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 trivial 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, $\mathbf{Mod}_k$, 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 $m \subsetneq I \subsetneq (1)$.

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

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$A$.

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

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, $\varphi(I) \in \text{Ideal}(R/I)$. 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).

Let $I_1 \lhd R, I_2 \lhd R$. We give following serveral constructions of ideals

$$I_1 \cdot I_2 = \{xy \in R | x \in I_1, y \in I_2\} \qquad \prod_{i=1}^{n} I_i = \{x_1x_2 \cdots x_n \in R | x_i \in I_i\}$$
$$I_1 + I_2 = \{x + y | x \in I_1, y \in I_2\} \qquad \sum_{\alpha} I_\alpha = \{\sum_{\alpha} x_\alpha | x_\alpha \in I_\alpha \text{ and only finite } x_\alpha \text{ are not zero}\}$$

$I_1 \cap I_2$ is obviously an ideal since $\forall x, y \in I_1 \cap I_2, r \in R, xr \in I_1 \cap I_2$ and $x + y \in I_1 \cap I_2$.

Examples 1.6. Let $A = \mathbb{Z}$, $(m), (n)$ two principal ideal generated by m and n.
$(m) + (n) = ((m, n))$ is generated by (m, n), the g.c.d of m and n
$(m) \cdot (n) = (m \cdot n)$
$(m) \cap (n) = ([m, n])$ is generated by $[m, n]$, the l.c.d of m and n.
If $(m, n) = 1$, then $(m) + (n) = (1), (m)(n) = (m) \cap (n)$.

Let $I \lhd R, x \in R$. (x, I) is ideal generated by x and elements of I. Since $(x) + I$ is minimal ideal contains both x and elements of I, $(x) + I = (x, I)$.

Definition 1.9. If $I_1 \lhd R, I_2 \lhd R$. I_1 and I_2 are called **coprime** if $I_1 + I_2 = (1)$.

Proposition 1.3. *If $I_1 \lhd R, I_2 \lhd R$ are coprime, then $I_1 \cdot I_2 = I_1 \cap I_2$.*

Proof. By definition, $I_1 \cdot I_2 \subseteq I_1 \cap I_2$. Let $x \in I_1 \cap I_2$, x can be represented by $x = ar_1 + br_2$, where $a \in I_1, b \in I_2$. Hence $x \in I_1 \cdot I_2 = I_1 \cap I_2$. □

Definition 1.10. Let A_α be a family of rings. Their **direct product** is defined as object $\prod_\alpha A_\alpha$ in **Rings** satisfying following universal property

$$\begin{tikzcd}
 & & A_i \\
Z \arrow[r, dashed, "\exists!"] \arrow[urr, bend left, "h_i"] \arrow[drr, bend right, "h_j"'] & \prod_\alpha A_\alpha \arrow[ur, "p_i"'] \arrow[dr, "p_j"] & \\
 & & A_j
\end{tikzcd}$$

If α is finite, then elements of $\prod_\alpha A_\alpha$ can be written as $(x_1, \cdots, x_n)$, $x_i \in A_i$ for some n.

$$(x_1, \cdots, x_n) \cdot (x_1', \cdots, x_n') = (x_1x_1', \cdots, x_nx_n')$$
$$(x_1, \cdots, x_n) + (x_1', \cdots, x_n') = (x_1 + x_1', \cdots, x_n + x_n')$$
$$1 = (1_{A_1}, \cdots, 1_{A_n})$$

Let A be a ring and $\mathfrak{a}_1, \cdots, \mathfrak{a}_n$ ideals of A. Define a homomorphism

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

by rules $\phi(x) = (x + \mathfrak{a}_1, \cdots, x + \mathfrak{a}_n)$.

Proposition 1.4 (**??**). *(1) If $\mathfrak{a}_i, \mathfrak{a}_j$ are coprime whenever $i \neq j$, then $\prod_i \mathfrak{a}_i = \bigcap_i \mathfrak{a}_i$;*
(2) ϕ is surjective $\Leftrightarrow$ $\mathfrak{a}_i, \mathfrak{a}_j$ are coprime whenever $i \neq j$;
(3) ϕ is injective $\Leftrightarrow$ $\bigcap_i \mathfrak{a}_i = (0)$.

Proof. (1) By 1.3 the case $n = 2$ is proved. Assume it is true when $n = k$. When $n = k + 1$, since $\mathfrak{a}_i$ and $\mathfrak{a}_{k+1}$ are coprime for $1 \leq i \leq k$, $\mathfrak{a}_i + \mathfrak{a}_{k+1} = (1)$. It implies that $x_i + y_i = 1$ for some $x_i \in \mathfrak{a}_i$, $y_i \in \mathfrak{a}_{k+1}, 1 \leq i \leq k$

$$\prod_{i=1}^k x_i = 1 \text{ in } A/\mathfrak{a}_{k+1}$$

that means $\prod_{i=1}^k x_i + x_{k+1} = 1$ for some $x_n \in \mathfrak{a}_{k+1}$ in R. Hence $\prod_{i=1}^k \mathfrak{a}_i$ and $\mathfrak{a}_{k+1}$ are coprime. Then

$$\prod_{i=1}^{k+1} \mathfrak{a}_i = (\prod_{i=1}^k \mathfrak{a}_i) \cdot \mathfrak{a}_k = (\bigcap_{i=1}^k \mathfrak{a}_i) \cap \mathfrak{a}_{k+1} = \bigcap_{i=1}^{k+1} \mathfrak{a}_i$$

by induction.

(2) If ϕ is surjective, then there exists $x \in A$ such that $\phi(x) = (\delta_1^i, \cdots, \delta_n^i)$. Hence $x \equiv 1 \mod \mathfrak{a}_i, x \equiv 0 \mod \mathfrak{a}_j$ whenever $i \neq j$. So

$$(1 - x) + x = 1$$

where $1 - x \in \mathfrak{a}_i, x \in \mathfrak{a}_j$. Hence $\mathfrak{a}_i$ and $\mathfrak{a}_j$ are coprime.

Since $\prod_{i=1}^n (A/\mathfrak{a}_i)$ can be linear represented by $(\delta_j^i)_{j=1}^n, 1 \leq i \leq n$, it is enough to show for any $(\delta_j^i)_{j=1}^n$, there is $x_i \in R$ such that $\phi(x_i) = (\delta_j^i)_{j=1}^n$.

Since $\mathfrak{a}_i$ and $\mathfrak{a}_j$ are coprime for all $j \neq i$, there are equations $x_j + x_i = 1, x_j \in \mathfrak{a}_j, y_j \in \mathfrak{a}_i$

$$\prod_{j \neq i} x_j \equiv 0 \mod \mathfrak{a}_i$$
$$\prod_{j \neq i} x_j = \prod_{j \neq i} (1 - y_j) \equiv 1 \mod \mathfrak{a}_j$$

whenever $i \neq j$. Hence $\phi(\prod_{j \neq i} x_j) = (\delta_j^i)_{j=1}^n$.

(3) $\phi(x) = 0$ means that $x \in \mathfrak{a}_i$ for all $1 \leq i \leq n$. Hence it is equivalent to $x \in \bigcap_{i=1}^n \mathfrak{a}_i$. Hence ϕ is injective $\Leftrightarrow \ker \phi = (0) \Leftrightarrow \bigcap_{i=1}^n \mathfrak{a}_i = 0$.

□

Following are equivalent criteria for primes ideals and maximal ideals

Proposition 1.5. *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 $R/\mathfrak{m}$ 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.

Conversely, if $R/\mathfrak{p}$ is integral 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 $(\mathfrak{m}, x) = (1)$. That means, there exists $y \in R$ such that $xy + m = 1$ for some $m \in \mathfrak{m}$. Obviously, $y \notin m$, so $\bar{x}\bar{y} = \bar{1}$ in $R/\mathfrak{m}$. 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.

□

Theorem 1.6 (Krull's theorem)**.** *If R is a ring and $R \neq 0$, then R has at least one maximal ideal.*

Proof. Since $R \neq 0$, $(0) \in \text{Ideal}(R)$ and $(0) \neq (1)$. We can order $\sum = \text{Ideal}(R) - \{(1)\}$ by inclusion($I_1 \leq I_2$ iff $I_1 \subseteq I_2$). Suppose $\{I_\alpha\}$ be a chain in $\sum$,i.e. $\forall I_\alpha, I_\beta \in \{I_\alpha\}$, $I_\alpha \leq I_\beta$ or $I_\beta \leq I_\alpha$. Denote $\bigcup_\alpha I_\alpha$ by I. I is obviously an ideal and $1 \notin I$ since for each $\alpha, 1 \notin I_\alpha$. Hence $I \in \sum$ and I is upper bound of $\{I_\alpha\}$. By Zorn's lemma, $\sum$ has at least one maximal element, it is an maximal ideal in R by definition. □

Corollary 1.7. *Let R be ring. If $I \lhd R$ and $I \neq (1)$, then I is contained in one maximal ideal.*

Proof. $R/I \neq 0$. By Krull's theorem, R/I has at least one maximal ideal $\bar{\mathfrak{m}}$. Then $\varphi^{\#}(\bar{\mathfrak{m}})$ is maximal ideal which contain I since $\varphi^{\#}$ induce one-to-one correspondence between $\sum_{R/I}$ and set of non-trivial ideals which contain I and $\varphi^{\#}$ preserves order. □

Corollary 1.8. *Any non-unit in R is contained in a maximal ideal.*

Definition 1.11. A ring with only one maximal ideal $\mathfrak{m}$ is called a local ring with maximal ideal $\mathfrak{m}$. Suppose $(R, \mathfrak{m})$ be a local ring with maximal ideal $\mathfrak{m}$. $R/\mathfrak{m}$ is called residue field of R.

Proposition 1.9 (**??**)**.** *(i) Let A be a ring and $\mathfrak{m} \neq (1)$ and ideal of A such that every $x \in A - \mathfrak{m}$ is a unit in A. Then A is local ring and $\mathfrak{m}$ its maximal ideal.*

(ii) Let A be a ring and $\mathfrak{m}$ a maximal ideal of A, such that every element of $1 + \mathfrak{m}$ is a unit. Then A is a local ring.

Proof. (i) Since elements in $A - \mathfrak{m}$ are all units and every ideal not equal to (1) contains non-unit, all maximal ideals are contained in $\mathfrak{m}$. Hence $\mathfrak{m}$ is maximal ideal and the only one.

(ii) Let $x \in A - \mathfrak{m}$. Since $\mathfrak{m}$ is maximal, $(\mathfrak{m}, x) = (1)$. That means there exist $y \in A$ and $m \in \mathfrak{m}$ such that $xy + m = 1$. Hence $xy = 1 - m$ is unit by hypothesis so is x. Hence A is local ring by (i).

□

Definition 1.12. Let R be a ring.

$$\mathbf{Rad}(R) = \big\{r \in R | r \text{ is nilpotent}\big\}$$

is called nilradical of R or simply radical of R.

$$\mathbf{JRad}(R) = \big\{r \in R | \forall y \in R, 1 - ry \text{ is unit}\big\}$$

is called Jacobson radical of R.

Proposition 1.10. **Rad**(R) *is intersection of all prime ideals of R;* **JRad**(R) *is intersection of all maximal ideals of R.*

Proof. If $\mathfrak{p} \lhd R$ is prime, then $R/\mathfrak{p}$ is integral. Hence every $x \notin \mathfrak{p}$ is not nilpotent otherwise $\bar{x}$ in $R/\mathfrak{p}$ is also nilpotent. Hence

$$\mathbf{Rad}(R) \subseteq \bigcap_{\mathfrak{p} \lhd R \text{ is prime}} \mathfrak{p}$$

If x is not nilpotent, then we need to prove that there is prime ideal does not contian x. Let $S = \{1, x, x^2, \cdots\}$ and $\sum$ be the set of ideals that disjoint with S. Since $(0) \in \sum$ and $\sum$ is ordered by inclusion, by Zorn's lemma $\sum$ has maximal element, denote it by $\mathfrak{p}$. We need to prove $\mathfrak{p}$ is a prime ideal.

Let $a \notin \mathfrak{p}, b \notin \mathfrak{p}$. $(a, \mathfrak{p})$ and $(b, \mathfrak{p})$ are not elements in $\sum$ since $\mathfrak{p}$ is maximal. That means there exist $m, n \geq 0$ such that $x^m \in (a, \mathfrak{p}), x^n \in (b, \mathfrak{p})$. It implies

$$x^m = r_1 a + p_1, x^n = r_2 b + p_2 \quad r_1, r_2 \in R$$

Hence $x^{m+n} = r_1 r_2 ab + (r_2 b p_1 + r_1 a p_1 + p_1 p_2) \in (ab, \mathfrak{p})$. Hence $(ab, \mathfrak{p}) \in \sum$ and therefore $ab \in \mathfrak{p}$. Hence $\mathfrak{p}$ is prime ideal and $x \in \mathfrak{p}$.

Let $x \in R$. If there is $y \in R$ such that $1 - xy$ is not unit, then there is a maximal $\mathfrak{m}$. Hence

$$x \notin \bigcap_{\mathfrak{m} \lhd R \text{ is maximal}} \mathfrak{m}$$

If $x \in \mathfrak{m}$ for some maximal ideal $\mathfrak{m}$, then $(x, \mathfrak{m}) = (1)$. That means $1 = rx + m$ for some $r \in R, m \in \mathfrak{m}$. Hence $1 - rx \in \mathfrak{m}$ is not unit. Hence $x \notin \mathbf{JRad}(R)$. □

Here we will introduce some essential facts about prime ideals that used frequently in algebraic geometry.

Proposition 1.11 (**??**). *(i) Let $\mathfrak{p}_1, \cdots, \mathfrak{p}_n$ be prime ideals and α be ideals contained in $\bigcup_{i=1}^n \mathfrak{p}_i$. Then $\mathfrak{a} \subseteq \mathfrak{p}_i$ for some i.*

(ii) Let $\mathfrak{a}_1, \cdots, \mathfrak{a}_n$ be ideals and let $\mathfrak{p}$ be a prime ideal which contains $\bigcap_{i=1}^n \alpha_i$. Then $\mathfrak{a}_i \subseteq \mathfrak{p}$ for some i. In particular, if $\mathfrak{p} = \bigcap_{i=1}^n \mathfrak{a}_i$, then $\mathfrak{p} = \mathfrak{a}_i$ for some i.

Proof. (i) When $n = 1$, it is true obviously.

If it is true that $\mathfrak{a} \nsubseteq \mathfrak{p}_i (1 \leq i \leq n)$ for some $n > 0$ can implies $\mathfrak{a} \nsubseteq \bigcup_{i=1}^n \mathfrak{p}_i$, then for given $\mathfrak{p}_1, \mathfrak{p}_2, \cdots, \mathfrak{p}_{n+1}$, if $\mathfrak{a} \nsubseteq \mathfrak{p}_i (1 \leq i \leq n+1)$, then $\mathfrak{a} \nsubseteq \bigcup_{i \neq j} \mathfrak{p}_i$. So for each $1 \leq j \leq n$, there is $x_j \in \mathfrak{a}$ such that $x_j \notin \mathfrak{p}_i$ whenever $i \neq j$.

Let

$$y = \sum_{j=1}^n x_1 x_2 \cdots \hat{x_j} \cdots x_n$$

Since $\mathfrak{p}_j$ is prime, $x_1 x_2 \cdots \hat{x_j} \cdots x_n \notin \mathfrak{p}_j$. Hence $y \notin \mathfrak{p}_j$ for all $1 \leq j \leq n$. But $y \in \mathfrak{a}$, hence $\mathfrak{a} \nsubseteq \bigcup_{j=1}^n \mathfrak{p}_j$. By induction, it is true for all $n > 0$.

(ii) If $\mathfrak{a}_i \nsubseteq \mathfrak{p}$ for all i, then there are $x_i \in \mathfrak{a}_i$ such that $x_i \notin \mathfrak{p}$ for all i. Since $\mathfrak{p}$ is prime, $x_1, x_2, \cdots, x_n \notin \mathfrak{p}$. But $x_1 x_2 \cdots x_n \in \prod_{i=1}^n \mathfrak{a}_i \subseteq \bigcap_{i=1}^n \mathfrak{a}_i$. Hence $\bigcap_{i=1}^n \mathfrak{a}_i \nsubseteq \mathfrak{p}$. Hence $\bigcap_{i=1}^n \mathfrak{a}_i \subseteq \mathfrak{p} \Rightarrow \mathfrak{a}_i \subseteq \mathfrak{p}$ for some i.

If $\bigcap_{i=1}^n \mathfrak{a}_i = \mathfrak{p}$, then $\mathfrak{p} \subseteq \mathfrak{a}_j$ for all j. But $\mathfrak{a}_j \subseteq \mathfrak{p}$, so $\mathfrak{a}_i = \mathfrak{p}$.

□

Let $I_1 \lhd R, I_2 \lhd R$.

$$(I_1 : I_2) := \{ r \in R | r I_2 \subseteq I_1 \}$$

Examples 1.7. 1) Let $I \lhd R$. $(0 : I) = ((0) : I) = \text{ann}(I)$ is called **annihilator** of I.

If $I = (x)$ is principal ideal, then $\text{ann}((x))$ is shortly denoted by $\text{ann}(x)$, called **annihilator of** x. If x is non-zerodivisor, then $\text{ann}(x) = 0$.

2) Let $R = \mathbb{Z}$, $I_1 = (m), I_2 = (n)$. $m = \prod_{i=1}^n p_i^{\alpha_i}, n = \prod_{i=1}^n p_i^{\beta_i}$ are prime decomposition by $p_1, \cdots, p_n$. Let $\gamma_i = \max\{\alpha_i - \beta_i, 0\}$, then $(I_1 : I_2) = (\prod_{i=1}^n p_i^{\gamma_i})$ and $\prod_{i=1}^n p_i^{\gamma_i} = \frac{m}{(m,n)}$.

Definition 1.13. Let $I \lhd R$.

$$\sqrt{I} = \{ x \in R | x^n \in I \text{ for some } n \}$$

is called radical ideal of I.

Remark 1.8. $\mathbf{Rad}(R) = \sqrt{(0)}$

Proposition 1.12. *$\sqrt{I}$ is the intersection of all primes ideals which contain I.*

Proof.

$$
\begin{aligned}
&x \in \sqrt{I}\\
\Leftrightarrow &\exists n > 0, x^n \in I\\
\Leftrightarrow &\exists n > 0, (\bar{x})^n \textbf{ in } R/I\\
\Leftrightarrow &\bar{x} \in \mathbf{Rad}(R/I) \text{ is intersection of prime ideals in } R/I\\
\Leftrightarrow &x = \varphi^{-1}(\bar{x}) \in \varphi^{\#}(\mathbf{Rad}(R/I)) \text{ is intersection of prime ideals which contain } I \text{ in } R
\end{aligned}
$$

□

Proposition 1.13. *D = set of zero-divisors of $A = \bigcup_{x\neq 0}\sqrt{(ann(x))}$*

Proof. First, $\sqrt{D} = D$ since D is prime.

Next, $\sqrt{\cup_\alpha E_\alpha} = \cup_\alpha \sqrt{E_\alpha}$ for any family of subset of R Hence $D = \sqrt{D} = \sqrt{\bigcup_{x\neq 0}\operatorname{ann}(x)} = \bigcup_{x\neq 0}\sqrt{\operatorname{ann}(x)}$. □

2. Topological properties of prime spectrum

Let R be a ring.

$$\mathrm{Spec}R = \{\text{all prime ideals of } R\}$$

We can give Spec$R$ topology called Zariski topology, which is the origin of modern algebraic geometry. Closed sets of Zariski topology is defined with form

$$V(I) = \{\mathfrak{p} \in \mathrm{Spec}R | I \subseteq \mathfrak{p}\}$$

where I is arbitrary ideal of R.

It is homework to check that these subsets of Spec$R$ satisfy closed set axioms

(1) $V(I_1) \cup V(I_2) = V(I_1 \cap I_2)$
(2) $\bigcap V(I) = V(\sum I)$
(3) $\emptyset = V(1)$ and Spec$R = V(0)$

Examples 2.1. Spec$\mathbb{Z}$

Spec$k[x]$, where k is a algebraic closed field.

$$D(I) = \mathrm{Spec}R \setminus V(I)$$

are used to denote the open sets of Spec$R$ in Zariski topology. In particular, if $I = (f)$ is principal ideal generated by x, then $D(I) = D(f)$ is called a principal open set.

Proposition 2.1. $V(I) = V(\sqrt{I}); D(I) = D(\sqrt{I})$

Proof. If I is contained in a prime ideal $\mathfrak{p}$, then $\forall x \in \sqrt{I}, \exists n > 0, x^n \in I$. So $x^n \in \mathfrak{p}$. Since $\mathfrak{p}$ is prime, $x \cdot x^{n-1} \in \mathfrak{p}$ implies that $x \in \mathfrak{p}$ or $x^{n-1} \in \mathfrak{p}$, then by induction of n, we can conclude that $x \in \mathfrak{p}$. Hence $\sqrt{I} \subseteq \mathfrak{p}$. Hence $V(I) = V(\sqrt{I})$. □

Proposition 2.2. *Principal open subsets of SpecR form topology base of Zariski topology.*

Proof. (1) $\bigcup_{f\in I} = D(I)$ for any open subset $D(I)$ of Spec$R$.
(2) For any ideal J, there is a principal ideal (f) such that $D_f \subseteq D(I)$. For example, we can choose any element f of I.

□

Proposition 2.3. *SpecR is quasi-compact.*

Proof. It is sufficient to prove for any principal open cover $\bigcup_i D_{f_i}$.

$\bigcup_i D_{f_i} = \mathrm{Spec}R$ means $\bigcap_i V(f_i) = V(1)$. Since $\bigcap_i V(f_i) = V(\sum_i (f_i))$, there are elements $r_i \in R$ such that

$$\sum_i r_i f_i = 1$$

and only finite a_i are not 0. Hence the correspondent finite D_{f_k} form a finte cover of Spec$R$. □