

Algebra (Honor Track)

Spring 2024

Commutative 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

1	Group Theory	7
1.1	Groups and subgroups	7
1.1.1	Important Examples of Groups	7
1.2	cosets, Lagrange theorem, quotient groups	8
1.2.1	Conjugation, normal subgroups, and quotient groups.	8
1.2.2	Some Technical Results	8
1.2.3	homomorphism	9
1.3	isomorphism theorems, composition series, statement of Holder Theorem	9
1.3.1	isomorphism theorems	9
1.4	Lattice	11
1.5	composition series, Jordan-Holder Theorem, simplicity of An, direct product groups	11
1.5.1	The simplicity of A_n , $n \geq 5$	11
2	Rings and Ideals	13
2.1	rings, ideals, quotient rings	13
2.2	Chinese Remainder Theorem	14
2.3	zero-divisors, nilpotent elements, units	14
2.4	prime ideals and maximal ideals	15
2.5	nilradical and Jacobson radical	17
2.6	operations on ideals	17
2.7	polynomial rings	17

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} = symmetric group of a regular 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 $\Omega = \{1, 2, \dots, n\}$, 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.

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

1.2 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 $H \trianglelefteq G$ 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. to be written ■

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 $\forall h_1 k_1 \cdot (h_2 k_2)^{-1} = h_1 k_1 k_2^{-1} h_2^{-1} \in HK$. Since $h_1(k_1 k_2^{-1}) \in HK = KH$, there exists h, k such that $h_1 k_1 k_2^{-1} = kh$. Then $kh_2^{-1} \in KH = HK$. ■

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

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

Lemma 1.2.4 Let $\phi : G \rightarrow H$ 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

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

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 $\phi : G \rightarrow H$ of groups is injective if and only if $\ker \phi = \{e_G\}$.

1.3 isomorphism theorems, composition series, statement of Holder Theorem

1.3.1 isomorphism theorems

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

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

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 $\phi : AB \rightarrow A/(A \cap B)$ 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.

$$\begin{array}{ccc}
 AB & \xrightarrow{\phi} & A/(A \cap B) \\
 & \searrow q & \nearrow f \\
 & AB/B &
 \end{array}$$

■

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

$$\phi : G/H \longrightarrow G/K$$

$$gH \longmapsto gK$$

- 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

$$\{\text{subgroups of } G \text{ containing } N\} \longleftrightarrow \{\text{subgroups of } G/N\}$$

$$A \longmapsto A/N$$

$$\pi^{-1}(\bar{A}) \longleftarrow \bar{A}$$

where $\pi : G \rightarrow G/N$ 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 $N \iff$ 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 1.1** 设 n 为正整数, A_n 为 n 的所有正因数的几何, 则 A_n 关于整除关系构成格。

■

■ **Example 1.2** 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 1.3** — 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 A_n , direct product groups

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

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

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

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

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,

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

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

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

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

Proof. to be written

1.5.1 The simplicity of A_n , $n \geq 5$

Proposition 1.5.3



2. Rings and Ideals

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

2.1 rings, ideals, quotient rings

Definition 2.1.1 — ring homomorphism. Let A, B be rings, $f : A \rightarrow B$ 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 2.1.2 — ideal of a ring. An ideal I of a ring A is an additive subgroup and is such that $AI \subseteq I$.

■ **Example 2.1** Every ring A has 2 trivial ideals: $\{0\}$ and A . ■

Below, I denotes the ideal of ring A .

Definition 2.1.3 — 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 $\phi : A \rightarrow A/I$ which maps each $x \in A$ to its coset $x+I$ is a surjective ring homomorphism.

Proposition 2.1.1 There is a one-to-one order preserving correspondence between

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

$$J \longmapsto J+I$$

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

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 2.1.2 If $f : A \rightarrow B$ 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 2.1.3 — fundamental homomorphism theorem. $f : A \rightarrow B$ is a ring homomorphism, I is the kernel of f , $g(a+I) := f(a)$ then g is a ring isomorphism.

$$\begin{array}{ccccc} A & \xrightarrow{f} & \text{Im}(f) & \hookrightarrow & B \\ & \searrow \phi & \uparrow g & & \\ & & A/I & & \end{array}$$

2.2 Chinese Remainder Theorem

Theorem 2.2.1 Let $N \in \mathbb{N}^+, N = n_1 n_2 \dots n_k$, where $n_i, n_j (i \neq j)$ are coprime. We have

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

is an isomorphism of rings.

2.3 zero-divisors, nilpotent elements, units

Definition 2.3.1 — 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 2.3.2 — integral domain. a ring with no zero-divisors $\neq 0$ and not a zero ring.

Definition 2.3.3 — 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 2.3.4 — 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 2.3.5 — field. A field is a ring A which $1 \neq 0$ and every non-zero elem. is a unit.

Proposition 2.3.1 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.

2.4 prime ideals and maximal ideals

Definition 2.4.1 — 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 2.4.2 — 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 2.4.1 \mathfrak{p} is prime $\iff A/\mathfrak{p}$ is an integral domain.

Proof. Easy to verify. ■

Proposition 2.4.2 \mathfrak{m} is maximal $\iff A/\mathfrak{m}$ is a field. Hence, a maximal ideal is prime.

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

Proposition 2.4.3 If $f : A \rightarrow B$ 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 2.4.4 Every ring $A \neq 0$ has at least one maximal ideal.

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

Definition 2.4.3 — 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 2.4.5 — 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. ■

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

Corollary 2.4.6 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 2.4.7 Every non-unit of A is contained in a maximal ideal.

Definition 2.4.4 — 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 2.4.8 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 2.4.9 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 exist other maximal ideals. Thus, A is a local ring. ■

Proposition 2.4.10 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 2.2** $A = F[X_1, \dots, X_n], F : \text{field}$. 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 2.3** 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 2.4.5 — principal integral domain. an integral domain where every ideal is principal.

Proposition 2.4.11 Every non-zero prime ideal is maximal.

Hint. The cancellation law applies in the integral domain. ■

2.5 nilradical and Jacobson radical

Proposition 2.5.1 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 2.5.2 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, $\mathfrak{N} \subseteq \cap_{p:\text{prime ideal } p}$. 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 2.5.1 — Jacobson radical. The Jacobson radical \mathfrak{N} of A is defined to be the intersection of all the maximal ideals of A .

It can be characterized as

Proposition 2.5.3 $x \in \mathfrak{N} \iff 1 - xy$ is a unit for all $y \in A$.

Proof. \implies : Suppose $1 - xy$ is not a unit. By corollary 2.3.7 it belongs to some maximal ideal m . But $x \in \mathfrak{N} \subseteq m$, hence $xy \in m$ and $1 \in m$, which is absurd.

\impliedby : 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. ■

2.6 operations on ideals

2.7 polynomial rings

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

Lemma 2.7.1 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 2.7.2 — 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 2.7.1 — 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 2.7.3 $f(a) = 0 \iff (X - a)|f$.

As to the number of roots, we have

Proposition 2.7.4 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 2.7.2 — Fraction Field of an integral domain. Let A be an integral domain, use $\text{Frac}(A)$ to denote ...

With fraction field, we can extend proposition 2.7.4,

Lemma 2.7.5 Let R be an integral domain, $f \in R[X] - \{0\}$, then f has at most $\deg f$ different roots in R .



3. Module Theory