

MA-312 Commutative Algebra

1. Ideals – Operation on ideals

All rings we consider in this course are commutative with an identity element, called the *unity*. For a ring A , let \mathcal{J}_A denote the set of ideals in A .

1.1. (Operations on ideals) Let A be a ring and let $\mathfrak{a}, \mathfrak{b}, \mathfrak{c} \in \mathcal{J}_A$.

(1). (Sums, product and intersection) a). The operations sum, intersection and product on \mathcal{J}_A are commutative and associative.

b). (Distributive law) $\mathfrak{a}(\mathfrak{b} + \mathfrak{c}) = \mathfrak{a}\mathfrak{b} + \mathfrak{a}\mathfrak{c}$. (**Remark:** In the ring \mathbb{Z} the operations \cap and $+$ are distributive over each other. This is not the case for general rings.)

c). (Modular law) If $\mathfrak{a} \subseteq \mathfrak{b}$ or $\mathfrak{a} \supseteq \mathfrak{c}$, then $\mathfrak{a} \cap (\mathfrak{b} + \mathfrak{c}) = \mathfrak{a} \cap \mathfrak{b} + \mathfrak{a} \cap \mathfrak{c}$.

d). $(\mathfrak{a} + \mathfrak{b})(\mathfrak{a} + \mathfrak{b}) \subseteq \mathfrak{a}\mathfrak{b}$. (**Remark:** In the ring \mathbb{Z} the equality $(\mathfrak{a} + \mathfrak{b})(\mathfrak{a} + \mathfrak{b}) = \mathfrak{a}\mathfrak{b}$ holds.)

e). $\mathfrak{a}\mathfrak{b} \subseteq \mathfrak{a} \cap \mathfrak{b}$. In particular, $\mathfrak{a} \cap \mathfrak{b} = \mathfrak{a}\mathfrak{b}$ if $\mathfrak{a} + \mathfrak{b} = A$. (Two ideals $\mathfrak{a}, \mathfrak{b}$ are called *coprime* or *comaximal* if $\mathfrak{a} + \mathfrak{b} = A$. Therefore for coprime ideals $\mathfrak{a}, \mathfrak{b}$, we have $\mathfrak{a} \cap \mathfrak{b} = \mathfrak{a}\mathfrak{b}$.)

(2). (Ideal quotient) For two ideals \mathfrak{a} and \mathfrak{b} in A , the ideal quotient of \mathfrak{a} by \mathfrak{b} is $(\mathfrak{a} : \mathfrak{b}) := \{a \in A \mid a\mathfrak{b} \subseteq \mathfrak{a}\}$ which is an ideal in A . In particular, $(\mathfrak{a} : \mathfrak{b})$ is $\{a \in A \mid a\mathfrak{b} = 0\}$ the annihilator of \mathfrak{b} and is denoted by $\text{ann}(\mathfrak{b})$. If \mathfrak{b} is a principal ideal $\mathfrak{b} = Ab$, then we simply write $(\mathfrak{a} : b)$ for $(\mathfrak{a} : \mathfrak{b})$. (In the ring $A = \mathbb{Z}$, let $\mathfrak{a} = \mathbb{Z}m$, $\mathfrak{b} = \mathbb{Z}n$. Then $(\mathfrak{a} : \mathfrak{b}) = \mathbb{Z}q$, where $q = \prod_{p \text{ prime}} p^{r_p}$, $r_p := \max(v_p(m) - v_p(n), 0) = v_p(m) - \min(v_p(m) - v_p(n), 0)$. Therefore $q = m / \gcd(m, n)$.)

For ideals $\mathfrak{a}, \mathfrak{a}_i, i \in I, \mathfrak{b}, \mathfrak{b}_i, i \in I, \mathfrak{c}$ in \mathcal{J}_A , we have

a). $\mathfrak{a} \subseteq (\mathfrak{a} : \mathfrak{b})$. **b).** $(\mathfrak{a} : \mathfrak{b})\mathfrak{b} \subseteq \mathfrak{a}$. **c).** $(\mathfrak{a} : \mathfrak{b}) : \mathfrak{c} = (\mathfrak{a} : \mathfrak{b}\mathfrak{c}) = (\mathfrak{a} : \mathfrak{c}) : \mathfrak{b}$.

d). $(\cap_{i \in I} \mathfrak{a}_i : \mathfrak{b}) = \cap_{i \in I} (\mathfrak{a}_i : \mathfrak{b})$. **e).** $(\mathfrak{a} : \sum_{i \in I} \mathfrak{b}_i) = \sum_{i \in I} (\mathfrak{a} : \mathfrak{b}_i)$.

(3). (Radical of an ideal) For an ideal \mathfrak{a} in A , the radical of \mathfrak{a} is

$$\{a \in A \mid a^n \in \mathfrak{a} \text{ for some } n \in \mathbb{N}^+\}$$

which is an ideal in A and is denoted by $r(\mathfrak{a})$ or $\sqrt{\mathfrak{a}}$.

a). $\mathfrak{a} \subseteq \sqrt{\mathfrak{a}}$. **b).** $\sqrt{\sqrt{\mathfrak{a}}} = \sqrt{\mathfrak{a}}$. **c).** $\sqrt{\mathfrak{a}\mathfrak{b}} = \sqrt{\mathfrak{a} \cap \mathfrak{b}} = \sqrt{\mathfrak{a}} \cap \sqrt{\mathfrak{b}}$ **d).** $\sqrt{\mathfrak{a} + \mathfrak{b}} = \sqrt{\sqrt{\mathfrak{a}} + \sqrt{\mathfrak{b}}}$.

e). $\sqrt{\mathfrak{a}} = A$ if and only if $\mathfrak{a} = A$. **f).** If \mathfrak{p} is a prime ideal in A , then $\sqrt{\mathfrak{p}^n} = \mathfrak{p}$ for all $n \in \mathbb{N}^+$.

(4). (Extensions and contractions) Let $\varphi : A \rightarrow B$ be a ring homomorphism.

For an ideal \mathfrak{a} in A , the extension of \mathfrak{a} in B under φ is the ideal $B\varphi(\mathfrak{a})$ generated by $\varphi(\mathfrak{a})$; (explicitly $B\varphi(\mathfrak{a}) = \{\sum_{j \in J} b_j \varphi(a_j) \mid J \text{ is a finite set, } b_j \in B, a_j \in \mathfrak{a}\}$. — In general, $\varphi(\mathfrak{a})$ need not be an ideal in B , for example, let $\varphi : \mathbb{Z} \rightarrow \mathbb{Q}$ be the natural inclusion and $\mathfrak{a} := \mathbb{Z}n, n \neq 0$.)

For an ideal \mathfrak{b} in B , the contraction of \mathfrak{b} in A under φ is the ideal $\varphi^{-1}(\mathfrak{b})$; (This is always an ideal in A .)

For $\mathfrak{a} \in \mathcal{J}_A$ (resp. $\mathfrak{b} \in \mathcal{J}_B$) the extension $B\varphi(\mathfrak{a})$ of \mathfrak{a} (resp. the contraction $\varphi^{-1}(\mathfrak{b})$ of \mathfrak{b}) is usually denoted by $\mathfrak{a}B$ (resp. $\mathfrak{b} \cap A$), when there is no possibility of confusion over which ring homomorphism is under discussion.

Let $\mathcal{C}_A^B \subseteq \mathcal{J}_A$ (resp. $\mathcal{E}_A^B \subseteq \mathcal{J}_B$) be the set of ideals in A which are contracted to A from B under φ (resp. the set of ideals in B which are extended to B from A under φ), i.e.

$$\mathcal{C}_A^B := \{\mathfrak{b} \cap A \mid \mathfrak{b} \in \mathcal{J}_B\} \quad \text{and} \quad \mathcal{E}_A^B := \{\mathfrak{a}B \mid \mathfrak{a} \in \mathcal{J}_A\}.$$

a). The maps $\mathcal{C}_A^B \rightarrow \mathcal{E}_A^B$, $\mathfrak{a} \mapsto \mathfrak{a}B$ and $\mathcal{E}_A^B \rightarrow \mathcal{C}_A^B$, $\mathfrak{b} \mapsto \mathfrak{b} \cap A$ are inclusion preserving bijective maps which are inverses to each other. (**Hint:** For $\mathfrak{a} \in \mathcal{J}_A$ (resp. $\mathfrak{b} \in \mathcal{J}_B$), $\mathfrak{a} \subseteq \mathfrak{a}B \cap A$, (resp. $\mathfrak{b} \supseteq (\mathfrak{b} \cap A)B$) and hence $\mathfrak{b} \cap A = (\mathfrak{b} \cap A)B \cap A$ and $\mathfrak{a}B = (\mathfrak{a}B \cap A)B$.)

b). The set \mathcal{C}_A^B is closed under intersections and radicals. Further, for ideals $\mathfrak{b}_1, \mathfrak{b}_2 \in \mathcal{J}_B$,

(i) $(\mathfrak{b}_1 + \mathfrak{b}_2) \cap A \supseteq (\mathfrak{b}_1 \cap A) + (\mathfrak{b}_2 \cap A)$. (ii) $(\mathfrak{b}_1 \mathfrak{b}_2) \cap A \supseteq (\mathfrak{b}_1 \cap A)(\mathfrak{b}_2 \cap A)$.

(iii) $(\mathfrak{b}_1 : \mathfrak{b}_2) \cap A \subseteq (\mathfrak{b}_1 \cap A) : (\mathfrak{b}_2 \cap A)$.

c). The set \mathcal{E}_A^B is closed under sums and products. Further, for ideals $\mathfrak{a}, \mathfrak{a}_1, \mathfrak{a}_2 \in \mathcal{J}_A$,

(i) $(\mathfrak{a}_1 \cap \mathfrak{a}_2)B \subseteq (\mathfrak{a}_1 B) \cap (\mathfrak{a}_2 B)$. (ii) $(\mathfrak{a}_1 : \mathfrak{a}_2)B \subseteq (\mathfrak{a}_1 B : \mathfrak{a}_2 B)$. (iii) $\sqrt{\mathfrak{a}B} \subseteq \sqrt{\mathfrak{a}B}$.

d). Suppose that φ is surjective. Then $\mathcal{C}_A^B = \{\mathfrak{a} \in \mathcal{J}_A \mid \text{Ker } \varphi \subseteq \mathfrak{a}\}$ and $\mathcal{E}_A^B = \mathcal{J}_B$. In particular, the map $\{\mathfrak{a} \in \mathcal{J}_A \mid \text{Ker } \varphi \subseteq \mathfrak{a}\} \rightarrow \mathcal{J}_B$, $\mathfrak{a} \mapsto \varphi(\mathfrak{a})$ is inclusion preserving bijective map with inverse $\mathfrak{b} \mapsto \mathfrak{b} \cap A$.

e). Let $\varphi : A \rightarrow A[X]$ be the natural inclusion and let $\pi : A \rightarrow A/\mathfrak{a}$ be the natural surjective map. Let $\eta := \pi[X] : A[X] \rightarrow (A/\mathfrak{a})[X]$ be the ring homomorphism defined by $\sum_{i=0}^n a_i X^i \mapsto \sum_{i=0}^n \pi(a_i) X^i$. Then

1) $\text{Ker } \eta = \mathfrak{a}A[X] = \{\sum_{i=0}^n a_i X^i \in A[X] \mid n \in \mathbb{N}, a_i \in \mathfrak{a} \text{ for all } i = 0, \dots, n\}$.

2) $\mathfrak{a}A[X] \cap A = \mathfrak{a}$. In particular, $\mathcal{C}_A^{A[X]} = \mathcal{J}_A$.

3) For ideals $\mathfrak{a}_1, \dots, \mathfrak{a}_r \in \mathcal{J}_A$ prove that $(\mathfrak{a}_1 \cap \dots \cap \mathfrak{a}_r)A[X] = (\mathfrak{a}_1 A[X]) \cap \dots \cap (\mathfrak{a}_r A[X])$.

1.2. (Prime ideals and maximal ideals) Let A be a ring.

(1). An ideal \mathfrak{p} in A is called a **prime ideal** if $\mathfrak{p} \neq A$ and if $ab \in \mathfrak{p}$ for arbitrary elements a, b in A , then either $a \in \mathfrak{p}$ or $b \in \mathfrak{p}$. The set of all prime ideals in A is denoted by $\text{Spec } A$.

a). For an ideal \mathfrak{p} in A , the following statements are equivalent :

(i) \mathfrak{p} is a prime ideal.

(ii) $A \setminus \mathfrak{p}$ is a multiplicatively closed set in A containing 1.

(iii) The residue class ring A/\mathfrak{p} is an integral domain.

(iv) $\mathfrak{p} \neq A$ and for arbitrary ideal $\mathfrak{a}, \mathfrak{b}$ in A with $\mathfrak{a}\mathfrak{b} \subseteq \mathfrak{p}$, either $\mathfrak{a} \subseteq \mathfrak{p}$ or $\mathfrak{b} \subseteq \mathfrak{p}$.

(2). The set \mathcal{J}_A is ordered by the natural inclusion, i.e. the natural inclusion \subseteq is a partial order on \mathcal{J}_A . An ideal \mathfrak{m} in A is called a **maximal ideal** if it is a maximal element in the partially ordered set $(\mathcal{J}_A \setminus \{A\}, \subseteq)$. Therefore an ideal \mathfrak{m} is a maximal ideal in A if and only if $\mathfrak{m} \neq A$ and if $\mathfrak{a} \in \mathcal{J}_A$ with $\mathfrak{m} \subseteq \mathfrak{a} \subseteq A$, then either $\mathfrak{a} = \mathfrak{m}$ or $\mathfrak{a} = A$. The set of all maximal ideals¹⁾ in A is denoted by $\text{Max } A$.

a). Prove that an ideal \mathfrak{m} in A is a maximal ideal if and only if the residue class ring A/\mathfrak{m} is a field. In particular, every maximal ideal in A is a prime ideal in A , i.e. $\text{Max } A \subseteq \text{Spec } A$.

(3). Let $\varphi : A \rightarrow B$ be a ring homomorphism.

a). If \mathfrak{q} be a prime ideal in B , then the contraction $\mathfrak{q} \cap A$ is a prime ideal in A . If \mathfrak{n} is a maximal ideal in B , then contraction $\mathfrak{n} \cap A$ need not be a maximal ideal in A .

b). Suppose that φ is surjective. Then

¹⁾ Prime ideals and maximal ideals play fundamental role in commutative algebra and algebraic geometry. The following theorem of Krull and its corollaries ensure that there are maximal (and hence prime) ideals, i.e. $\text{Max } A \neq \emptyset$.

Theorem (Krull) Every non-zero ring A has at least one maximal ideal.

Corollary Let \mathfrak{a} be an ideal in A , $\mathfrak{a} \neq A$. Then there exists a maximal ideal in A which contains \mathfrak{a} .

Corollary. Every non-unit in A is contained in some maximal ideal.

i) There a bijecction between the prime ideals of A containing $\text{Ker } \varphi$ onto the set of all prime ideals in B . (**Hint:** In fact, the map $\mathfrak{p} \mapsto \mathfrak{p}B$ is a bijection with inverse $\mathfrak{q} \mapsto \mathfrak{q} \cap A$. See ???)
 ii) Then there a bijecction between the maximal ideals of A containing $\text{Ker } \varphi$ onto the set of all maximal ideals in B . (**Remark:** In the case when φ is injective, the general situation is very complicated. In fact the behavior of prime ideals under extensions of this sort is one of the central problems of *algebraic number theory*.)

c). consider the natural inclusion $\mathbb{Z} \rightarrow \mathbb{Z}[i]$, where $i := \sqrt{-1}$. A prime ideal Zp in \mathbb{Z} may or may not remain prime when it is extended to $\mathbb{Z}[i]$. For example :

- i) The extension of the prime ideal $(Z2)$ to $\mathbb{Z}[i]$ is the square of the prime ideal $(1+i)^2$ in $\mathbb{Z}[i]$.
- ii) Let p be a prime number with $p \equiv 1 \pmod{4}$, then $p\mathbb{Z}[i]$ is a product of two distinct prime ideals in $\mathbb{Z}[i]$. (for example $5\mathbb{Z}[i] = (2+i)(2-i)$.)
- iii) Let p be a prime number with $p \equiv 3 \pmod{4}$, then $p\mathbb{Z}[i]$ is a prime ideal in $\mathbb{Z}[i]$.

1.3. (Nil-radical and Jacobson-radical)

(1). The set of all nilpotent elements in a ring A is an ideal. This ideal is called the nil-radical of A and is denoted by \mathfrak{n}_A .

a). The nil-radical of A is the intersection of all the prime ideal in A . i.e. $\mathfrak{n}_A = \bigcap_{\mathfrak{p} \in \text{Spec } A} \mathfrak{p}$.

(2). The intersection of all maximal ideals in a ring A is called the Jacobson-radical of A and is denoted by \mathfrak{m}_A .

a). For an element $x \in A$, the following statements are equivalent :

- (i) $x \in \mathfrak{m}_A$.
- (ii) For every $a \in A$, $1 - ax$ is a unit in A .

b). Let $P := A[X_i]_{i \in I}$ with $I \neq \emptyset$. Then the Jacobson-radical \mathfrak{m}_P and the nil-radical \mathfrak{n}_P of P are equal. (**Hint:** $1 + X_i \mathfrak{m}_P \subseteq P^\times$.)

c). Let $R := A[[X_1, \dots, X_n]]$, $n \in \mathbb{N}^+$ be the formal power series ring in n indeterminates over A . Then the Jacobson-radical $\mathfrak{m}_R = \{f \in R \mid f(0) \in \mathfrak{m}_A\}$ and the nil-radical $\mathfrak{n}_R = \{f \in R \mid \text{all coefficients of } f \subseteq \mathfrak{n}_A\}$. (**Hint:** Use T??.)

1.4. (Prime avoidance theorem)

a). Let $\mathfrak{p}_1, \dots, \mathfrak{p}_n$ be prime ideals in A and \mathfrak{a} be an ideal in A . Suppose that $\mathfrak{a} \subseteq \bigcup_{i=1}^n \mathfrak{p}_i$. Then show that \mathfrak{a} is conatined in one of the prime ideal \mathfrak{p}_i , i.e. $\mathfrak{a} \subseteq \mathfrak{p}_i$ for some j with $1 \leq j \leq n$. (**Hint:** We may assume that $\mathfrak{p}_i \not\subseteq \mathfrak{p}_j$ for all $i \neq j$ and that \mathfrak{a} is not conatined in any of the \mathfrak{p}_j . Then (see ??) for every $j \in I$ there exists an element $x_j \in (\mathfrak{a} \cap \bigcap_{i \neq j} \mathfrak{p}_i) \setminus \mathfrak{p}_j$. The element $x_1 + \dots + x_n \in \mathfrak{a}$ does not belong to any of the \mathfrak{p}_j a contradiction.)

1.5. (Minimal prime ideals) Let A be a ring and let \mathfrak{a} be an ideal in A . A minimal element in the set $V(\mathfrak{a}) = \{\mathfrak{p} \in \text{Spec } \mathfrak{A} \mid \mathfrak{a} \subseteq \mathfrak{p}\}$ (partially ordered by the inclusion) is called a minimal prime ideal of \mathfrak{a} . A minimal prime ideal of the zero ideal 0 in A is called a minimal prime ideal in A . The set of minimal prrome ideals of \mathfrak{a} is denoted by $\text{Min}(\mathfrak{a})$.

a). Every prime ideal in A containing the ideal \mathfrak{a} in A contains a minimal prime ideal of \mathfrak{a} . (**Hint:** For $\mathfrak{p} \in V(\mathfrak{a})$, the set $\{\mathfrak{p}' \in \text{Spec } A \mid \mathfrak{a} \subseteq \mathfrak{p}' \subseteq \mathfrak{p}\}$ (inductively ordered with respect to the reverse inclusion) has a minimal element with respect to the inclusion.)

b). The radical of the ideal \mathfrak{a} is the intersection of the minimal prime ideals of \mathfrak{a} , i.e. $\mathfrak{a} = \bigcap_{\mathfrak{p} \in \text{Min}(\mathfrak{a})} \mathfrak{p}$.

c). If \mathfrak{a} is a radical ideal, i.e. $\mathfrak{a} = \sqrt{\mathfrak{a}}$, then the set of elements $\{a \in A \mid a \text{ is a zero-divisor in } A/\mathfrak{a}\}$ is the union of the minimal prime ideals of \mathfrak{a} .

- d).** Suppose that A is noetherian. Then the set of minimal prime ideals of \mathfrak{a} is finite. (**Hint:** Let \mathfrak{a} be a maximal in the set of the ideals $\{\mathfrak{a} \mid \text{Min}(\mathfrak{a}) \text{ is not finite}\}$ in A . There exist elements $a, b \in A$ such that $a \notin \mathfrak{a}, b \notin \mathfrak{a}, ab \in \mathfrak{a}$. Now, consider the minimal prime ideals of $\mathfrak{a} + Aa, \mathfrak{a} + Ab$.)
- e).** The prime ideal $\mathfrak{p} \supseteq \mathfrak{a}$ is a minimal prime ideal of \mathfrak{a} if and only if for every $x \in \mathfrak{p}$, there exist a $n \in \mathbb{N}$ and a $s \in A, s \notin \mathfrak{p}$ such that $x^n s \in \mathfrak{a}$. (**Hint:** Pass to the ring $A_{\mathfrak{p}}$.)
- f).** All elements of a minimal prime ideals of A are zero-divisors.

On the other side one can see (simple) test-exercises ; their solutions need not be submitted.

Test-Exercises

T1.1. Let A be a ring, P be the polynomial algebra $A[X_i]_{i \in I}$ and $f = \sum a_\nu X^\nu \in P$.

- a). f is nilpotent if and only if all the coefficients of f are nilpotent.
- b). f is a unit in P if and only if a_0 is a unit in A and all coefficients a_ν , $\nu \neq 0$, of f are nilpotent. (Hint: We may assume that $P = A[X]$. Let $m := \deg f > 0$. It is enough to prove that a_m is nilpotent. But $fg = 1$ with $g = b_0 + \dots + b_n X^n$, and so by induction $a_m^{i+1} b_{n-i} = 0$ for $i = 0, \dots, n$. Variant: Pass to the ring A_S , $S := S(a_m)$, and apply the degree formula.)
- c). (Theorem of McCoy) f is a zero-divisor in P if and only if there exists $a \in A$, $a \neq 0$ such that $af = 0$. (Hint: We may assume that I is finite. First suppose that $P = A[X]$, $fg = 0$, $m := \deg f$, $\deg g > 0$. In the case $a_i g = 0$ for all i the assertion is trivial. Otherwise, let r the maximum of i with $1 \leq i \leq m$ and $a_i g \neq 0$. Then $\deg(a_r g) < \deg g$ and $f \cdot (a_r g) = 0$. — Now, suppose that $n \geq 1$ and $f = \sum_{i=0}^m f_i X_n^i$ with $f_i \in Q := A[X_1, \dots, X_{n-1}]$. If $fg = 0$ with $g \in Q$, $g \neq 0$, then $hg = 0$ for all $h = \sum_{i=0}^m f_i X_{n-1}^{s_i}$ in Q with $s_i \in \mathbb{N}$ arbitrary. Apply the induction hypothesis to h and choose s_i so that s_{i+1} enough bigger than s_i .)
- d). f is idempotent if and only if $f = a_0$ is a constant polynomial and a_0 is idempotent in A . (Hint: We may assume that $P = A[X]$. Since f is idempotent so are a_0 and $(f - a_0)^2$, and hence $(f - a_0)^2 = 0$ and $f = a_0$.)

T1.2. a). Compute the Jacobson-radicals $\mathfrak{m}_{\mathbb{Z}}$, \mathfrak{m}_{A_m} and the nil-radicals $\mathfrak{n}_{\mathbb{Z}}$, \mathfrak{n}_{A_m} , where A_m is a prime ring of characteristic of $m > 0$.

b). Let A_i , $i \in I$, be a family of rings. For the product ring $A = \prod_{i \in I} A_i$, show that $\mathfrak{m}_A = \prod_{i \in I} \mathfrak{m}_{A_i}$ and $\mathfrak{n}_A \subseteq \prod_{i \in I} \mathfrak{n}_{A_i}$ (give example where the inclusion is proper!).

c). Let A be a ring and let B be a finite A -algebra. Then $\mathfrak{m}_A B \subseteq \mathfrak{m}_B$.

T1.3. Let A be a ring, R be the formal power series ring $A[[X]]$ in one indeterminate X over A and $f = \sum_{n=0}^{\infty} a_n X^n \in R$.

- a). If f is nilpotent, then all the coefficients of f are nilpotent. Is the converse true?
- b). f is a unit in R if and only if a_0 is a unit in A .