Algebra (Honor Track)
Spring 2024

Communitative Algebra

Notes

ymy

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.

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

1.2 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. *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 $khh_2^{-1} \in KH = HK$. ∎

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 $\phi : G \to H$ 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 $\phi(g_1)\phi(g_2)^{-1} = \phi(g_1 g_2^{-1}) \in \phi(G)$
(2) If $g_1, g_2 \in ker\ \phi$, then

$$\phi(g_1 g_2^{-1}) = e_H e_H^{-1} = e_H$$

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

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

∎

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

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

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

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 $H \le K$. 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 1.1** 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 。 ■

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, $f : A \to B$ 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 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 $\phi : A \to A/I$ 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

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

$$J \longmapsto J + I$$

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

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 2.1.2 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 2.1.3 — 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.

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

2.2 zero-divisors, nilpotent elements, units

Definition 2.2.1 — 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 2.2.2 — integral domain. a ring with no zero-divisors $\neq 0$ and not a zero ring.

Definition 2.2.3 — 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 2.2.4 — 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 2.2.5 — field. A field is a ring A which $1 \neq 0$ and every non-zero elem. is a unit.

Proposition 2.2.1 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.

2.3 prime ideals and maximal ideals

Definition 2.3.1 — 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 2.3.2 — 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).

Proposition 2.3.1 $\mathfrak{p}$ is prime $\iff A/\mathfrak{p}$ is an integral domain.

Proof. Easy to verify. ■

Proposition 2.3.2 $\mathfrak{m}$ 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. ■

3. Module Theory