SEMINAR NOTES: COMMUTATIVE ALGEBRAS

ZOU HAITAO

Contents

1. Rings and Ideals

Definition 1.1. A **ring** R is a set with two maps (addition) $+ : R \times R \to R$, (multiplication)$\times : R \times R \to R$(denote $+(x, y)$ by $x + y$ and $\times(x, y)$ by $x \times y$)that satisfy following properties

(1) R is a abelian group with respect to addition, its identity is denoted by 0;
(2) R is a monoid with identity $1 \in R$ with respect to multiplication;
(3) $z \times (x + y) = z \times x + z \times y$ and $(x + y) \times z = x \times z + y \times z$ for any given x, y, z.

We typically write xy for $x \times y$.

In a ring R, if $1 = 0$, then R has only one elements, it is trival and called **zero ring**. Denoted zero ring by 0.

Suppose R be a ring. R is commutative if for any $x, y \in R$, $xy = yx$. Rings mentioned in this notes will always be commutative other assumption.

Definition 1.2. Let A and B be two rings. 1_A and 1_B are their identities. A ring homomorphism from A to B is a map $f : A \to B$, which preserves both addition and multiplication structure, that means, for any $x, y \in A$

$$f(x + y) = f(x) + f(y)$$
$$f(xy) = f(x)f(y)$$
$$f(1_A) = 1_B$$

Suppose $f : A \to B$ be a ring homomorphism. We have $f(0_A) = f(1_A - 1_A) = f(1_A) - f(1_A) = 1_B - 1_B = 0_B$.

(1) If f is surjective as map, then f is called surjective homomorphism.
(2) If f is injective as map, then f is called injective homomorphism.

Definition 1.3. An **isomorphism** between two rings A and B is a ring homomorphism $f : A \to B$ such that there is another ring homomorphism $g : B \to A$ satisfying

$$f \circ g = \mathrm{id}_B \quad g \circ f = \mathrm{id}_A$$

Remark 1.1. f is isomorphism if and only if f is both surjective and injective as ring homomorphism.

Proof. If f is isomorphism, then $f(x) = f(y)$ implies $g(f(x)) = g(f(y))$. But $g \circ f = \mathrm{id}_A$, so $x = y$. Hence f is injective. For any $b \in B$, $b = f \circ g(b)$ since $f \circ g = \mathrm{id}_B$. Let $a = g(b), b = f(a)$. That means f is surjective.

If f is both injective and surjective homomorphism, then we only need to check if f^{-1} is ring homomorphism. $f(f^{-1}(b_1 + b_2)) = b_1 + b_2 = f \circ f^{-1}(b_1) + f \circ f^{-1}(b_2) = f(f^{-1}(b_1) + f^{-1}(b_2))$. Since f is surjective, $f^{-1}(b_1 + b_2) = f^{-1}(b_1) + f^{-1}(b_2)$.

Similarly, $f^{-1}(b_1 b_2) = f^{-1}(b_1)f^{-1}(b_2)$. □

It is not always true in arbitrary category(**Top**, **Sch**/k, **Mod**$_k$, etc).

If two rings are isomorphic, then we view them as same object in ring category.

Definition 1.4. Let R be a ring. We call $i : \tilde{R} \to R$ is a subring if i is injective ring homomorphism, written as $\tilde{R} \subset R$

Remark 1.2. The definition of subring in "Atiyah& MacDonald" is not exact since it doesn't requrie $\tilde{R}$ to be even a ring.

Remark 1.3. $i(\tilde{R}) \simeq \tilde{R}$, so $\tilde{R}$ can be viewed as $i(\tilde{R})$ whose elements are in R.

Definition 1.5. Let R be a ring, I be an additive subgroup of R. I is called an **ideal** of R if for any $r \in R$

$$rI := ra|a \in I \subset I$$
$$Ir := ar|a \in I \subset I$$

Since R is commutative, $Ir = rI$. We only need to check one of them. If I is ideal of R, then we denote the fact by $I \lhd R$.

An ideal $\mathfrak{p} \lhd R$ is called **prime ideal** if $xy \in \mathfrak{p}$ implies either $x \in \mathfrak{p}$ or $y \in \mathfrak{p}$.

An ideal $\mathfrak{m} \lhd R$ is called **maximal ideal** if $\mathfrak{m} \neq (1)$ and if there is no ideal I such that $m \subsetneq I \subsetneq (1)$.

$$\text{Ideal}(R) := \{\text{ideals of } R\}$$

Let $\varphi : A \to B$ be a ring homomorphism. Then there is induced map

$$\varphi^{\#} : \text{Ideal}(B) \to \text{Ideal}(A)$$
$$\mathfrak{b} \mapsto \varphi^{-1}(\mathfrak{b})$$

For any $x, y \in \varphi^{-1}(\mathfrak{b})$, $\varphi(x+y) = \varphi(x)+\varphi(y) \in \mathfrak{b}$, $\varphi(ax) = \varphi(a)\varphi(x) \in \mathfrak{b}$ implies that $ax \in \varphi^{-1}(b)$. Hence $\varphi^{-1}(\mathfrak{b}) \in \text{Ideal}(A)$. Furthermore, it can be checked that $\varphi^{\#}$ is map from Spec$B$ to Spec$A$.

$$\ker\varphi := \{a \in A|\varphi(a) = 0\} = \varphi^{-1}((0))$$

If $a_0 \in \ker\varphi$, then for any $a \in A$, $\varphi(aa_0) = \varphi(a)\varphi(a_0) = 0$, so $aa_0 \in \ker\varphi$. Hence $\ker\varphi \in \text{Ideal}(A)$. Since 0 is contained in any ideals, $\varphi^{\#}(\mathfrak{b}) = \varphi^{-1}(\mathfrak{b}) \supset \ker\varphi$

Lemma 1.1. *Let $I \lhd R$. Relation such that $\sim_I$ on R defined as $x \sim_I y$ if and only if $x - y \in I$ is a equivalence relation.*

Proof.
(1) $x - x = 0 \in I \Rightarrow x \sim_I x$
(2) $x - y \in I \Rightarrow y - x = -(x - y) \in I \Rightarrow y \sim_I x$
(3) $x \sim_I y, y \sim_I z \Rightarrow x - y \in I, y - z \in I \Rightarrow x - z = (x - y) + (y - z) \in I \Rightarrow x \sim_I z$.

□

Definition 1.6. Let I be a ring

$$R/I := (R/\sim_I, \times, +)$$
$$\bar{x} + \bar{y} = \overline{x+y}$$
$$\bar{x} \times \bar{y} = \overline{xy}$$

is called quotient ring of R by ideal I.

Remark 1.4. It is easy to check R/I is well defined

$$\varphi : R \to R/I$$
$$r \mapsto \bar{r}$$

$\varphi(r_1 + r_2) = \overline{r_1 + r_2} = \bar{r_1} + \bar{r_2} = \varphi(r_1) + \varphi(r_2)$, $\varphi(r_1r_2) = \overline{r_1r_2} = \bar{r_1}\bar{r_2} = \varphi(r_1)\varphi(r_2)$ and $\overline{1_R}\bar{r} = \overline{1_Rr} = \bar{r}$, so $\varphi(1_R) = \overline{1_R}$ is identity of R/I. Hence φ is ring homomorphism.

FACT:
(1) $\ker\varphi = I$;
(2) φ is surjective;
(3) $\varphi^{\#}$ is injective. If $\varphi^{\#}(\bar{\alpha}) = \varphi^{\#}(\bar{\beta})$, then $\varphi^{-1}(\bar{\alpha}) = \varphi^{-1}(\bar{\beta})$. φ is surjective so $\bar{\alpha} = \bar{\beta}$.

(4) If $\ker\varphi \subset I \lhd R$, then for any $\bar{i} \in \varphi(I)$, $\bar{r}\bar{i} = \overline{ri} = \varphi(ri)$ and $\varphi(I)$ is additive subgroup of R/I, $\varphi(I) \in \mathrm{Ideal}(R/I)$. φ is surjective, so $I = \varphi^{-1}(\varphi(I)) = \varphi^{\#}(\varphi(I))$.

(3) and (4) implies following proposition.

Proposition 1.2. *$\varphi^{\#}$ is one-to-one correspondence between Ideal(B/I) and set of ideals contain I in R.*

□

Definition 1.7. Let R be a ring.

(1) $x \in R$ is called **zero divisor** if there is $r \in R, r \neq 0$ such that $rx = 0$.
(2) $x \in R$ is called **nilpotent element** if $x^n = 0$ for some $n > 0$.
(3) $x \in R$ is an **unit** of R if x has inverse under multiplication.
(4) If R has no zero divisors except 0, then R is called **integral domain**.

Remark 1.5. A nilpotent element in a ring is always zero divisor since $xx^{n-1} = 0$. If x is a unit in R, then x is not a zero divisor. Conversely, it is not always true.

Definition 1.8. A **principal ideal** of R is an ideal that can be generated by one element, written as (x), where x is the generator.

For simple example, $(3, 6) \lhd \mathbb{Z}$ is principal ideal generated by 6. R itself is also a principal ideal since it can be generated by 1, written as (1).

Following are equivalent criteria for primes ideals and maximal ideals

Proposition 1.3. *Let R be a ring.*

(1) $\mathfrak{p} \lhd R$ is prime ideal if and only if $R/\mathfrak{p}$ is integral domain.
(2) $\mathfrak{m} \lhd R$ is maximal ideal if and only if R/m is a field.

Proof. (1) Let $\mathfrak{p} \lhd R$ be a prime ideal. For any $x, y \in R$, $\bar{x}, \bar{y} = \bar{0}$ is equivalent to $xy \in \mathfrak{p}$. But $xy \in \mathfrak{p}$ implies that either $x \in \mathfrak{p}$ or $y \in \mathfrak{p}$, equivalently, $\bar{x} = 0$ or $\bar{y} = 0$. This shows that $R/\mathfrak{p}$ is integral domain.

Conversly, if $R/\mathfrak{p}$ is ingegral domain, then for any $x, y \in R$ such that $xy \in \mathfrak{p}$, $\bar{x}\bar{y} = \bar{0}$ in $R/\mathfrak{p}$, we have $\bar{x} = \bar{0}$ or $\bar{y} = \bar{0}$. That means $x \in \mathfrak{p}$ or $y \in \mathfrak{p}$. Hence we can conclude the equivalence.

(2) Let $\mathfrak{m} \lhd R$ be a maximal ideal. If $\bar{x} \in R/\mathfrak{m}, \bar{x} \neq \bar{0}$, then $x \notin \mathfrak{m}$. Since $\mathfrak{m}$ is maximal, $m \subsetneq (\mathfrak{m}, x) \subset (1)$ implies that $(\mathfrak{m}, 1) = (1)$. That means, there exists $y \in R$ such that $xy = 1$. Obviously, $y \notin m$, so $\bar{x}\bar{y} = \bar{1}$. Hence each non-zero element in $R/\mathfrak{m}$ is unit. Hence $R/\mathfrak{m}$ is a field.

Conversely, if $R/\mathfrak{m}$ is a field, then $\bar{x} \in R/\mathfrak{m}, \bar{x} \neq 0$ is unit. But $\bar{x} \neq \bar{0}$ is equivalent to $x \notin \mathfrak{m}$ and $\bar{x}$ is unit $R/\mathfrak{m}$ if and only if x is unit in R. So $(\mathfrak{m}, x) = (1)$ if $x \notin \mathfrak{m}$. Hence $\mathfrak{m}$ is maximal. The proof is complete.

□