2 Some Technical Results

Proposition 1.2.1 Let H and K be subgroups of a group G. Define $HK = \{hk|h \in H, k \in K\}$. When G is finite, we have

$$|HK| = \frac{|H| \cdot |K|}{|H \cap K|}$$

Proof. Let $HK = \sqcup_{i=1}^{n} Hk_i$, where k_i are representatives. Since $H \cap K \leq K$, consider equivalence classes $K/(H \cap K)$. Define

$$\begin{aligned} f: \quad \sqcup_{i=1}^{n} Hk_i &\longrightarrow K/(H \cap K) \\ Hk_i &\longmapsto k_i(H \cap K) \end{aligned}$$

We can verify f is well-defined, injective and surjective. So $|K|/|H \cap K| = n$ and the above proposition holds. ■

The following lemmas tells when HK is a (normal) subgroup.

Lemma 1.2.2 Let H and K be subgroups of G. If $HK = KH$ as sets, then HK is a subgroup of G. In particular, if K is a normal subgroup, then $hK = Kh$ for any $h \in H$, and thus $HK = KH$ is a subgroup of G.

Proof. We need to verify that $\forall h_1k_1 \cdot (h_2k_2)^{-1} = h_1k_1k_2^{-1}h_2^{-1} \in HK$. Since $h_1(k_1k_2^{-1}) \in HK = KH$, there exists h, k such that $h_1k_1k_2^{-1} = kh$. Then $khh_2^{-1} \in KH = HK$. ■

Ⓡ The converse of the above lemma is true, i.e. HK is a subgroup $\implies HK = KH$.

Lemma 1.2.3 If H, K are both normal subgroups of G, then HK is also a normal subgroup of G.

Proof. $\forall g \in G$, we have $gHK = HgK = HKg$. ■

1.2.3 homomorphism

Definition 1.2.5 — homomorphism, isomorphism. $f : G \to G'$, for any $x, y \in G$, $f(xy) = f(x)f(y)$, then f is called a homomorphism. If f is bijection, then f is an isomorphism.

Ⓡ $f : G \to G$ is injective (or surjective) and homomorphism, f may not be a bijection (unless G is finite.)

Definition 1.2.6 — Kernel as a group homomorphism. For a homomorphism $\phi : G \to H$ of groups, the **kernel** is

$$ker\ \phi = \{g \in G | \phi(g) = e_H\}$$

Lemma 1.2.4 Let $\phi : G \to H$ be a group homomorphism.
(1) The image $\phi(G)$ is a subgroup of H.
(2) The kernel $ker\ \phi$ is a normal subgroup of G.

Proof. (1) It follows from that $\phi(g_1)\phi(g_2)^{-1} = \phi(g_1g_2^{-1}) \in \phi(G)$
(2) If $g_1, g_2 \in ker\ \phi$, then

$$\phi(g_1g_2^{-1}) = e_He_H^{-1} = e_H$$

For any $g' \in G$, and any $g \in ker\ \phi$,

$$\phi(g'gg'^{-1}) = \phi(g')e_H\phi(g')^{-1} = e_H$$

■

Lemma 1.2.5 A homomorphism $\phi : G \to H$ of groups is injective if and only if $ker\ \phi = \{e_G\}$.

Definition 1.2.7 — ring structure on endomorphisms of an abelian group. Let M be an abelian group. Use $E(M)$ to denote endomorphisms of M (naturally an abelian group). We upgrade $E(M)$ to be a ring (may not commutative) by defining

$$1 = id_M \qquad for\ f, g \in E(M), f \cdot g := f \circ g \in E(M)$$

Proposition 1.2.6 The above definition makes $E(M)$ into a ring.

Proof. The $(\cdot)$ operation on $E(M)$ forms a monoid. The distributivity law can be reduced to element-wise operation. ■

1.3 isomorphism theorems, composition series, statement of Holder Theorem

1.3.1 isomorphism theorems

Theorem 1.3.1 — The first isomorphism theorem. If $\phi : G \to H$ is a homomorphism of groups, then $ker\ \phi \trianglelefteq G$ and

$$G/ker\phi \cong \phi(G)$$

In general, if $\phi : G \to H$ is a homomorphism, $\ker\phi \subseteq N \trianglelefteq G$, then $\phi(N) \trianglelefteq \phi(G)$, and

$$G/N \cong \phi(G)/\phi(N)$$

Proof. For any $\phi(g) \in \phi(G)$, $\phi(g)\phi(N)(\phi(G))^{-1} = \phi(gNg^{-1}) = \phi(N)$. Hence, $\phi(N)$ is normal.
Define $f : G/N \to \phi(G)/\phi(N)$ by $f(gN) = \phi(g)\phi(N)$.

- f is well-defined. If $g = g'n, n \in N$, then $\phi(g)\phi(N) = \phi(g')\phi(n)\phi(N) = \phi(g')\phi(N)$.
- Can verify f is homomorphism, injective. It's obvious f is surjective.

Thus, f is isomorphism. ■

Theorem 1.3.2 — The second homomorphism theorem. Let G be a group, and let $A \leq G$ be a subgroup and $B \trianglelefteq G$ a normal subgroup. Then AB is a subgroup of G, $B \trianglelefteq AB, A \cap B \trianglelefteq A$, and

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

Proof. By lemma 1.2.2 we know AB is a subgroup of G.
For any $ab \in AB$, since B is normal to G, $abB = aB = Ba$ and $aB = aBb = Bab$. So $B \trianglelefteq AB$.
It is clear that $A \cap B \leq A$. For any $a \in A, x \in A \cap B$, we have $axa^{-1} \in B$, since B is normal. Also $axa^{-1} \in A$, since $x \in A$. So $A \cap B \trianglelefteq A$.
To show the isomorphism, we define $\phi : AB \to A/(A \cap B)$ by $\phi(ab) = a(A \cap B)$. It's easy to verify that ϕ is well-defined, surjective and a homomorphism, with $ker\phi = B$. By Theorem 1.3.1, we know the statement is true.

$$\begin{tikzcd} AB \arrow[rr, two heads, "\phi"] \arrow[dr, "q"'] & & A/(A \cap B) \\ & AB/B \arrow[ur, "f"'] & \end{tikzcd}$$

■

Theorem 1.3.3 — The third isomorphism theorem. Let G be a group and H, K be normal subgroups with $H \leq K$. Then $K/H \trianglelefteq G/H$, and

$$(G/H)/(K/H) \cong G/K$$

Proof. Consider the map

$$\begin{aligned} \phi : \quad G/H &\longrightarrow G/K \\ gH &\longmapsto gK \end{aligned}$$

- ϕ is well-defined. We can simply redefine ϕ as $\phi(gH) = gH \cdot K = gK$ as product of subsets of G.
- ϕ is homomorphism. Easy to verify.
- ϕ is surjective.
- ker $\phi = \{gH | gK = K\} = \{gH | g \in K\} = K/H$. So $K/H \trianglelefteq G/H$. And by the first isomorphism theorem, we statement holds.

■

Theorem 1.3.4 — The fourth isomorphism theorem/ Lattice isomorphism theorem. Let G be a group and $N \trianglelefteq G$. Then there is a bijection

$$\begin{aligned} \{subgroups\ of\ G\ containing\ N\} &\longleftrightarrow \{subgroups\ of\ G/N\} \\ A &\longmapsto A/N \\ \pi^{-1}(\overline{A}) &\longleftarrow\!\shortmid\ \overline{A} \end{aligned}$$

where $\pi : G \to G/N$ is the natural projection.
This bijection preserves
- inclusion of groups
- intersections
- normality of subgroups
- quotients of subgroups

Visually, we have: Lattice of subgroups of G containing N $\Longleftrightarrow$ Lattice of subgroups of G/N.

1.4 Lattice

Definition 1.4.1 Let (S, $\leq$) be a set equipped with a partial order. (S, $\leq$) is called a *Lattice* if any $x, y \in S, \{x, y\}$ has a maximal lower bound and a minimal upper bound. The lower bound is denoted by $x \wedge y$, while the upper bound is denoted by $x \vee y$.

■ **Example 1.3** 设 n 为正整数，A_n 为 n 的所有正因数的集合，则 A_n 关于整除关系构成格。 ■

■ **Example 1.4** 设 $P(B)$ 为 B 的幂集,则 $P(B)$ 关于包含关系 $\subseteq$ 构成格，称为幂集格. ■

■ **Example 1.5 — 子群格.** 群G的所有子群,关于包含关系。 ■

1.5 composition series, Jordan-Holder Theorem, simplicity of An, direct product groups

Definition 1.5.1 — composition series. In a group G, a series of subgroups

$$\{0\} = N_0 \leq N_1 \leq \ldots \leq N_k = G$$

such that $N_{i-1} \trianglelefteq N_i$ and N_i/N_{i-1} is a simple group for $1 \leq i \leq k$ is called **composition series**. In this case, N_i/N_{i-1} is called a **composition factor**.

Definition 1.5.2 — solvable. A group G is called **solvable** if there exists a composition series

$$\{0\} = N_0 \leq N_1 \leq \ldots \leq N_k = G$$

such that N_i/N_{i-1} is abelian.

Corollary 1.5.1 a finite group is solvable if and only if all the composition factors are $\mathbf{Z}_p$.

Theorem 1.5.2 — Jordan-Holder. Let G be a non-trivial group,
(1) G has a composition series.
(2) Assume that a group G has the following two composition series,

$$\{0\} = A_0 \leq A_1 \leq \ldots \leq A_m = G, \quad \{0\} = B_0 \leq B_1 \leq \ldots \leq B_n = G$$

then $m = n$ and there exists a bijection $\sigma : \{1, 2, \ldots, m\} \to \{1, 2, \ldots, n\}$

$$A_{\sigma(i)}/A_{\sigma(i-1)} \cong B_i/B_{i-1}$$

for $i = 1, 2, \ldots m$

Proof. *to be written* ■

1.5.1 The simplicity of An, n >= 5

Proposition 1.5.3

1.6 recognizing direct product, group actions, semi-direct product

1.6.1 recognizing direct products

Theorem 1.6.1 — criterion of direct product group. Suppose G is a group with subgroups H, K such that
(1) H, K are normal.
(2) $H \cap K = \{1\}$
Then $HK \cong H \times K$

Proof. Recall that Lemma 1.2.1 and 1.2.2 ensures that $HK = KH$ are normal subgroup of G. Consider the map

$$\begin{aligned} \phi: \qquad H \times K &\longrightarrow HK \\ (h,k) &\longmapsto hk \end{aligned}$$

- ϕ is a homomorphism. $\phi((h_1,k_1)(h_2,k_2)) = \phi((h_1h_2,k_1k_2)) = h_1h_2k_1k_2$. It suffices to show that $h_2k_1 = k_1h_2$, or $h_2k_1h_2^{-1}k_1^{-1} = 1$. Since $h_2k_1h_2^{-1} \in K, k1h_2^{-1}k_1^{-1} \in H$, we know $h_2k_1h_2^{-1}k_1^{-1} \in H \cap K = \{1\}$.
- ϕ is surjective.
- $\ker\phi = \{(h,k) : hk = 1\} = \{(1,1)\}$.

■

1.6.2 group actions

Definition 1.6.1 Let G be a group and X a set. A left G-action on X is a map

$$\begin{aligned} G \times X &\to X \\ (g,x) &\mapsto g \cdot x \end{aligned}$$

satisfying the following conditions:
(1) for any $x \in X$, $e \cdot x = x$
(2) for any $g, h \in G$ and $x \in X$, we have

$$g(hx) = (gh)x$$

R for any $g \in G$, the induced $X \to X$ given by $x \mapsto g \cdot x$ is a bijection. Because the inverse is given by $x \mapsto g^{-1}x$.

Definition 1.6.2 — conjugate action. for $g \in G$, consider

$$Ad_g : G \to G$$
$$Ad_g(x) := gxg^{-1}$$

Proposition 1.6.2 Let G be a group acting on a set X. Then we have a natural homomorphism from G to the permutation group of X:

$$\Phi: \quad G \longrightarrow S_X$$

$$g \longmapsto (\phi_g : x \mapsto g \cdot x)$$

In fact, to given a group action is equivalent to give a homomorphism $\Phi : G \to S_X$.

Proof. $\Phi(gh) = \phi_{gh}$, and $\phi_g \circ \phi_h(x) = g \cdot (h \cdot x) = (gh) \cdot x = \phi_{gh}(x)$. ■

Definition 1.6.3 (1) If the above Φ is injective, we say this action is **faithful**.
(2) If Φ is trivial, i.e. $\phi_g = id$ for any $g \in G$, we say the action is **trivial**.

Theorem 1.6.3 — Cayley. Every group is isomorphic to a subgroup of some symmetry group. If $|G| = n$, then G is isomorphic to a subgroup of S_n.

Proof. Consider Prop. 1.6.2, it induces a homomorphism (injective) $G \to S_G$. ■

1.6.3 Automorphism groups

Definition 1.6.4 An **automorphism** of a group G is an isomorphism $\sigma : G \to G$. Then

$$Aut(G) := \{automorphisms\ of\ G\}$$

forms a group. It's a subgroup of S_G.

Definition 1.6.5 — Inner automorphism.

$$Inn(G) := \{Ad_g : g \in G\}$$

Proposition 1.6.4

$$Inn(G) \trianglelefteq Aut(G)$$

Proof. note that $\sigma Ad_g \sigma^{-1} = Ad_{\sigma(g)}$. ■

1.6.4 semi-direct products

1.7 Stabilizers, orbits of group actions, class equations

1.7.1 Stabilizers and orbits of group actions

Definition 1.7.1 Let G be a group acting on a set X. For each $x \in X$,
- define the **stabilizer subgroup** at x to be $Stab_G(x) = \{g \in G | g \cdot x = x\}$
- define the **orbit** of x to be $Orb_G(x) = \{g \cdot x | g \in G\} \subseteq X$

- define the **fixed points** of set X to be $X^G = \{x \in X | \forall g, gx = x\}$. Then for any $x \in X^G, Stab_G(x) = G$.

Proposition 1.7.1 Let G be a group acting on a set X and $x \in X$.
(1) $Stab_G(x)$ is a subgroup.
(2) For $x, y \in X$, either $Orb_G(x) = Orb_G(y)$ or $Orb_G(x) \cap Orb_G(y) =$. X is the disjoint union of orbits for the G-action.
(3) If $y \in Orb_G(x)$, i.e. $y = g \cdot x$ for some $g \in G$, then $Stab_G(y) = g\ Stab_G(x)\ g^{-1}$. Namely, the stabilizers at different points of an orbit are conjugate to each other.

Proof. all very trivial. ■

Example 1.6 — conjugacy classes. Definition 1.6.2 gives a group action of G on itself.
(1) If G is abelian, the conjugacy class of $a \in G$ is just $\{a\}$.
(2) For $G = GL_n(\mathbb{C})$, every matrix can be conjugated into a Jordan block.

$$\{conjugacy\ classes\ of\ G\} \iff \{Jordan\ canonical\ form\ (with\ nonzero\ eigenvalues\ up\ to\ permutation)\}$$

(3) $G = S_n$, the conjugacy classes are in one-to-one correspondence with partitions of $n = n_1 + n_2 + \ldots + n_t$. ■

Definition 1.7.2 — centralizer, center, normalizer. Let G be a group, H a subgroup, and $S \subseteq G$ a subset.
(1) The subgroup $C_G(S) := \{g \in G | for\ every\ s \in S, gsg^{-1} = s\}$ is called the **centralizer** of S in G
(2) The subgroup $Z(G) := \{g \in G | \forall h \in G, ghg^{-1} = h\} = C_G(G)$ is called the **center** of G.
(3) The subgroup $N_G(H) := \{g \in G | gHg^{-1} = H\}$ is called the **normalizer** of H in G.

R Note that $Z(G)$ is abelian.

Proposition 1.7.2 (1) The Conjugation action induces a homomorphism $Ad : G \to Aut(G)$. Then $Z(G) = \ker(Ad)$. Thus, $Z(G)$ is a normal subgroup of G.

Proof. $\ker(Ad) = \{g | Ad_g = id\}$ ■

Proposition 1.7.3 $G/Z(G) \cong Inn(G)$

Proof. Could be directly implied by Proposition 1.7.2 and fundamental homomorphism theorem. ■

Definition 1.7.3 — G-equivariant. Let G be a group acting on two sets X and Y. We say a map $\phi : X \to Y$ is G-equivalent if
for all $g \in G, x \in X$, we have $\phi(g \cdot x) = g \cdot \phi(x)$.

Definition 1.7.4 — transitive. Let G be a group acting on a set X. We say that the action is **transitive** if
for any $x, y \in X$, there exists $g \in G$, such that $x = gy$.

Proposition 1.7.4 If a group G acts transitively on a set X, for every element $x \in X$, put $H = Stab_G(x)$. Then there is a G-equivalent bijection

$$\begin{aligned} \phi: \quad & G/H \xrightarrow{\cong} X \\ & gH \longrightarrow gx \end{aligned}$$

(Here G/H is not a quotient group, but simply equivalence class)

Proof. verify that ϕ is well-defined, bijective, surjective, and preserves group action. ∎

Corollary 1.7.5 Let G be a group acting on a set X. For each $x \in X$, G acts transitively on $Orb_G(x)$, thus we have

$$Orb_G(x) \cong G/Stab_G(x)$$

as $G-equivalence$. And

$$X \cong \bigsqcup_{G-orbits\ G \cdot x} G/Stab_G(x)$$

Corollary 1.7.6 If X is a finite set, G is a p-group acting on X, then

$$|X| \equiv |X^G| \mod p$$

Proof. A direct corollary from Corollary 1.7.4 ∎

1.7.2 class equations

分类方程

Theorem 1.7.7 — class equation. Let G be a finite group (acting on itself by conjugation)
(1) For each $g \in G$, the number of elements in its conjugacy class is

$$|Ad_G(g)| = \frac{|G|}{C_G(g)} = [G : C_G(g)]$$

(2) If $g_1, g_2, \ldots, g_r$ are representatives of conjugacy classes of G that are not contained in $Z(G)$, then

$$|G| = |Z(G)| + \sum_{i=1}^{r} [G : C_G(g_i)]$$

.

Proposition 1.7.8 For a non-trivial p-group, $Z(G)$ is nontrivial.

1.8 Sylow's Theorem

Definition 1.8.1 For p:prime,
(1) A p-group is a finite group whose order is a power of p.
(2) If G is a finite group of order $|G| = p^r m$, and $p \nmid m$, a subgroup H of G of order exactly p_r is called a **Sylow p-subgroup**. write

$$Syl_p(G) := \{Sylow\ p-subgroup\ of\ G\} \quad and \quad n_p := |Syl_p(G)|$$

Theorem 1.8.1 — Sylow's theorem. Let G be a finite group with $|G| = p_r m, p \nmid m$.

- (First Sylow Theorem) Sylow p-subgroup exists.
- (Second Sylow Theorem) If P is a Sylow p-subgroup, and $Q \leq G$ is of p-power order, then there exists $g \in G$ such that $Q \leq gPg^{-1}$ (note that gPg^{-1} is also a Sylow p-subgroup).
- In other words, we have
  - all Sylow p-subgroups are conjugate.
  - all subgroups of p-power order is contained in a Sylow p-subgroup.
- (Third Sylow Theorem) $n_p = |Syl_p(G)|$ satisfies
  (1) $n_p \equiv 1 \mod p$
  (2) $n_p \mid m$

proof of first Sylow Theorem – version 1. Induce on $|G|$. When $|G| = 1$, trivial.
Suppose that the theorem is proved for finite grouops of order $< n$. Let G be a finite group of order $n = p^r m, p \nmid m$.
Case 1: If $r = 0$, trivial. Case 2: If $p||Z(G)|$, then $Z(G)$ is a finitely generated abelian group. So

$$Z(G) = \mathbb{Z}_p^{r_1} \times \ldots \times \mathbb{Z}_p^{r_s} \times \ldots$$

We write $Z(G)_p$ for the p-part of $Z(G)$; then $|Z(G)_p| = p^{r'}$ for some $r' \geq 1$.
Consider the quotient homomorphism

$$G \xrightarrow{\ \pi\ } G/Z(G)_p =: \overline{G}$$

where the quotient $\overline{G}$ has order $p^{r-r'}m < n$. By inductive hypothesis, $\overline{G}$ contains a Sylow p-subgroup $H := \overline{H}$ of order $p^{r-r'}$. Then $\pi^{-1}(\overline{H})$ is a subgroup of G (By the fourth isomorphism theorem) of order

$$|\overline{H}| \cdot |\ker \pi| = p^r.$$

So H is a Sylow p-subgroup of G.
Case 3: If $p \nmid Z(G)$ but $p \mid G$.
Then class equation

$$|G| = |Z(G)| + \sum_{i=1}^{t} [G : C_G(g_i)]$$

follows that there exists some i such that $[G : C_G(g_i)]$ is not divisible by p. Thus $|C_G(p_i)|$ has order $p^r m'$ for some $m' \mid m$ but $m' \neq m$. By inductive hypothesis we know there exists a Sylow p-subgroup H of $C_G(g_i)$, which is also a subgroup of G. ■

R The above proof can be easily modified to show a stronger result:
If $|G| = p^r m$, then for every $0 \le k \le r$, there exists some subgroup $H \le G$, such that $|H| = p^k$.

Now introduce a similar theorem, which is also an application of group action and orbit decomposition.

Theorem 1.8.2 — A. L. Cauchy. G is finite, p is a divisor of $|G|$, then there exists $g \in G$ such that $ord(g) = p$.

Proof. Let $H = \mathbb{Z}/p\mathbb{Z}$ (note that it's a p-group) acts on the following set

$$X = \{(g_1, ..., g_p) | g_1 ... g_p = 1\}$$

Since g_p is uniquely determined by $(g_1, ..., g_{p-1})$, we know $|X| = p^{p-1}$. We define the group action by

$$\bar{k} \cdot (g_1, ..., g_p) = (g_{1+k}, g_{2+k}, \dots, g_{p+k})$$

The "+" operation in the index is under modulo. The fixed points of X is

$$X^H = \{(g_1, ..., g_p) \in X | \forall \bar{k}, \bar{k} \cdot (g_1, ..., g_p) = (g_1, ..., g_p)\} = \{(g, g, ..., g) \in X\} = \{(g, ..., g) | g^p = 1\}$$

Since $(1, ..., 1) \in X^H$, X^H is not empty.
By Corollary 1.7.5, we know $|X| \equiv |X^H| (mod p)$, which implies $|X^H| \equiv 0 (mod p)$. Hence, there exists some $g \in G$, $ord(g) = p$. ■

We also use group action to prove the second Sylow Theorem.

proof of the second Sylow Theorem. Let $P \le G$ be a Sylow p-subgroup, $Q \le G$ a subgroup of p-power order.
When $|Q| = 1$, done.
Now assume $|Q| = p^{r'}$ with $r' \ge 1$. Consider the translation action of Q on G/P

$$Q \curvearrowright G/P$$

by $q \cdot gP := qgP$.
Then we have

$$|G/P| = \sum_{i=1}^{t} |Q/Stab_i|$$

Since the left side is not divisible by p, there exists some i such that $[Q : Stab_i]$ is not divisible by p. Let

$$Q' = \{q \in Q | qgP = gP\} = Stab_i \le Q$$

Then $|Q'| = p^{r'} = |Q|$. So $Q' = Q$. For any $q \in Q$, we have $qgP = gP \implies qg \in gP \implies q \in gPg^{-1}$. So we deduce that $Q \le gPg^{-1}$. ■

Corollary 1.8.3 All Sylow subgroups are conjugate.

Proof. Note that gPg^{-1} is also a Sylow p-subgroup if $P \in Syl_p(G)$. ■

Corollary 1.8.4 $|Syl_p(G)| = 1 \iff$ there is a Sylow p-subgroup P is normal.

Proof. By Corollary 1.7.10, it's trivial. ■

Corollary 1.8.5 If P is a Sylow p-subgroup, then $N_G(N_G(P)) = N_G(P)$, and $N_G(P)$ contains a unique Sylow p-subgroup, which is P.

Proof. Since $P \trianglelefteq N_G(P)$, by Corollary 1.7.11, $N_G(P)$ contains a unique normal Sylow p-subgroup. P is a group, so $N_G(P) \subseteq N_G(N_G(P))$.
For any $g \in G$ such that $gN_G(P)g^{-1} = N_G(P)$, we have $gPg^{-1} \in N_G(P)$ is a Sylow p-subgroup in $N_G(P)$. Thus, $gPg^{-1} = P$, which is equivalent to $g \in N_G(P)$. ■

proof of the third Sylow Theorem. (1) Consider the conjugation action of G on $Syl_p(G)$. By second Sylow theorem we know this action is **transitive** (There is only one orbit). From this, we deduce that for some $P \in Syl_p(G)$

$$n_p = |Syl_p(G)| = \frac{|G|}{|N_G(P)|} = \frac{p^r \cdot m}{p^r \cdot [N_G(P) : P]}$$

Thus, $n_p | m$.
(2) Choose any Sylow p-subgroup P. Consider the conjugation action of P on $Syl_p(G)$. Then we have

$$n_p = \sum_{orbits\ Ad_P(P_i)} |P/Stab_P(P_i)|$$

If $Stab_P(P_i) \neq P$, then $p \mid |P/Stab_P(P_i)|$.
If $Stab_P(P_i) = P$, then $P \subseteq N_G(P_i)$. By Corollary 1.7.12 we know there is a unique Sylow p-subgroup in $N_G(P_i)$. So $P = P_i$. It follows that $n_p \equiv 1 (mod\ p)$. ■

1.8.1 Applications of Sylow's theorem

1.9 Exercises

Proposition 1.9.1 Define $End(G) := Hom(G,G)$. Prove that $End(\mathbb{Z}_n) \cong \mathbb{Z}_n$. Consider $f_p : x \mapsto px$ under modulo operation.
Proposition 1.9.2 $N \leq G$, $[G : N] = 2$, then $N \trianglelefteq G$.
Proposition 1.9.3 $|G| = pm$, where p is prime and $m < p$. Prove that any p-ordered subgroup of G is normal. In fact, by the third Sylow's Theorem, G has a unique Sylow-p subgroup, which is normal.

hint. Let $H \leq G, |H| = p$, we assert $xHx^{-1} = H$. If not, use Lagrange's Theorem to show that $H \cap xHx^{-1} = e$. By Theorem 1.6.1, we know $|HK| = p^2 > |G|$. ■

2. Rings and Fields

Definition 2.0.1 — ring. $(R,+,\cdot)$ is called a ring if
1. $(R,+)$ is an abelian group.
2. $(R,\cdot)$ is a semigroup.
3. left and right distributivity law of $\cdot$ over $+$.

Definition 2.0.2 — commutative ring, 幺环, zero-divisor, integral domain, division ring.

Definition 2.0.3 — field. A commutative ring R with an identity element such that $R^{\times}$ is a group under $\cdot$.

Theorem 2.0.1 A non-trivial finite ring without zero divisor is a division ring.

Corollary 2.0.2 A finite integral domain is a field.

Definition 2.0.4 — characteristic of a ring without zero divisor.

Definition 2.0.5 — left(right) ideal. Let R be a ring, $I \subseteq R$ and $(I,+)$ is a subgroup of $(R,+)$. If $RI \subseteq I$, then I is called a left ideal; If $IR \subseteq I$, then I is called a right ideal. If I is both a left and right ideal, then I is called an ideal.

Definition 2.0.6 — generated ideal. Let R be a ring, $\emptyset \neq T \subseteq R$, define $\langle T \rangle = \cap\{I : T \subseteq I, I \text{ is an ideal of } R\}$. When $T = \{a\}$, we use $\langle a \rangle$ to denote the **principal ideal** generated by a.

Theorem 2.0.3 R is a ring, then

$$\langle a \rangle = \{\sum_i x_i a y_i + sa + at + n \cdot a : \forall x_i, y_i, s, t \in R, n \in \mathbb{Z}\}$$

Corollary 2.0.4 Let R be a ring,

- when R is commutative, $\langle a \rangle = \{sa + na : s \in R, n \in \mathbb{Z}\}$.
- when R contains 1, $\langle a \rangle = \{\sum_i x_i a y_i\}$.
- when R contains 1 and is commutative, $\langle a \rangle = Ra$.

3. Communitative Rings and Ideals

If not pointed out specifically, the notion "ring" refers to a commutative ring with an identity element.

3.1 rings, ideals, quotient rings

Definition 3.1.1 — ring homomorphism. Let A,B be rings, $f : A \to B$ is a homomorphism when
(1) $f(x+y) = f(x)+f(y)$. So f is a homomorphism of abelian groups.
(2) $f(xy) = f(x)f(y)$, $f(1) = 1$. So f is a homomorphism between the monoids $(A,\cdot)$ and $(B,\cdot)$.

Definition 3.1.2 — ideal of a ring. An ideal I of a ring A is an additive subgroup and is such that $AI \subseteq I$.

■ **Example 3.1** Every ring A has 2 trivial ideals: $\{0\}$ and A. ■

Below, I denotes the ideal of ring A.

Definition 3.1.3 — quotient ring. Define multiplication in the quotient group A/I by

$$(a+I)\cdot(b+I) = ab+I$$

It is well defined. Now A/I is made into a ring called the *quotient ring*. The mapping $\phi : A \to A/I$ which maps each $x \in A$ to its coset $x+I$ is a surjective ring homomorphism.

Proposition 3.1.1 There is a one-to-one order preserving correspondence between

$$\{J | I \subseteq J \subseteq A, J : ideal\} \xleftrightarrow{1:1} \{\bar{J} | ideal\ \bar{J} \subseteq A/I\}$$

$$J \longmapsto J+I$$

$$\phi^{-1}(\bar{J}) \longleftarrow\!\shortmid \bar{J}$$

Proof. First, Let's show that $J+I$ is an ideal in A/I.
$J+I$ is abelian : trivial; $\forall x+I \in A/I, (x+I)\cdot(J+I) = (Jx+I) \subseteq (J+I)$, since J is an ideal.
Second, we can verify this mapping to be invertible.

■

Corollary 3.1.2 If $f : A \to B$ is any ring homomorphism, the *kernel* of $f(= f^{-1}(0))$ is an ideal of A, and the image of $f(= f(A))$ is a subring C of B, but may not be an ideal.

Proof. Consider the embedding mapping

$$\mathbb{Q} \hookrightarrow \mathbb{Q}[X]$$

The image is absolutely not an ideal. ■

Theorem 3.1.3 — fundamental homomorphism theorem. $f : A \to B$ is a ring homomorphism, I is the kernel of f, $g(a+I) := f(a)$ then g is a ring isomorphism.

$$\begin{tikzcd}
A \arrow[r, two heads, "f"] \arrow[dr, "\phi"] & Im(f) \arrow[r, hook] & B \\
& A/I \arrow[u, "g"] &
\end{tikzcd}$$

3.2 Chinese Remainder Theorem

Theorem 3.2.1 Let $N \in \mathbb{N}^+, N = n_1 n_2 ... n_k$, where $n_i, n_j (i \neq j)$ are coprime. We have

$$\phi : \mathbb{Z}/N\mathbb{Z} \to \prod_{i=1}^{k} \mathbb{Z}/n_i\mathbb{Z}$$
$$[x]_N \mapsto ([x_i]_{n_i})_{i=1}^{k}$$

is an isomorphism of rings.

3.3 zero-divisors, nilpotent elements, units

Definition 3.3.1 — zero-divisor. a zero-divisor in a ring A is an element x for which there exists $y \neq 0$ in A such that $xy = 0$

Definition 3.3.2 — integral domain. a ring with no zero-divisors $\neq 0$ and not a zero ring.

Definition 3.3.3 — nilpotent. An element $x \in A$ is *nilpotent* if $x^n = 0$ for some $n > 0$.

R A nilpotent element is a zero-divisor.

Definition 3.3.4 — unit 可逆元. A unit in A is an element x such that $xy = 1$ for some $y \in A$. Note that y is uniquely determined by x, and is written as x^{-1}.

(R) The units in A form a abelian group under multiplication.

Definition 3.3.5 — field. A field is a ring A which $1 \neq 0$ and every non-zero elem. is a unit.

Proposition 3.3.1 Let A be a ring $\neq 0$. The following are equivalent:
(1) A is a field;
(2) The only ideals in A are 0 and (1);
(3) Every non-trivial homomorphism of A into a non-zero ring B is injective.

3.4 prime ideals and maximal ideals

Definition 3.4.1 — prime ideal. An ideal $\mathfrak{p}$ in A is *prime* if $\mathfrak{p} \neq (1)$ and if $xy \in \mathfrak{p} \implies x \in \mathfrak{p}$ or $y \in \mathfrak{p}$

Definition 3.4.2 — maximal ideal. An ideal $\mathfrak{m}$in A is *maximal* if $\mathfrak{m}\neq (1)$ and if there is no ideal α such that $\mathfrak{m}\subset \alpha \subset (1)$(strict inclusion).

(R) $\mathfrak{m}$ can be $\{0\}$.

Proposition 3.4.1 $\mathfrak{p}$ is prime $\iff$ $A/\mathfrak{p}$ is an integral domain.

Proof. Easy to verify. ■

Proposition 3.4.2 $\mathfrak{m}$ is maximal $\iff$ A/m is a field. Hence, a maximal ideal is prime.

Proof. By Proposition 2.1.1 and Proposition 2.2.1, the statement holds. ■

Proposition 3.4.3 If $f : A \to B$ is a ring homomorphism and q is a prime ideal of B, then $f^{-1}(q)$ is a prime ideal in A.

Proof. If $a,b \in A$ such that $f(a) = f(b) \in q$. Then $f(a-b) = f(a) - f(b) \in q$. Thus, $f^{-1}(q)$ is abelian. For any $a \in f^{-1}(q), x \in A$, we have $f(ax) = f(a)f(x) \in Bq = q$. Thus, $f^{-1}(q)$ is an ideal. For any $a,b \in A, ab \in f^{-1}(q) \iff f(ab) \in q \iff f(a)\cdot f(b) \in q \iff f(a) \in q \vee f(b) \in q \iff a \in f^{-1}(q) \vee b \in f^{-1}(q) \iff f^{-1}(q)$ is a prime ideal. ■

(R) If m is a maximal ideal of B, it is not necessarily true that $f^{-1}(m)$ is maximal in A. Consider $A = \mathbb{Z}, B = \mathbb{Q}, m = \{0\}$.

Theorem 3.4.4 Every ring $A \neq 0$ has at least one maximal ideal.

This theorem relys on Zorn's Lemma. We first introduce it.

Definition 3.4.3 — chain in a partially ordered set. Let S be a non-empty partially ordered set. A subset T of S is a chain if either $x \leq y$ or $y \leq x$ for every pair of elements in T.

Lemma 3.4.5 — Zorn. If every chain T of S has an upper bound in S, then S has at least one maximal element. Zorn's Lemma is equivalent to the axiom of choice.

Proof. Let's prove theorem 2.3.4, using Zorn's Lemma.
Let $\Sigma = \{I : I \text{ is ideal}, I \neq (1)\}$. Order Σ by inclusion. Σ is not empty, since $0 \in \Sigma$. For each chain, consider the union as another ideal $\neq (1)$ to be an upper bound. Then Zorn's lemma yields that there is a maximal element. ■

Ⓡ If A is Noetherian, we can avoid the use of Zorn's lemma.

Corollary 3.4.6 If $a \neq (1)$ is an ideal of A, there exists a maximal ideal of A containing a.

Proof. Replace Σ by $\{I : I \text{ is ideal containing } a, I \neq (1)\}$ in the proof of Theorem 2.3.4 . ■

Corollary 3.4.7 Every non-unit of A is contained in a maximal ideal.

Definition 3.4.4 — local ring, residue field. If a ring A has exactly one maximal ideal m (e.g. fields), then A is called a *local ring*. The field $k = A/m$ is called the residue field of A.

Proposition 3.4.8 Let A be a ring and $m \neq (1)$ an ideal of A such that $\forall x \in A - m$ is a unit in A. Then A is a local ring and m its maximal ideal.

First, we observe the following

Lemma 3.4.9 Every element in a maximal ideal is not a unit.

proof of Proposition 2.3.8. From corollary 2.3.6 and lemma 2.3.9 we know m is a maximal ideal. Also from lemma 2.3.9, we know there doesn't exists other maximal ideals. Thus, A is a local ring. ■

Proposition 3.4.10 Let A be a ring and m a maximal ideal, such that every element of $1+m$ is a unit in A. Then A is a local ring.

Proof. Make an analogy to Bezout Theorem. Let $x \in A - m$. Since m is maximal, the ideal generated by x and m is (1), hence there exists $y \in A, t \in m$ such that $xy + t = 1$. Thus $xy = 1 - t \in 1 + m$, which means x is a unit. ■

■ **Example 3.2** $A = F[X_1, \ldots, X_n], F$: field. Let $f \in A$ be an irreducible polynomial. By unique factorization, the ideal (f) is prime. When $n \geq 2$, it's not a *principal ideal domain*. ■

■ **Example 3.3** Every ideal in $\mathbf{Z}$ is of the form (m) for some $m \geq 0$. The ideal is prime $\iff$ $m = 0$ or is a prime number. For all ideals (p) are maximal. ■

Definition 3.4.5 — principal integral domain. an integral domain where every ideal is principal.

Proposition 3.4.11 Every non-zero prime ideal is maximal in principal integral domain.

Hint. The cancellation law applies in the integral domain.
Let (x) be a prime ideal and $(x) \subset (y)$. Then $x = yz$ for some z. $sincey \notin (x)$, we know $z \in (x)$. Thus $z = xt$ and $x = ytx$, which implies $yt = 1$, and $(y) = 1$. ∎

3.5 nilradical and Jacobson radical

Proposition 3.5.1 The set $\mathfrak{N}$ of all nilpotent elements in a ring A is an ideal, and $A/\mathfrak{N}$ has no nilpotent element $\neq 0$.

Proof. For any $x, y \in \mathfrak{N}$, there exists $n \geq 0$ such that, $(x-y)^n = 0$. Thus, $x - y \in \mathfrak{N}$ and $\mathfrak{N}$ is abelian group. It's easy to show that $\mathfrak{N}$ is an ideal. If there exists $a \in A$, such that $\exists n > 0, (a+\mathfrak{N})^n = 0 = a^n + \mathfrak{N}$, then $a \in \mathfrak{N}$. Hence, $A/\mathfrak{N}$ has no non-zero nilpotent element. ∎

The ideal $\mathfrak{N}$ is called the *nilradical* of A.

Proposition 3.5.2 The nilradical of A is the intersection of all the prime ideals of A.

Proof. We observe that every nilpotent element belongs to any prime ideal. Hence, $\mathfrak{N} \subseteq \cap_{p:prime\ ideal} p$. On the other side, for each element within the intersection of all prime ideals, 试图用Zorn's lemma寻找一个极大理想，证明这也是一个prime ideal. 从而non-nilpotent element不属于这个ideal. ∎

Definition 3.5.1 — Jacobson radical. The Jacobson radical $\mathfrak{R}$ of A is defined to be the intersection of all the maximal ideals of A.

It can be characterized as

Proposition 3.5.3 $x \in \mathfrak{R} \iff 1 - xy$ is a unit for all $y \in A$.

Proof. $\Longrightarrow$: Suppose $1 - xy$ is not a unit. By corollary 2.3.7 it belongs to some maximal ideal m. But $x \in \mathfrak{R} \subseteq m$, hence $xy \in m$ and $1 \in m$, which is absurd.
$\Leftarrow$: 考虑Bezout定理。If $x \notin m$ for some maximal ideal m, then $m + (x)$ generate the unit ideal (1), so that $u + xy = 1$ for some $u \in m, y \in A$. Hence $1 - xy \in m$ is not a unit. ∎

3.6 operations on ideals

Definition 3.6.1 — intersection. the ideal $A \cap B$

(R) The union of A, B is typically not an ideal.

Definition 3.6.2 — sum. the ideal $A + B$

Definition 3.6.3 — product. AB denotes the ideal generated by elements in set AB, i.e. $AB = \{\sum_{finite} a_i b_i : a_i \in A, b_i \in B\}$

Definition 3.6.4 — coprime. ideals A, B are coprime if $A+B=(1)$.

Ⓡ different prime ideals are not necessarily coprime. For example, let $A = F[X,Y], p_1 = (X), p_2 = (Y)$.

Definition 3.6.5 Let A be a ring and $\alpha_1, ..., \alpha_n$ ideals of A. Define a homomorphism

$$\phi : A \to \prod_{i=1}^{n}(A/\alpha_i)$$

by the rule $\phi(x) = (x+\alpha_1, ..., x+\alpha_n)$.

Ⓡ Let a, b be ideals of ring A, then $ab \subseteq a \cap b$

Proposition 3.6.1 (1) If a_i, a_j are coprime whenever $i \neq j$, then $\prod a_i = \cap a_i$.
(2) ϕ is surjective $\iff$ a_i, a_j are coprime whenever $i \neq j$.
(3) ϕ is injective $\iff$ $\cap a_i = (0)$

Proof. The third statement can be shown by $\ker\phi = \cap \alpha_i$ ■

Ⓡ (2) is the generalized form of Chinese Remainder Theorem.

Proposition 3.6.2 Let $p_1, ..., p_n$ be prime ideals and let α be an ideal contained in $\cup_{i=1}^{n} p_i$. Then $\alpha \subseteq p_i$ for some i.

Proof. Prove by induction on n in the form

$$a \nsubseteq p_i (1 \leq i \leq n) \implies a \nsubseteq \cup_{i=1}^{n} p_i$$

n = 1 : trivial. If $n > 1$ and the result is true for n - 1, then for each i there exists $x_i \in a$ such that $x_i \notin p_j (\forall j \neq i)$. If there is some i such that $x_i \notin p_i$, succeed. If not, then $x_i \in p_i$ for all i, consider

$$y = \sum_{i=1}^{n} x_1 x_2 ... x_{i-1} x_{i+1} ... x_n$$

. ■

Proposition 3.6.3 Let $a_1, ...a_n$ be ideals and p be a prime ideal, $p \supseteq \cap_{i=1}^{n} a_i$. Then $p \supseteq a_i$ for some i. If $p = \cap a_i$, then $p = a_i$ for some i.

Proof. We observe that if $x, y \notin p$, then $xy \notin p$. ■

Definition 3.6.6 — ideal quotient. If a, b are ideals in a ring Am their *ideal quotient* is

$$(a : b) = \{x \in A : xb \subseteq a\}$$

Ⓡ $(a : b)$ is an ideal.

Definition 3.6.7 — annihilator. $(0 : b)$ is called the *annihilator* of b and denoted by $Ann(b)$.

3.7 extension and contraction

let $f : A \to B$ be a ring homomorphism.

Definition 3.7.1 — extension. If a is an ideal in A, we define the *extension* a^e to be the ideal generated by $f(a)$ in B. Explicitly, a^e is the set of all sums $\sum y_i f(x_i)$ where $x_i \in a, y_i \in B$.

Definition 3.7.2 — contraction. If b is an (prime) ideal of B, then $f^{-1}(b)$ is always an (prime) ideal of A, called the contraction b^c of b.

To show its correctness, we have the following

Proposition 3.7.1 Let $f : A \to B$ be a surjective ring homomorphism. There is a one-to-one correspondence between the ideals of $f(A) = B$ and ideals of A which contain $\ker f$, and prime ideals correspond to prime ideals.

$$\begin{tikzcd}
\{ideals\ of\ A : A \supseteq \ker f\} \arrow[r, leftrightarrow, "1:1"] & \{ideals\ of\ B\} \\
I \arrow[r, mapsto] & f(I) \\
f^{-1}(J) & J \arrow[l, mapsto]
\end{tikzcd}$$

Proof. We only show that prime-ideal correspondence. If I is prime, for any $f(a), f(b)$ where $a, b \in I$, $f(a)f(b) \in f(I) \iff f(ab) \in f(I) \iff ab \in I \iff a \in I \text{ or } b \in I \iff f(a) \in f(I) \text{ or } f(b) \in f(I)$. Thus, $f(I)$ is prime. The other side is similar. ■

3.8 polynomial rings

Here, we mainly consider integral domain or field to be the ring. We will use the notion of **degree**.

Lemma 3.8.1 Let R be an integral domain. For all non-zero $f, g \in R[X]$ we have $\deg(fg) = \deg f + \deg g$. And $R[X]$ is also an integral domain, with $R[X]^\times = R^\times$.

Now about polynomials over a field F.

Proposition 3.8.2 — 带余除法. For any $a, d \in F[X], d \neq 0$, there exists unique $q, r \in F[X]$ such that $\deg(r) < \deg(d), a = dq + r$. Here, we define $deg(0) = -\infty$.

Proof. To find r, consider set $\{a - dq : q \in F[X]\}$. There exists element such that $\deg(a - dq)$ is minimal. ■

Definition 3.8.1 — root. For a commutative ring R, $f \in R[X], a \in R$ such that $f(a) = 0$. Then a is called a root of f.

By proposition 2.7.2, we immediately get

Proposition 3.8.3 $f(a) = 0 \iff (X - a)|f$.

As to the number of roots, we have

Proposition 3.8.4 F : field, $f \in F[X] - \{0\}$, then f has at most $\deg f$ roots in F.

Proof. Use proposition 2.7.3 and induce on the degree of f. ■

Definition 3.8.2 — Fraction Field of an integral domain. Let A be an integral domain, use *Frac(A)* to denote ...

With fraction field, we can extend proposition 2.7.4,

Lemma 3.8.5 Let R be an integral domain, $f \in R[X] - \{0\}$, then f has at most $\deg f$ different roots in R.

4. Module Theory

4.1 modules and module homomorphisms

Definition 4.1.1 Let A be a communitative ring. An $A-$module is an abelian group M on which A acts linearly, i.e. for any $a,b \in A, x,y \in M$

$$a(x+y) = ax+ay \qquad (a+b)x = ax+bx \qquad (ab)x = a(bx) \qquad 1x = x$$

Proposition 4.1.1 There is a one-on-one correspondence between all A-module structure on M (denoted as $Mod_A(M)$) and ring homomorphisms $Hom(A,E(M))$.

Proof. check both sides.

$$\begin{array}{ccc} Mod_A(M) & \xleftrightarrow{1:1} & Hom(A,E(M)) \\ M & \longmapsto & (a \mapsto (m \mapsto am)) \\ a \cdot m := f(a)(m) & \longleftarrow\!\shortmid & f \end{array}$$

■

■ **Example 4.1** 1) An ideal α of A is an A-module.
2) If A is a field, then $A-$module = vector space.
3) If $A = k[X]$ where k is a field, then $A-module$ is a $k-$ vector space with a linear transformation.
4) If $A = \mathbb{Z}$ then $Z-module$ = Abelian group. ■

Definition 4.1.2 — module homomorphism. Let M,N be $A-$modules. A mapping $f : M \to N$

is an $A-$homomorphism if

$$f(x+y) = f(x) + f(y) \qquad f(ax) = a \cdot f(x)$$

Definition 4.1.3 The set of all A-module homomorphisms from M to N can be turned into an $A-$module as follows

$$(f+g)(x) := f(x) + g(x) \qquad (af)(x) := a(f(x))$$

This A-module is denoted by $Hom_A(M,N)$

4.2 submodules and quotient modules

Definition 4.2.1 A submodule M' of M is a subgroup of M which is closed under A-action.

Definition 4.2.2 — quotient. The abelian group M/M' inherits an $A - module$ structure by defining

$$a(x+M') = ax + M'$$

The quotient map $\pi : M \to M/M'$ is an A-module homomorphism.

Proposition 4.2.1 — A generalization of lattice homomorphism theorem in ring ideals. There is a one-to-one order-preserving correspondence between submodules of M which contains M' and submodules of M/M'.

Definition 4.2.3 — kernel, image. If $f : M \to N$ is an A-module homomorphism, define

$$\ker(f) = \{x \in M : f(x) = 0 \in N\} \qquad Im(f) = f(M) \qquad Coker(f) = N/Im(f)$$

Proposition 4.2.2 $\ker f$ is a submodule of M, $Im(f)$ is a submodule of N.

Proposition 4.2.3

$$M/\ker f \cong Im(f)$$

4.3 operations on submodules

Let $(M_i)_{i \in I}$ be a family of submodules of M.

Definition 4.3.1 — sum. $\sum M_i$ is the set of all finite sums $\sum x_i$, where $x_i \in M_i$. It's the smallest submodule that contains all the M_i.

Definition 4.3.2 — intersection. The intersection $\cap M_i$ is again a submodule of M.

Definition 4.3.3 Let α be an ideal of A, $M : A - module$ then αM is a sub A-module.

Definition 4.3.4 — annihilator.

4.4 direct sum and product

4.5 finitely generated modules

> **Definition 4.5.1 — free module.** A *free* A $-$ *module* is one which is isomorphic to some $\oplus_{i\in I}A$. A finitely generated free $A-module$ is isomorphic to $A\oplus\cdots\oplus A$ (n summands), which is denoted by A^n.

Proposition 4.5.1 M is a finitely generated A-module $\iff$ M is isomorphic to a quotient of A^n for some integer $n>0$.

Proof. $\implies$: consider

$$\begin{array}{rccc} \phi: & A^n & \longrightarrow & M \\ & (a_i) & \longmapsto & \sum a_i x_i \end{array}$$

Then $M\cong A/\ker\phi$.
$\impliedby$: consider

$$\begin{tikzcd} A^n \arrow[rr, "f"] \arrow[dr, two heads, "q"'] & & M \\ & A^n/N \arrow[ur, bend right, "\phi"'] & \end{tikzcd}$$

Then $f:=q\circ\phi$ is surjective homomorphism. And $(f(e_i))$ generates M since (e_i) generates A^n, where $e_i=(0,0,...,1,...,0)$. ■

Proposition 4.5.2 Let M be a finitely generated A-module, let α be an ideal of A, $\phi\in E(M)$ such that $\phi(M)\subseteq\alpha M$. Then there exists (a_i) such that

$$\phi^n+a_1\phi^{n-1}+...+a_n=0$$

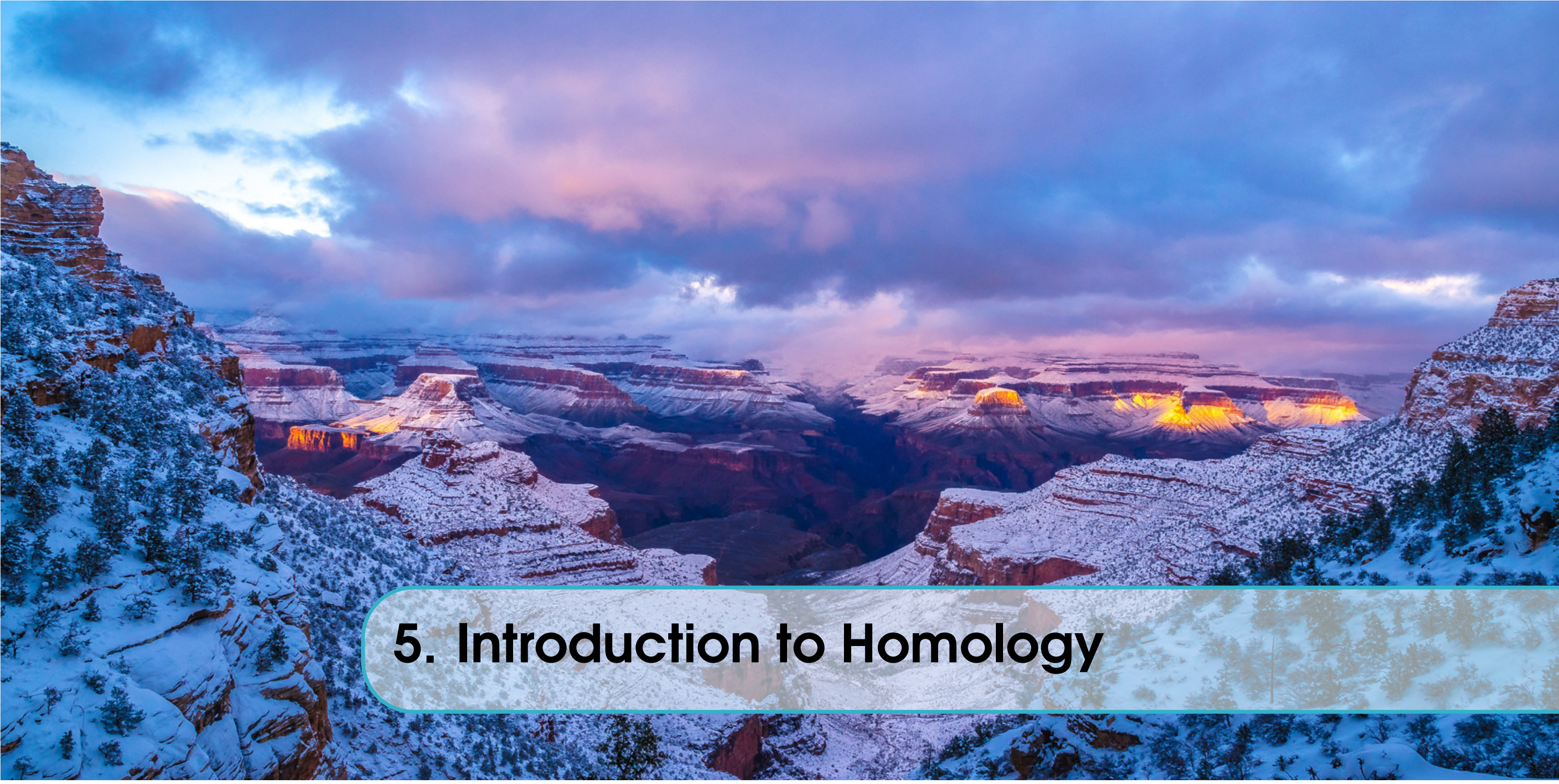
Proof. Let $x_1,...,x_n$ be generators of M, then each $\phi(x_i)\in\alpha M$, so that $\phi(x_i)=\sum_j a_{ij}x_j$, where $a_{ij}\in\alpha$. So ϕ is equivalent to a matrix over ring α. But $Cayley-Hamilton$ theorem, we know $Char_\phi(\phi)=0\in E(M)$. 参考高代的证明。 ■

> **Corollary 4.5.3** Let M be a finitely generated $A-module$, α be an ideal of A such that $\alpha M=M$. Then there exists $x\equiv 1(mod\ \alpha)$ such that $xM=0$.

Proof. take $\phi=id$ in Proposition 3.5.2, and $x=1+a_1+...+a_n$. ■

> **Theorem 4.5.4 — Nakayama's lemma.** Let M be a finitely generated $A-module$ and α an ideal of A contained in the Jacobson radical $\mathfrak{R}$ of A. Then $\alpha M=M$ implies $M=0$.

Proof. By 3.5.3 we get some $x\equiv 1$ (mod $\mathfrak{R}$), and x is a unit in A. Hence $M=0$. ■



5. Introduction to Homology

Definition 5.0.1 — A-module category. Suppose A is a commutative ring with an identity, we denoted as Mod_A as the class of all $A-modules$.

Definition 5.0.2 — complex 复形, exact 正和. Suppose M is a sequence of $A-modules$ and $A-$homomorphisms

$$\dots \longrightarrow M_{i-1} \xrightarrow{f_i} M_i \xrightarrow{f_{i+1}} M_{i+1} \longrightarrow \dots$$

is said to be a *complex* if for any i, $f_{i+1} \circ f_i = 0$, i.e. $Im(f_i) \subseteq \ker f_{i+1}$.
we say it's *exact at* M_i, if $Im(f_i) = \ker f_{i+1}$
we say it is *exact*, if it's exact at all M_i.

Definition 5.0.3 — homology group. For a complex (chain) M, since $Im(f_i)$ is a submodule of $\ker f_{i+1}$, we define a group

$$H_i(M) = \frac{\ker f_{i+1}}{Im(f_i)}$$

called *(co)homology as i*

■ **Example 5.1** If $0 \to M' \xrightarrow{f} M \xrightarrow{g} M'' \to 0$ is exact, then

- f is injective.
- g is surjective
- $\ker g = Im(f)$

i.e. $M/Im(f) \cong M''$. ■

Proposition 5.0.1 — exact test. In the category of Mod_A, we have

1. $M' \xrightarrow{u} M \xrightarrow{v} M'' \to 0$ is exact if and only if
   For any $N \in Mod_A$, the sequence $0 \to Hom_A(M'', N) \xrightarrow{\bar{v}} Hom_A(M, N) \xrightarrow{\bar{u}} Hom_A(M', N)$ is exact.

2. $0 \to N' \xrightarrow{u} N \xrightarrow{v} N''$ is exact if and only if
   For any $M \in Mod_A$, the sequence $0 \to Hom(M,N') \xrightarrow{\overline{u}} Hom(M,N) \xrightarrow{\overline{v}} Hom(M,N'')$ is exact.

Proof. For (1).
$\Longrightarrow$ The condition means $v : surj \wedge Im(u) = \ker v$. So $v \circ u = 0 \in Hom(M',M'')$. For any $f \in Hom(M'',N)$, $\overline{v}$ maps f to $f \circ v$. Since v is surjective, then $f_1 \circ v = f_2 \circ v \implies f_1 = f_2$. Thus, $\overline{v}$ is injective. It's easy to show $Im(\overline{v}) \subseteq \ker \overline{u}$. $\ker \overline{u} \subseteq Im(\overline{v})$ can be deduced by the following claim:

$$\begin{tikzcd}
M \arrow[r, two heads, "v"'] \arrow[rr, bend left, "g"] & M'' \arrow[r, "f"'] & N \\
m \arrow[r, mapsto] & v(m) \arrow[r, mapsto] & g(m)
\end{tikzcd}$$

If $g : M \to N$ such that (for any $v(m) = 0 \in M''$, then $g(m) = 0 \in N$), then there exists unique $f : M'' \to N$ such that $g = f \circ v$, where all the maps are homomorphisms.
proof of the claim
Since v is surjective, the only possible f maps $v(m)$ to $g(m)$. We need to verify f is a module homomorphism. First, it is well defined since $\ker v \subseteq \ker g$. The homomorphism follows naturally.
$\Longleftarrow$ First, we show v surjective $\iff M''/Im(v) = \{0\}$. Take $N = M''/Im(v)$, we have

$$\begin{tikzcd}
Hom_A(M'',N) \arrow[r, hook] & Hom_A(M,N) \\
(M'' \xrightarrow{quotient} N) \arrow[r, mapsto] & M \arrow[r, "v"'] \arrow[rr, bend right, "zero-map"'] & M'' \arrow[r, "quotient"'] & N = M''/Im(v)
\end{tikzcd}$$

Hence, the quotient map (a surjective one) is zero map, which means $N = \{0\}$.
Second, we show $Im(u) \subseteq \ker v$. The condition $(\overline{u} \circ \overline{v})$ means the following diagram commutes for any $N \in Mod_A, f \in Hom_A(M'',N)$.

$$\begin{tikzcd}
M' \arrow[r, "u"'] \arrow[drr, "zero-map"] & M \arrow[r, "v"'] & M'' \arrow[d, "f"] \\
 & & N
\end{tikzcd}$$

Take $N = M'', f = id$, which yields $v \circ u = 0$.
Finally, we show $\ker v \subseteq Im(u)$.

$$\begin{tikzcd}
M' \arrow[r, "u"'] \arrow[rr, bend left, "zero-map"] & M \arrow[r, "f=quotient"'] \arrow[d, "v"] & N = M/Im(u) \\
 & M'' \arrow[ur, "g"] &
\end{tikzcd}$$

The conditions and the proposition can be converted as, for any $f : M \to N$ such that $f \circ u = zero-map$, there exists $g : M'' \to N$, such that $f = g \circ v$. Since we know $Im(u) \subseteq \ker v$, we can take $N = M/Im(u)$ and $f = quotient$. If g is well-defined, then $\ker v \subseteq \ker f = Im(u)$.
(2) *to be written* ■

Definition 5.0.4 — covariant functor 共变函子. A functor $\mathscr{F} : Mod_A \to Mod_B$ consists of the following data
(1) for any $M \in Mod_A$, give $\mathscr{F}M \in Mod_B$.
(2) for any $A-module$ homomorphism $g : M \to N$, give a $B-module$ homomorphism $\mathscr{F}(g) : \mathscr{F}M \to \mathscr{F}N$ such that
- $\mathscr{F}(g \circ h) = \mathscr{F}(g) \circ \mathscr{F}(h)$.
- $\mathscr{F}(id_M) = id_{\mathscr{F}M}$.

Moreover, if $\mathscr{F} : Hom_A(M,N) \to Hom_B(\mathscr{F}M, \mathscr{F}N)$ is a group homomorphism for all M,N, i.e. $\mathscr{F}(g+h) = \mathscr{F}(g) + \mathscr{F}(h)$, we say $\mathscr{F}$ is an addictive functor.

Definition 5.0.5 — contravariant functor 反变函子. A functor $\mathscr{F} : Mod_A^{op} \to Mod_B$ consists of the following data
(1) for any $M \in Mod_A$, give $\mathscr{F}M \in Mod_B$.
(2) for any $A-module$ homomorphism $g : M \to N$, give a $B-module$ homomorphism $\mathscr{F}(g) : \mathscr{F}N \to \mathscr{F}M$ such that
- $\mathscr{F}(g \circ h) = \mathscr{F}(h) \circ \mathscr{F}(g)$.
- $\mathscr{F}(id_M) = id_{\mathscr{F}M}$.

■ **Example 5.2** Let $M,N \in Mod_A$, define functor

$$Hom_A(M,\cdot) : \quad Mod_A \longrightarrow Mod_A$$

$$T \longmapsto Hom_A(M,T)$$

$$(T_1 \xrightarrow{f} T_2) \longmapsto Hom(M,T_1) \longrightarrow Hom(M,T_2)$$

$$(M \to T_1) \longmapsto (M \to T_1 \xrightarrow{f} T_2)$$

This functor is addictive and covariant. ■

Proof. check that $\mathscr{F}(g \circ h) = \mathscr{F}(g) \circ \mathscr{F}(h)$. Others are trivial. ■

■ **Example 5.3** In a similar way, we can define $Hom_A(\cdot,N)$. Show that it is a contravariant functor. ■

Definition 5.0.6 — exact functor 正和函子. Let $\mathscr{F} : Mod_A \to Mod_B, \mathscr{G} : Mod_A^{op} \to Mod_B$ be addictive.
(1) Say $\mathscr{F}$ is *left exact* if for any short exact seq $0 \to M \to N \to R \to 0$ in Mod_A, the sequence $0 \to \mathscr{F}M \to \mathscr{F}N \to \mathscr{F}R$ is exact.

Respectively, $\mathscr{G}$ is *left exact* if for any short exact seq $0 \to M \to N \to R \to 0$ in Mod_A, the sequence $0 \to \mathscr{G}R \to \mathscr{G}N \to \mathscr{G}M$ is exact.
(2) Say $\mathscr{F}$ is *right exact* if for any short exact seq $0 \to M \to N \to R \to 0$ in Mod_A, the sequence $\mathscr{F}M \to \mathscr{F}N \to \mathscr{F}R \to 0$ is exact.
Respectively, $\mathscr{G}$ is *left exact* if for any short exact seq $0 \to M \to N \to R \to 0$ in Mod_A, the sequence $\mathscr{G}R \to \mathscr{G}N \to \mathscr{G}M \to 0$ is exact.
(3) Say $\mathscr{F}(respectively, \mathscr{G})$ is exact if $\mathscr{F}(or, \mathscr{G})$ is both left and right exact.

Proposition 5.0.2 $Hom_A(M, \cdot)$ and $Hom_A(\cdot, N)$ are left exact functors.

Proof. By Proposition 4.0.1. ∎