

Commutative Algebra

Seminar Note

Liyve

2025-06-25*

Abstract

Note about [AM18, *Introduction to Commutative Algebra*].

Table of Contents

1	Rings and Ideals	1
1.1	Rings and Ring Homomorphisms	1
1.2	Ideals and Quotient Rings	2
1.3	Zero-Divisors, Nilpotent Elements and Units	2
1.4	Prime Ideals and Maximal Ideals	3
1.5	Nilradical and Jacobson Radical	4
1.6	Operations on Arbitrary Families of Ideals	6
1.7	Extension and Contraction of Ideals	9
1.8	Spectrum and Zariski Topology	10
1.9	Affine Algebraic Varieties	11
2	Modules	11
2.1	Modules and Module Hom	11
2.2	Submodules and Quotient Modules	12
2.3	Operation of Submodule	12
2.4	Direct Sum and Direct Product	13
2.5	Finitely Generated Module	13

1 Rings and Ideals

1.1 Rings and Ring Homomorphisms

Definition 1.1.1 (Ring). A ring A is a set with two binary operations, usually called addition and multiplication, such that:

1. $(A, +)$ is an abelian group,
2. (A, \cdot) is a semigroup,
3. Multiplication is distributive over addition: for all $a, b, c \in A$, $a \cdot (b + c) = a \cdot b + a \cdot c$ and $(a + b) \cdot c = a \cdot c + b \cdot c$.
4. Multiplication is commutative: for all $a, b \in A$, $a \cdot b = b \cdot a$.
5. There exists a multiplicative identity $1 \in A$ such that for all $a \in A$, $a \cdot 1 = 1 \cdot a = a$.

Definition 1.1.2 (Ring Homomorphism). A ring homomorphism is a mapping $f : A \rightarrow B$ between rings A and B such that for all $a, a' \in A$:

1. $f(a + a') = f(a) + f(a')$,

*Last modified on 2025-06-25.

2. $f(a \cdot a') = f(a) \cdot f(a')$,
3. $f(1_A) = 1_B$.

1.2 Ideals and Quotient Rings

Definition 1.2.1 (Ideal). An ideal \mathfrak{a} of a ring A is a subset $\mathfrak{a} \subseteq A$ such that:

1. $(\mathfrak{a}, +)$ is a subgroup of $(A, +)$,
2. For all $a \in \mathfrak{a}$ and $r \in A$, both ra and ar are in \mathfrak{a} (i.e., \mathfrak{a} is closed under multiplication by elements of A).

Definition 1.2.2 (Quotient Ring). The quotient ring A/\mathfrak{a} is defined as follows: Let A be a ring and \mathfrak{a} an ideal of A . The set of cosets

$$A/\mathfrak{a} = \{a + \mathfrak{a} \mid a \in A\}$$

forms a ring with operations defined by

$$(a + \mathfrak{a}) + (b + \mathfrak{a}) = (a + b) + \mathfrak{a}, \quad (a + \mathfrak{a}) \cdot (b + \mathfrak{a}) = (ab) + \mathfrak{a}.$$

The natural projection $\pi : A \rightarrow A/\mathfrak{a}$ given by $\pi(a) = a + \mathfrak{a}$ is a surjective ring homomorphism with kernel \mathfrak{a} .

Proposition 1.2.3 (Correspondence of Ideals). Let A be a ring and $\mathfrak{a} \triangleleft A$ an ideal. There is a bijective correspondence between the set of ideals of A containing \mathfrak{a} and the set of ideals of the quotient ring A/\mathfrak{a} .

Explicitly, for each ideal \mathfrak{b} of A with $\mathfrak{a} \subseteq \mathfrak{b}$, the image $\bar{\mathfrak{b}} = \mathfrak{b}/\mathfrak{a}$ is an ideal of A/\mathfrak{a} . Conversely, for each ideal $\bar{\mathfrak{b}}$ of A/\mathfrak{a} , its preimage under the natural projection $\pi : A \rightarrow A/\mathfrak{a}$ is an ideal of A containing \mathfrak{a} .

This correspondence preserves inclusion, sums, intersections, and properties such as being prime or maximal (with suitable conditions).

$$\{\mathfrak{b} \triangleleft A \mid \mathfrak{a} \subseteq \mathfrak{b}\} \leftrightarrow \{\bar{\mathfrak{b}} \triangleleft A/\mathfrak{a}\}$$

Definition 1.2.4 (Kernel). Let $f : A \rightarrow B$ be a ring homomorphism. The kernel of f , denoted $\ker f$, is the set

$$\ker f = \{a \in A \mid f(a) = 0_B\}$$

where 0_B is the additive identity in B . The kernel $\ker f$ is an ideal of A .

Definition 1.2.5 (Image). Let $f : A \rightarrow B$ be a ring homomorphism. The image of f , denoted $\operatorname{Im} f$, is the set

$$\operatorname{Im} f = \{f(a) \mid a \in A\}$$

which is a subring of B .

1.3 Zero-Divisors, Nilpotent Elements and Units

Definition 1.3.1 (Zero Divisor). Let A be a ring. An element $a \in A$, $a \neq 0$, is called a **zero-divisor** if there exists a nonzero $b \in A$ such that $ab = 0$ or $ba = 0$.

Definition 1.3.2 (Integral Domain). A ring A is called an **integral domain** if $A \neq \{0\}$ and A has no zero-divisors; that is, for all $a, b \in A$, if $ab = 0$, then either $a = 0$ or $b = 0$.

Definition 1.3.3 (Nilpotent). Let A be a ring. An element $a \in A$ is called **nilpotent** if there exists a positive integer n such that $a^n = 0$.

Definition 1.3.4 (Unit). An element $u \in A$ of a ring A is called a **unit** if there exists $v \in A$ such that $uv = vu = 1$, where 1 is the multiplicative identity in A . The set of all units in A is denoted by A^\times .

Definition 1.3.5 (Principal Ideal). An ideal \mathfrak{a} of a ring A is called a **principal ideal** if there exists an element $a \in A$ such that

$$\mathfrak{a} = (a) = \{ra \mid r \in A\}.$$

That is, \mathfrak{a} is generated by a single element a .

Proposition 1.3.6. Let $A \neq 0$, then TFAE:

1. A is a field
2. the only ideals in A are (0) and $A (= (1))$.
3. $\forall f : A \rightarrow B \neq 0$ is injective.

Proof.

- (1) \implies (2) : Let $\mathfrak{a} \triangleleft A$. If $\mathfrak{a} \neq 0$, then $\exists x$ is a unit, $x \in \mathfrak{a}$
(2) \implies (3) : The kernel $\ker f$ is either $\{0\}$ or A . If $\ker f = A$, then f is the zero map, so $\text{Im } f = \{0\}$, contradicting $B \neq 0$. Thus, $\ker f = \{0\}$, so f is injective.
(3) \implies (1) : Let x be not a unit. $(x) \neq (1)$. Let $B = A/(x)$, $f(x) = 0 \implies x = 0$.

□

1.4 Prime Ideals and Maximal Ideals

Definition 1.4.1 (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 1.4.2 (Maximal Ideal). An ideal \mathfrak{m} in A is maximal if $\mathfrak{m} \neq (1)$ and there is no ideal \mathfrak{a} s.t. $\mathfrak{m} \subsetneq \mathfrak{a} \subsetneq (1)$.

Proposition 1.4.3.

1. \mathfrak{p} is prime ideal $\Leftrightarrow A/\mathfrak{p}$ is integral domain.
2. \mathfrak{m} is maximal ideal $\Leftrightarrow A/\mathfrak{m}$ is field. Hence maximal ideals are prime.
3. Let $f : A \rightarrow B$ is ring homomorphism. \mathfrak{p} is a prime ideal in B , then $f^{-1}(\mathfrak{p})$ is prime in A .

Proof.

- (1)(2) : Omitted. cf.[聂灵沼 21, Ch.3, Sec.4, p.110, thm.7, thm.8]
(3) : You can consider the preimage $f^{-1}(\mathfrak{p}) = \{a \in A \mid f(a) \in \mathfrak{p}\}$. If $xy \in f^{-1}(\mathfrak{p})$, then $f(xy) = f(x)f(y) \in \mathfrak{p}$. Since \mathfrak{p} is prime, $f(x) \in \mathfrak{p}$ or $f(y) \in \mathfrak{p}$, so $x \in f^{-1}(\mathfrak{p})$ or $y \in f^{-1}(\mathfrak{p})$.

In particular, you can consider $A/f^{-1}(\mathfrak{p}) \cong B/\mathfrak{p}$.

□

Remark. Note that if $\mathfrak{m} \triangleleft B$ is maximal, then $f^{-1}(\mathfrak{m})$ is a maximal ideal of A if f is surjective. In general, the preimage of a maximal ideal under a ring homomorphism need not be maximal unless the map is surjective.

Let $f : \mathbb{Z} \rightarrow \mathbb{Q}$ be the natural embedding, $\mathfrak{m} = (0)$. \mathbb{Q} is a field, \mathfrak{m} is maximal, but its preimage $f^{-1}(\mathfrak{m}) = (0)$ in \mathbb{Z} is properly contained in (p) , for any $p \in \mathbb{N}$.

Lemma 1.4.4 (Zorn's lemma). Let S be a non-empty partially ordered set such that every chain (i.e., totally ordered subset) in S has an upper bound in S . Then S contains at least one maximal element; that is, there exists $m \in S$ such that if $m \leq s$ for some $s \in S$, then $m = s$.

Theorem 1.4.5 (Existence of Maximal Ideals). Every nonzero ring A with 1 has at least one maximal ideal.

Proof. Let S be the set of all proper ideals of A , partially ordered by inclusion. S is nonempty since (0) is a proper ideal (as $A \neq 0$). Any chain of ideals in S has an upper bound given by the union of the chain, which is again a proper ideal. By Zorn's Lemma, S has a maximal element, which is a maximal ideal of A .

□

Corollary 1.4.6 (Every Ideal is Contained in a Maximal Ideal). If \mathfrak{a} be a proper ideal of A , then $\exists \mathfrak{m}$ is maximal, s.t. $\mathfrak{a} \subseteq \mathfrak{m}$.

Proof. Let \mathfrak{a} be a proper ideal of A (i.e., $\mathfrak{a} \neq (1)$). Consider the quotient ring A/\mathfrak{a} . By the existence of maximal ideals, A/\mathfrak{a} has a maximal ideal $\bar{\mathfrak{m}}$. The preimage $\mathfrak{m} = \pi^{-1}(\bar{\mathfrak{m}})$ under the natural projection $\pi : A \rightarrow A/\mathfrak{a}$ is a maximal ideal of A containing \mathfrak{a} . \square

Corollary 1.4.7 (Every Non-Unit is Contained in a Maximal Ideal). Every non-unit element of A is contained in some maximal ideal of A . Let $a \in A$ be a non-unit. Then the ideal (a) generated by a is a proper ideal, i.e., $(a) \neq (1)$. By the previous corollary, there exists a maximal ideal \mathfrak{m} such that $(a) \subseteq \mathfrak{m}$. Thus, $a \in \mathfrak{m}$.

Proof. Let S be the set of all proper ideals of A , partially ordered by inclusion. S is nonempty since (0) is a proper ideal (as $A \neq 0$). Any chain of ideals in S has an upper bound given by the union of the chain, which is again a proper ideal. By Zorn's Lemma, S has a maximal element, which is a maximal ideal of A . \square

Definition 1.4.8 (Local Ring). A ring A is called a **local ring** if it has a unique maximal ideal \mathfrak{m} . That is, there exists exactly one maximal ideal in A .

Definition 1.4.9 (Residue Field). Let A be a local ring with unique maximal ideal \mathfrak{m} . The **residue field** of A is the quotient ring

$$k = A/\mathfrak{m}$$

which is a field. The natural projection $A \rightarrow k$ is called the **residue map**.

Proposition 1.4.10.

1. Let A be a ring and $\mathfrak{m} \neq (1)$, s.t. $\forall x \in A \setminus \mathfrak{m}$ is a unit. Then A is a local ring, and \mathfrak{m} is maximal.
2. Let A be a ring and \mathfrak{m} maximal ideal of A , s.t. $1 + \mathfrak{m}$ is a unit of A . Then A is a local ring.

Proof.

- (1) : Every non-unit is contained in \mathfrak{m} . Hence \mathfrak{m} is the only maximal ideal.
- (2) : $\forall \mathfrak{n} \triangleleft A$. If $\mathfrak{n} \not\subseteq \mathfrak{m}$, take $x \in \mathfrak{n} \setminus \mathfrak{m}$. $(x) + \mathfrak{m} = (1)$. $\exists y \in A, m \in \mathfrak{m}, xy + m = 1 \implies xy = 1 - m$ is a unit. Then $\mathfrak{n} = (1)$. Contradiction!

\square

Definition 1.4.11 (Semi-local Ring). A ring A is called **semi-local** if A has only finitely many maximal ideals.

Definition 1.4.12 (PID). An integral domain A is called a **principal ideal domain (PID)** if every ideal of A is principal; that is, for every ideal $\mathfrak{a} \subseteq A$, there exists $a \in A$ such that $\mathfrak{a} = (a) = \{ra \mid r \in A\}$.

Proposition 1.4.13. In PID, \mathfrak{a} is prime $\Leftrightarrow \mathfrak{a}$ is maximal.

Proof. If $(x) \neq (1)$ is prime. Let $(x) \subsetneq (y)$. Then $x \in (y) \implies \exists z$ s.t. $x = yz$. $y \notin (x) \implies z \in (x) \implies \exists t$, s.t. $z = xt$. \square

1.5 Nilradical and Jacobson Radical

Proposition 1.5.1.

1. The set \mathfrak{N} of all nilpotent elements of A is an ideal.

$$\mathfrak{N} = \{a \in A \mid a \text{ is nilpotent}\}$$

2. And A/\mathfrak{N} has no non-zero nilpotent element.

Proof.

- (1) : If $x \in \mathfrak{N}$, then $ax \in \mathfrak{N}$, for $\forall a \in A$. $\forall x, y \in \mathfrak{N}$, $\exists m, n$, $x^m = y^n = 0$, then

$$(x + y)^{m+n-1} = 0 \implies x + y \in \mathfrak{N}.$$

(2) : If $\bar{x}^n = 0$, $x^n \in \mathfrak{N} \implies \exists k, x^{nk} = 0 \implies x \in \mathfrak{N} \implies \bar{x} = 0$.

□

Definition 1.5.2 (Nilradical). The set \mathfrak{N} is called **Nilradical** of A .

Proposition 1.5.3. The nilradical \mathfrak{N} of a ring A is equal to the intersection of all prime ideals of A . That is, an element $a \in A$ is nilpotent if and only if a belongs to every prime ideal of A .

Let

$$\mathfrak{N}' = \bigcap_{\mathfrak{p} \text{ prime}} \mathfrak{p}$$

We need to show $\mathfrak{N} = \mathfrak{N}'$

Proof.

($\mathfrak{N} \subseteq \mathfrak{N}'$) : If $x \in \mathfrak{N}$, then $x^n = 0 \in \mathfrak{p}$ for any \mathfrak{p} . It implies $x \in \mathfrak{p}$ for any \mathfrak{p} .

($\mathfrak{N}' \subseteq \mathfrak{N}$) : Suppose $\forall n > 0, x^n \neq 0$. Let

$$\Sigma = \{\mathfrak{a} \triangleleft A \mid x^n \notin \mathfrak{a}, \forall n > 0\}.$$

Let T be a totally ordered chain in Σ . Consider $\mathfrak{a}_T = \bigcup_{\mathfrak{a} \in T} \mathfrak{a}$. We claim that $\mathfrak{a}_T \in \Sigma$.

- \mathfrak{a}_T is an ideal: Since T is a chain, the union of the ideals in T is again an ideal.
- For all $n > 0$, if $x^n \in \mathfrak{a}_T$, then $x^n \in \mathfrak{a}$ for some $\mathfrak{a} \in T$, contradicting the definition of Σ .

Thus, every chain in Σ has an upper bound, so by Zorn's Lemma, Σ has a maximal element, say \mathfrak{p} . We claim that \mathfrak{p} is a prime ideal.

Suppose $a, b \notin \mathfrak{p}$. Then the ideals $\mathfrak{a}_1 = \mathfrak{p} + (a)$ and $\mathfrak{a}_2 = \mathfrak{p} + (b)$ strictly contain \mathfrak{p} , so by maximality, there exist $n_1, n_2 > 0$ such that $x^{n_1} \in \mathfrak{a}_1$ and $x^{n_2} \in \mathfrak{a}_2$. Thus,

$$x^{n_1} = y_1 + az_1, \quad x^{n_2} = y_2 + bz_2$$

for some $y_1, y_2 \in \mathfrak{p}, z_1, z_2 \in A$. Then

$$x^{n_1+n_2} = (x^{n_1})(x^{n_2}) = (y_1 + az_1)(y_2 + bz_2)$$

Expanding and using that \mathfrak{p} is an ideal, all terms except abz_1z_2 are in \mathfrak{p} , so

$$x^{n_1+n_2} - abz_1z_2 \in \mathfrak{p} \implies x^{n_1+n_2} \in \mathfrak{p} + (ab)$$

Thus, $x^{n_1+n_2} \in \mathfrak{p} + (ab)$, so by maximality, $x^m \in \mathfrak{p} + (ab)$ for some $m > 0$, but $x^m \notin \mathfrak{p}$ by construction, so $ab \notin \mathfrak{p}$.

Therefore, \mathfrak{p} is a prime ideal not containing any power of x , contradicting $x \in \bigcap_{\mathfrak{p} \text{ prime}} \mathfrak{p}$. Thus, $\mathfrak{N} = \mathfrak{N}'$. □

Definition 1.5.4 (Jacobson Radical). Let \mathfrak{R} be the intersection of all maximal ideals of A :

$$\mathfrak{R} = \bigcap_{\mathfrak{m} \text{ maximal}} \mathfrak{m}$$

This ideal is called the **Jacobson radical** of A .

Proposition 1.5.5. $x \in \mathfrak{R} \iff 1 - xy$ is a unit in A for all $y \in A$

Proof. (\implies) : Suppose $x \in \mathfrak{R}$, but $1 - xy$ is not a unit for some $y \in A$. Then the ideal $(1 - xy)$ is proper, so it is contained in some maximal ideal \mathfrak{m} . Thus, $1 - xy \in \mathfrak{m}$. But $x \in \mathfrak{R} \subseteq \mathfrak{m}$, so $xy \in \mathfrak{m}$, hence $1 = (1 - xy) + xy \in \mathfrak{m}$, which is impossible since \mathfrak{m} is proper. Therefore, $1 - xy$ must be a unit for all $y \in A$.

(\impliedby) : Suppose $x \notin \mathfrak{m}$ for some maximal ideal \mathfrak{m} . Then the ideal generated by x and \mathfrak{m} is the whole ring: $(x) + \mathfrak{m} = (1)$. This means there exist $y \in A$ and $t \in \mathfrak{m}$ such that $xy + t = 1$, or equivalently, $1 - xy = t \in \mathfrak{m}$. Since \mathfrak{m} is maximal, $1 - xy$ is not a unit only if it lies in some maximal ideal, but by assumption $x \notin \mathfrak{m}$, so $1 - xy$ cannot be non-invertible. Therefore, if $1 - xy$ is a unit for all $y \in A$, then x must be contained in every maximal ideal, i.e., $x \in \mathfrak{R}$. □

1.6 Operations on Arbitrary Families of Ideals

Let $\{\mathfrak{a}_i\}_{i \in I}$ be a family of ideals in a ring A .

Definition 1.6.1 (Sum of Ideals). The **sum** $\sum_{i \in I} \mathfrak{a}_i$ is defined as:

$$\sum_{i \in I} \mathfrak{a}_i = \{a_1 + a_2 + \cdots + a_n \mid a_k \in \mathfrak{a}_{i_k}, i_k \in I, n \geq 1\}$$

Definition 1.6.2 (Intersection of Ideals). The **product** $\prod_{i \in I} \mathfrak{a}_i$ is defined as:

$$\prod_{i \in I} \mathfrak{a}_i = \left\{ \sum_{k=1}^m a_{1,k} \cdots a_{n,k} \mid a_{j,k} \in \mathfrak{a}_j, m \geq 1 \right\}$$

(For infinite families, the product is usually defined only for finite subfamilies.)

Definition 1.6.3 (Product of Ideals). The **intersection** $\bigcap_{i \in I} \mathfrak{a}_i$ is defined as:

$$\bigcap_{i \in I} \mathfrak{a}_i = \{a \in A \mid a \in \mathfrak{a}_i \text{ for all } i \in I\}$$

1. Distributive law:

$$\mathfrak{a}(\mathfrak{b} + \mathfrak{c}) = \mathfrak{a}\mathfrak{b} + \mathfrak{a}\mathfrak{c}$$

2. Modular law:

$$\mathfrak{a} \cap (\mathfrak{b} + \mathfrak{c}) = \mathfrak{a} \cap \mathfrak{b} + \mathfrak{a} \cap \mathfrak{c}, \text{ if } \mathfrak{a} \supseteq \mathfrak{b} \text{ or } \mathfrak{a} \supseteq \mathfrak{c}$$

In general, we have $\mathfrak{a} + \mathfrak{b}(\mathfrak{a} \cap \mathfrak{b}) \subseteq \mathfrak{a}\mathfrak{b}$. Clearly, $\mathfrak{a}\mathfrak{b} \subseteq \mathfrak{a} \cap \mathfrak{b}$, hence $\mathfrak{a} \cap \mathfrak{b} = \mathfrak{a}\mathfrak{b}$ provided $\mathfrak{a} + \mathfrak{b} = (1)$.

Definition 1.6.4 (Coprime). Let $\mathfrak{a}, \mathfrak{b}$ be ideals of A . We call $\mathfrak{a}, \mathfrak{b}$ are coprime, when $\mathfrak{a} + \mathfrak{b} = A$.

Definition 1.6.5 (Direct Product of Rings). Let $\{A_i\}_{i \in I}$ be a family of rings. The **direct product** $\prod_{i \in I} A_i$ is defined as

$$\prod_{i \in I} A_i := \{(x_i)_{i \in I} \mid x_i \in A_i \text{ for all } i \in I\}$$

with addition and multiplication defined componentwise:

$$(x_i) + (y_i) = (x_i + y_i), \quad (x_i) \cdot (y_i) = (x_i y_i)$$

for all $(x_i), (y_i) \in \prod_{i \in I} A_i$.

Let A_i be rings, and let $p_i : \prod_{j \in I} A_j \rightarrow A_i$ be the projection onto the i -th component, defined by $p_i((x_j)_{j \in I}) = x_i$.

Definition 1.6.6 (Chinese Remainder Map). Let $\{\mathfrak{a}_i\}_{i \in I}$ be a family of ideals of A . Define the canonical ring homomorphism

$$\Phi : A \rightarrow \prod_{i \in I} A/\mathfrak{a}_i, \quad a \mapsto (a + \mathfrak{a}_i)_{i \in I}$$

where each component is the natural projection $\phi_i : A \rightarrow A/\mathfrak{a}_i, a \mapsto a + \mathfrak{a}_i$.

This map Φ is a ring homomorphism, called the **Chinese Remainder map** associated to the family $\{\mathfrak{a}_i\}$.

Proposition 1.6.7. Let $\{\mathfrak{a}_i\}_{i=1}^n$ be a family of ideals of A .

1. $\forall i \neq j, \mathfrak{a}_i, \mathfrak{a}_j$ are coprime, then $\prod_{i=1}^n \mathfrak{a}_i = \bigcap_{i=1}^n \mathfrak{a}_i$.
2. ϕ is surjective $\Leftrightarrow \mathfrak{a}_i, \mathfrak{a}_j$ are coprime.
3. ϕ is injective $\Leftrightarrow \bigcap_{i=1}^n \mathfrak{a}_i = 0$.

Proof. Omitted. cf.[AM18, ch.1, sec.6, p.7, prop.1.10]. □

Theorem 1.6.8 (Chinese Remainder Theorem). Let A be a ring and $\mathfrak{a}_1, \dots, \mathfrak{a}_n$ be ideals of A such that $\mathfrak{a}_i + \mathfrak{a}_j = (1)$ for all $i \neq j$ (i.e., the ideals are pairwise coprime). Then the canonical map

$$\Phi : A \rightarrow \prod_{i=1}^n A/\mathfrak{a}_i, \quad a \mapsto (a + \mathfrak{a}_1, \dots, a + \mathfrak{a}_n)$$

is surjective, and its kernel is $\bigcap_{i=1}^n \mathfrak{a}_i$. Thus,

$$A / \left(\bigcap_{i=1}^n \mathfrak{a}_i \right) \cong \prod_{i=1}^n A/\mathfrak{a}_i$$

as rings.

In particular, if $A = \mathbb{Z}$ and the $\mathfrak{a}_i = (n_i)$ with $\gcd(n_i, n_j) = 1$ for $i \neq j$, then

$$\mathbb{Z}/(n_1 n_2 \cdots n_k) \cong \mathbb{Z}/n_1 \times \cdots \times \mathbb{Z}/n_k.$$

Proof. Let $\Phi : A \rightarrow \prod_{i=1}^n A/\mathfrak{a}_i$ be the canonical map, $a \mapsto (a + \mathfrak{a}_1, \dots, a + \mathfrak{a}_n)$.

- **Kernel:** $\ker \Phi = \bigcap_{i=1}^n \mathfrak{a}_i$, since $a \in \ker \Phi$ iff $a \in \mathfrak{a}_i$ for all i .
- **Surjectivity:** For any $(b_1 + \mathfrak{a}_1, \dots, b_n + \mathfrak{a}_n) \in \prod_{i=1}^n A/\mathfrak{a}_i$, we want $a \in A$ such that $a \equiv b_i \pmod{\mathfrak{a}_i}$ for all i .

Since the ideals are pairwise coprime, for each i there exists $e_i \in A$ such that $e_i \equiv 1 \pmod{\mathfrak{a}_i}$ and $e_i \equiv 0 \pmod{\mathfrak{a}_j}$ for $j \neq i$. (This follows from the Chinese Remainder construction: for each i , let $J_i = \bigcap_{j \neq i} \mathfrak{a}_j$, then $J_i + \mathfrak{a}_i = (1)$, so $1 = x_i + y_i$ with $x_i \in J_i$, $y_i \in \mathfrak{a}_i$; set $e_i = x_i$.)

Then set $a = \sum_{i=1}^n b_i e_i$. For each k , $a \equiv b_k e_k \equiv b_k \pmod{\mathfrak{a}_k}$, since $e_k \equiv 1 \pmod{\mathfrak{a}_k}$ and $e_i \equiv 0 \pmod{\mathfrak{a}_k}$ for $i \neq k$.

Thus, Φ is surjective.

- **Isomorphism:** By the First Isomorphism Theorem, $A/\ker \Phi \cong \text{Im } \Phi = \prod_{i=1}^n A/\mathfrak{a}_i$.

Therefore,

$$A / \left(\bigcap_{i=1}^n \mathfrak{a}_i \right) \cong \prod_{i=1}^n A/\mathfrak{a}_i.$$

□

Remark. The union of ideals is not necessarily an ideal unless one contains the others.

In general, the union $\mathfrak{a} \cup \mathfrak{b}$ fails to be closed under addition. For example, in \mathbb{Z} , the ideals (2) and (3) have union $\{\dots, -6, -4, -3, -2, 0, 2, 3, 4, 6, \dots\}$, but $2 \in (2)$ and $3 \in (3)$, yet $2 + 3 = 5 \notin (2) \cup (3)$.

Proposition 1.6.9.

1. Let $\mathfrak{p}_1, \dots, \mathfrak{p}_n$ be prime ideals and let \mathfrak{a} be an ideal contained in $\bigcup_{i=1}^n \mathfrak{p}_i$. Then $\mathfrak{a} \subseteq \mathfrak{p}_i$ for some i .
2. Let $\mathfrak{a}_1, \dots, \mathfrak{a}_n$ be ideals and let \mathfrak{p} be a prime ideal containing $\bigcap_{i=1}^n \mathfrak{a}_i$. Then $\mathfrak{p} \supseteq \mathfrak{a}_i$ for some i .
If $\mathfrak{p} = \bigcap \mathfrak{a}_i$, then $\mathfrak{p} = \mathfrak{a}_i$ for some i .

Proof. Omitted. cf.[AM18, ch.1, sec.6, p.8, prop.1.11].

□

Definition 1.6.10 (Quotient of Ideals). The set $(\mathfrak{a} : \mathfrak{b}) = \{x \in A \mid x\mathfrak{b} \subseteq \mathfrak{a}\}$ is **quotient** of \mathfrak{a} and \mathfrak{b} . This set is an ideal of A .

If $\mathfrak{b} = (x)$ is a principal ideal of A , then $(\mathfrak{a} : \mathfrak{b})$ is denoted by $(\mathfrak{a} : x)$.

Definition 1.6.11 (Annihilator). The set $(0 : \mathfrak{b}) = \{x \in A \mid x\mathfrak{b} = 0\}$ is called the **annihilator** of \mathfrak{b} . It is denoted by $\text{Ann}(\mathfrak{b})$.

Proposition 1.6.12 (Zero-Divisors). The set of zero-divisors of a ring A is the set

$$D = \{a \in A \mid \exists b \in A, b \neq 0, ab = 0 \text{ or } ba = 0\}.$$

This set is not necessarily an ideal, but it is a union of ideals of A .

$$D = \bigcup_{x \neq 0} \text{Ann}(x),$$

Moreover, it is a union of prime ideals of A .

$$D = \bigcup_{\mathfrak{p} \text{ prime}} \mathfrak{p},$$

where the union is taken over all prime ideals of A .

In particular, every zero-divisor lies in some prime ideal.

Definition 1.6.13 (Radical of an Ideal). Let \mathfrak{a} be an ideal of a ring A . The **radical** of \mathfrak{a} , denoted $\sqrt{\mathfrak{a}}$ or $r(\mathfrak{a})$, is defined as

$$\sqrt{\mathfrak{a}} = \{x \in A \mid \exists n > 0, x^n \in \mathfrak{a}\}$$

That is, x is in the radical of \mathfrak{a} if some power of x lies in \mathfrak{a} . The radical $\sqrt{\mathfrak{a}}$ is itself an ideal of A .

If $\mathfrak{a} = (0)$, then $\sqrt{(0)}$ is the set of all nilpotent elements, i.e., the nilradical of A .

Proposition 1.6.14.

1. $r(\mathfrak{a}) \supseteq \mathfrak{a}$.
2. $r(r(\mathfrak{a})) = r(\mathfrak{a})$.
3. $r(\mathfrak{a}\mathfrak{b}) = r(\mathfrak{a} \cap \mathfrak{b}) = r(\mathfrak{a}) \cap r(\mathfrak{b})$.
4. $r(\mathfrak{a}) = (1) \Leftrightarrow \mathfrak{a} = (1)$.
5. $r(\mathfrak{a} + \mathfrak{b}) = r(r(\mathfrak{a}) + r(\mathfrak{b}))$.
6. If \mathfrak{p} is prime, $r(\mathfrak{p}^n) = \mathfrak{p}$ for all $n > 0$.

Proof. Left to the reader. (Easy to check) □

Proposition 1.6.15.

$$r(\mathfrak{a}) = \bigcap_{\mathfrak{p} \supseteq \mathfrak{a}, \mathfrak{p} \text{ prime}} \mathfrak{p}$$

Hint: Consider nilradical of the quotient ring A/\mathfrak{a} , and the corresponding of ideals.

Proof.1. Let $\pi : A \rightarrow A/\mathfrak{a}$ be the canonical projection. By the Correspondence Theorem, there is a bijection between the set of prime ideals of A containing \mathfrak{a} and the set of prime ideals of A/\mathfrak{a} .

The nilradical of A/\mathfrak{a} , denoted $\mathfrak{N}(A/\mathfrak{a})$, is the intersection of all prime ideals of A/\mathfrak{a} :

$$\mathfrak{N}(A/\mathfrak{a}) = \bigcap_{\bar{\mathfrak{p}} \text{ prime in } A/\mathfrak{a}} \bar{\mathfrak{p}}$$

The preimage of this intersection under π is the intersection of all prime ideals of A containing \mathfrak{a} :

$$\pi^{-1}(\mathfrak{N}(A/\mathfrak{a})) = \bigcap_{\mathfrak{p} \supseteq \mathfrak{a}, \mathfrak{p} \text{ prime}} \mathfrak{p}$$

On the other hand, $\mathfrak{N}(A/\mathfrak{a})$ consists of all elements $\bar{x} = x + \mathfrak{a}$ such that $(x + \mathfrak{a})^n = \mathfrak{a}$ for some $n \geq 1$, i.e., $x^n \in \mathfrak{a}$. Thus,

$$\pi^{-1}(\mathfrak{N}(A/\mathfrak{a})) = \{x \in A \mid x^n \in \mathfrak{a} \text{ for some } n \geq 1\} = r(\mathfrak{a})$$

Therefore,

$$r(\mathfrak{a}) = \bigcap_{\mathfrak{p} \supseteq \mathfrak{a}, \mathfrak{p} \text{ prime}} \mathfrak{p}$$

□

Proof.2. Let $x \in r(\mathfrak{a})$. Then $x^n \in \mathfrak{a}$ for some $n > 0$. For any prime ideal $\mathfrak{p} \supseteq \mathfrak{a}$, since \mathfrak{p} is prime and $x^n \in \mathfrak{p}$, it follows that $x \in \mathfrak{p}$. Thus, x is in every prime ideal containing \mathfrak{a} , so $x \in \bigcap_{\mathfrak{p} \supseteq \mathfrak{a} \text{ prime}} \mathfrak{p}$.

Conversely, suppose $x \notin r(\mathfrak{a})$. Then $x^n \notin \mathfrak{a}$ for all $n > 0$. Consider the quotient ring A/\mathfrak{a} and the image \bar{x} of x . Then $\bar{x}^n \neq 0$ for all $n > 0$. By the proof of the nilradical as intersection of primes, there exists a prime ideal $\bar{\mathfrak{p}}$ of A/\mathfrak{a} not containing any power of \bar{x} . The preimage \mathfrak{p} of $\bar{\mathfrak{p}}$ under the projection $A \rightarrow A/\mathfrak{a}$ is a prime ideal of A containing \mathfrak{a} but not x . Thus, $x \notin \bigcap_{\mathfrak{p} \supseteq \mathfrak{a} \text{ prime}} \mathfrak{p}$.

Therefore, $r(\mathfrak{a}) = \bigcap_{\mathfrak{p} \supseteq \mathfrak{a} \text{ prime}} \mathfrak{p}$. \square

Definition 1.6.16 (Radical of a Subset). More general, let $S \subseteq A$ be any subset of a ring A . The **radical** of S , denoted \sqrt{S} or $r(S)$, is defined as the intersection of all prime ideals of A containing S :

$$\sqrt{S} = \bigcap_{\mathfrak{p} \supseteq S, \mathfrak{p} \text{ prime}} \mathfrak{p}$$

Proposition 1.6.17.

1. $r(\bigcap_{\alpha} E_{\alpha}) = \bigcap_{\alpha} r(E_{\alpha})$.
2. $D = \bigcap_{x \neq 0} r(\text{Ann}(x))$.
3. $r(\mathfrak{a}), r(\mathfrak{b})$ are coprime $\implies \mathfrak{a}, \mathfrak{b}$ are coprime.

1.7 Extension and Contraction of Ideals

Let $f : A \rightarrow B$ be a ring homomorphism.

Definition 1.7.1 (Extension). Given an ideal $\mathfrak{a} \subseteq A$, the **extension** of \mathfrak{a} to B is the ideal

$$\mathfrak{a}^e = f(\mathfrak{a})B = \left\{ \sum_{i=1}^n f(a_i)b_i \mid a_i \in \mathfrak{a}, b_i \in B, n \geq 1 \right\}$$

That is, \mathfrak{a}^e is the ideal of B generated by the image of \mathfrak{a} .

Definition 1.7.2 (Contraction). Given an ideal $\mathfrak{b} \subseteq B$, the **contraction** of \mathfrak{b} to A is the ideal

$$\mathfrak{b}^c = f^{-1}(\mathfrak{b}) = \{a \in A \mid f(a) \in \mathfrak{b}\}$$

Proposition 1.7.3.

1. The extension of an ideal is always an ideal; the contraction of an ideal is always an ideal.
2. If $\mathfrak{a} \subseteq A$, then $\mathfrak{a} \subseteq (\mathfrak{a}^e)^c$.
3. If $\mathfrak{b} \subseteq B$, then $(\mathfrak{b}^c)^e \subseteq \mathfrak{b}$.
4. The set $C = \{\mathfrak{a}^e \mid \mathfrak{a} \triangleleft A\}$, and $E = \{\mathfrak{b}^c \mid \mathfrak{b} \triangleleft B\}$, then $C = \{\mathfrak{a} \mid \mathfrak{a}^{ec} = \mathfrak{a}\}$, and $E = \{\mathfrak{b} \mid \mathfrak{b}^{ce} = \mathfrak{b}\}$.
5. There is a correspondence between ideals of A and ideals of B that are stable under extension and contraction, i.e., there is a bijective between E and C .
6. If f is surjective, then every ideal of B is the extension of its contraction.
7. The contraction of a prime ideal of B is a prime ideal of A .
8. The extension of a prime ideal of A need not be prime in B .

Proof. Left to the reader. (Easy to check) cf.[AM18, ch.1, sec.7, p.10, prop.1.17] \square

1.8 Spectrum and Zariski Topology

This section all of proofs will be omitted, since we have discussed in seminar

Definition 1.8.1 (Spectrum of a Ring). The **spectrum** of a ring A , denoted $\text{Spec } A$, is the set of all prime ideals of A :

$$\text{Spec } A = \{ \mathfrak{p} \subseteq A \mid \mathfrak{p} \text{ is a prime ideal} \}$$

Proposition 1.8.2 (Topology Structure of Spectrum). Let A be a ring and let X be the set of all prime ideals of A . For each subset E of A , let $V(E) = \{ \mathfrak{p} \in \text{Spec } A \mid E \subseteq \mathfrak{p} \}$. Then we have: - If \mathfrak{a} is the ideal generated by E , $V(E) = V(\mathfrak{a}) = V(\text{r}(\mathfrak{a}))$. - $V(0) = \text{Spec } A$; $V(1) = \emptyset$. - $V(\bigcup_{\alpha} \mathfrak{a}_{\alpha}) = \bigcap_{\alpha} V(\mathfrak{a}_{\alpha})$. - $V(\mathfrak{a}) \cup V(\mathfrak{b}) = V(\mathfrak{a} \cap \mathfrak{b}) = V(\mathfrak{a}\mathfrak{b})$.

Definition 1.8.3 (Zariski Topology). The spectrum $\text{Spec } A$ is equipped with the **Zariski topology**, where the closed sets are of the form

$$V(E) = \{ \mathfrak{p} \in \text{Spec } A \mid E \subseteq \mathfrak{p} \}$$

for some subset $E \subseteq A$.

In particular, for an ideal $\mathfrak{a} \subseteq A$, $V(\mathfrak{a}) = \{ \mathfrak{p} \mid \mathfrak{a} \subseteq \mathfrak{p} \}$.

Proposition 1.8.4 (Open set of Spectrum). For each $f \in A$, let X_f denote complement of $V(f)$ in $X = \text{Spec } A$. The basic open sets are complements of $V(f)$ for $f \in A$: X_f . The basic open sets is a basis of Zariski topology.

1. $X_f \cap X_g = X_{fg}$.
2. $X_f = \emptyset \Leftrightarrow f$ is nilpotent.
3. $X_f = X \Leftrightarrow f$ is a unit.
4. $X_f = X_g \Leftrightarrow \text{r}((f)) = \text{r}((g))$.
5. Each X_f is quasi-compact.
6. An open subset of X is quasi-compact if and only if it is a finite union of basic open sets X_{f_1}, \dots, X_{f_n} for some $f_1, \dots, f_n \in A$.

Proposition 1.8.5 (Closures of Spectrum). Denote a prime ideal of A by a letter x or y when thinking of it as a point of $X = \text{Spec } A$. When thinking of x as a prime ideal of A , we denote it by \mathfrak{p}_x .

1. The set $\{x\}$ is closed in $\text{Spec } A \Leftrightarrow \mathfrak{p}$ is maximal.
2. $\overline{\{x\}} = V\mathfrak{p}_x$.
3. $y \in \overline{\{x\}} \Leftrightarrow \mathfrak{p}_x \subseteq \mathfrak{p}_y$
4. X is a T_0 -space.

Remark. The Zariski topology is generally not Hausdorff; its closed sets are typically large. The points corresponding to maximal ideals are called **closed points**.

Proposition 1.8.6 (Irreducible). A topology space X is said **irreducible** if $X \neq \emptyset$ and if every pair of non-empty open sets in X intersect, or equivalently if every non-empty open set is dense in X .

1. $\text{Spec } A$ is irreducible if and only if the nilradical of A is a prime ideal.
2. If Y is an irreducible subspace of X , then the closure \overline{Y} of Y in X is irreducible.
3. Every irreducible subspace of X is contained in a maximal irreducible subspace.
4. The maximal irreducible subspaces of X are closed and cover X . They are called the **irreducible components** of X .
5. The irreducible components of $\text{Spec } A$ are the closed sets $V(\mathfrak{p})$, where \mathfrak{p} is a minimal prime ideal of A .

Remark. Let $A \neq 0$ is ring. Then A has the minimal prime ideal with respect to inclusion. (You can consider Zorn's lemma to prove this remark)

Definition 1.8.7 (Induced Map on Spectra). The map $f : A \rightarrow B$ induces a map on spectra:

$$f^* : \text{Spec } B \rightarrow \text{Spec } A, \quad \mathfrak{q} \mapsto f^{-1}(\mathfrak{q})$$

where $\text{Spec } A$ denotes the set of all prime ideals of A .

1.9 Affine Algebraic Varieties

Let k be a field. An **affine algebraic variety** over k is a subset $V \subseteq k^n$ defined as the common zeros of a set of polynomials:

$$V = V(S) = \{x \in k^n \mid f(x) = 0 \ \forall f \in S\}$$

for some subset $S \subseteq k[x_1, \dots, x_n]$.

The set of all polynomials vanishing on V is an ideal:

$$I(V) = \{f \in k[x_1, \dots, x_n] \mid f(x) = 0 \ \forall x \in V\}$$

There is a correspondence between affine varieties and radical ideals of $k[x_1, \dots, x_n]$ (Hilbert's Nullstellensatz).

The coordinate ring of V is defined as

$$k[V] = k[x_1, \dots, x_n]/I(V)$$

which encodes the algebraic structure of V .

2 Modules

2.1 Modules and Module Hom

Definition 2.1.1 (Module). Let A be a ring. An **A -module** M is an abelian group $(M, +)$ together with an action $A \times M \rightarrow M$, $(a, m) \mapsto am$, such that for all $a, b \in A$ and $m, n \in M$:

1. $a(m + n) = am + an$
2. $(a + b)m = am + bm$
3. $(ab)m = a(bm)$
4. $1m = m$ (if A has 1)

Definition 2.1.2 (Submodule). A **submodule** N of an A -module M is a subgroup $N \leq M$ such that $an \in N$ for all $a \in A$, $n \in N$.

Definition 2.1.3 (Module Homomorphism). Let M, N be A -modules. A map $f : M \rightarrow N$ is an **A -module homomorphism** if for all $m, m' \in M$ and $a \in A$:

- $f(m + m') = f(m) + f(m')$
- $f(am) = af(m)$

The set of all A -module homomorphisms from M to N is denoted $\text{Hom}_A(M, N)$.

Moreover, the set $\text{Hom}_A(M, N)$ forms an abelian group under pointwise addition:

$$(f + g)(m) = f(m) + g(m)$$

for all $f, g \in \text{Hom}_A(M, N)$ and $m \in M$.

If A is commutative, then $\text{Hom}_A(M, N)$ is itself an A -module, with scalar multiplication defined by

$$(af)(m) = a \cdot f(m)$$

for $a \in A$, $f \in \text{Hom}_A(M, N)$, and $m \in M$.

2.2 Submodules and Quotient Modules

Definition 2.2.1 (Quotient Module). If $N \leq M$ is a submodule, the **quotient module** M/N is the abelian group of cosets $m + N$ with A -action $a(m + N) = am + N$.

Theorem 2.2.2 (Correspondence Theorem for Submodules). Let M be an A -module and $N \leq M$ a submodule. There is a bijective correspondence between the set of submodules of M containing N and the set of submodules of the quotient module M/N .

Definition 2.2.3 (Kernel, Image and Cokernel). Let $f : M \rightarrow N$ be an A -module homomorphism.

- The **kernel** is $\ker f = \{m \in M \mid f(m) = 0\}$, a submodule of M .
- The **image** is $\operatorname{Im} f = \{f(m) \mid m \in M\}$, a submodule of N .
- The **cokernel** is $\operatorname{Coker} f = N / \operatorname{Im} f$.

Proposition 2.2.4 (First Isomorphism Theorem). Let $f : M \rightarrow N$ be an A -module homomorphism. Then

$$M / \ker f \cong \operatorname{Im} f$$

as A -modules.

Proof. Define $\varphi : M / \ker f \rightarrow \operatorname{Im} f$ by $\varphi(m + \ker f) = f(m)$. This map is well-defined, A -linear, and bijective. \square

2.3 Operation of Submodule

Let M be an A -module, and let $\{N_i\}_{i \in I}$ be a family of submodules of M .

Definition 2.3.1 (Sum of Submodules). The **sum** of submodules $\{N_i\}$ is defined as:

$$\sum_{i \in I} N_i = \{n_1 + \cdots + n_k \mid n_j \in N_{i_j}, i_j \in I, k \geq 1\}$$

This is the smallest submodule of M containing all the N_i .

Definition 2.3.2 (Intersection of Submodules). The **intersection** of submodules $\{N_i\}$ is:

$$\bigcap_{i \in I} N_i = \{m \in M \mid m \in N_i \text{ for all } i \in I\}$$

This is the largest submodule contained in all the N_i .

Proposition 2.3.3 (Lattice Structure). The set of submodules of M forms a lattice under sum and intersection:

- $N_1 + N_2$ is the least upper bound (join) of N_1 and N_2 .
- $N_1 \cap N_2$ is the greatest lower bound (meet).

Proposition 2.3.4 (Second Isomorphism Theorem). Let M be an A -module, and let N, P be submodules of M . Then

$$(N + P) / P \cong N / (N \cap P)$$

as A -modules.

Proof. Define the map $\varphi : N \rightarrow (N + P) / P$ by $\varphi(n) = n + P$. This is an A -module homomorphism with kernel $N \cap P$, and it is surjective. By the First Isomorphism Theorem, $N / (N \cap P) \cong (N + P) / P$. \square

Proposition 2.3.5 (Third Isomorphism Theorem). Let M be an A -module, and let $N \subseteq P \subseteq M$ be submodules. Then

$$(M / N) / (P / N) \cong M / P$$

as A -modules.

Proof. Consider the natural map $\varphi : M/N \rightarrow M/P$ given by $m + N \mapsto m + P$. This is a well-defined A -module homomorphism with kernel P/N . By the First Isomorphism Theorem, $(M/N)/(P/N) \cong M/P$. \square

Definition 2.3.6 (Submodule Generated by a Subset). Given a subset $S \subseteq M$, the submodule generated by S is:

$$\langle S \rangle = \left\{ \sum_{j=1}^n a_j s_j \mid a_j \in A, s_j \in S, n \geq 1 \right\}$$

This is the smallest submodule of M containing S .

Definition 2.3.7 (Product of Ideal and Submodule). Let A be a ring, M an A -module, $\mathfrak{a} \subseteq A$ an ideal, and $N \leq M$ a submodule. The **product** $\mathfrak{a}N$ is defined as the submodule of M generated by all products an with $a \in \mathfrak{a}, n \in N$:

$$\mathfrak{a}N = \left\{ \sum_{i=1}^k a_i n_i \mid a_i \in \mathfrak{a}, n_i \in N, k \geq 1 \right\}$$

This is the smallest submodule of M containing all elements an with $a \in \mathfrak{a}, n \in N$.

Definition 2.3.8 (Quotient of Submodules). $N, P \leq M$, then $(N : P) := \{ a \in A \mid aP \subseteq N \}$ is an ideal of A .

Definition 2.3.9 (Annihilator of a Module). Let M be an A -module. The **annihilator** of M is

$$\text{Ann}_A(M) := (0 : M) = \{ a \in A \mid am = 0 \text{ for all } m \in M \}$$

which is an ideal of A .

Proposition 2.3.10. If $\mathfrak{a} \subseteq \text{Ann}(M)$, then M is also A/\mathfrak{a} -module. The multiplication defined by $\bar{a}m = am$, It's easy to check well-defined.

Definition 2.3.11. If $\text{Ann}(M) = 0$, then A -module M is faithful.

If $\text{Ann}(M) = \mathfrak{a}$, then M is faithful as a A/\mathfrak{a} -module.

2.4 Direct Sum and Direct Product

Definition 2.4.1 (Direct Sum and Direct Product of Modules). Let $\{M_i\}_{i \in I}$ be a family of A -modules.

- The **direct product** $\prod_{i \in I} M_i$ is the set of all tuples $(m_i)_{i \in I}$ with $m_i \in M_i$, with addition and scalar multiplication defined componentwise.
- The **direct sum** $\bigoplus_{i \in I} M_i$ is the subset of the direct product consisting of tuples $(m_i)_{i \in I}$ such that $m_i = 0$ for all but finitely many i .

Both $\prod_{i \in I} M_i$ and $\bigoplus_{i \in I} M_i$ are A -modules.

2.5 Finitely Generated Module

Definition 2.5.1 (Finitely Generated Module). An A -module M is **finitely generated** if there exist elements $m_1, \dots, m_n \in M$ such that every $m \in M$ can be written as

$$m = a_1 m_1 + \dots + a_n m_n$$

for some $a_1, \dots, a_n \in A$. In other words, $M = \langle m_1, \dots, m_n \rangle$.

Definition 2.5.2 (Free Module). Let A be a ring and S a set. The **free A -module** on S , denoted $F = \bigoplus_{s \in S} A$, is the set of all functions $f : S \rightarrow A$ such that $f(s) = 0$ for all but finitely many $s \in S$. Equivalently, elements of F are finite formal sums

$$\sum_{i=1}^n a_i e_{s_i}$$

where $a_i \in A$, $s_i \in S$, and e_s is the function with $e_s(t) = \delta_{s,t}$.

F is an A -module with addition and scalar multiplication defined componentwise.

If S is finite with n elements, then $F \cong A^n$ as A -modules.

A module M is **free** if it is isomorphic to a free module on some set S ; that is, $M \cong \bigoplus_{s \in S} A$ for some S .

Proposition 2.5.3. An A -module M is finitely generated if and only if there exists an integer $n \geq 0$ and a submodule $N \leq A^n$ such that $M \cong A^n/N$.

Proof Sketch: If M is finitely generated by m_1, \dots, m_n , define a surjective A -module homomorphism $\varphi : A^n \rightarrow M$ by $\varphi(a_1, \dots, a_n) = a_1 m_1 + \dots + a_n m_n$. Then $M \cong A^n / \ker \varphi$. Conversely, any quotient of A^n is finitely generated. \square

Proposition 2.5.4. A quotient of a finitely generated module is finitely generated.

Proof. Hint: Let M be generated by m_1, \dots, m_n and $N \leq M$. Then M/N is generated by the images of m_1, \dots, m_n in M/N . \square

Theorem 2.5.5 (Hamilton-Cayley Theorem). Let M be a finitely generated A -module. Let $\mathfrak{a} \triangleleft A$, and let $\phi : M \rightarrow M$ be an A -module endomorphism such that $\phi(M) \subseteq \mathfrak{a}M$. Then there exist $a_1, \dots, a_n \in \mathfrak{a}$ (for some n) such that

$$\phi^n + a_1 \phi^{n-1} + \dots + a_n = 0$$

as endomorphisms of M .

Proof. Let M be generated by m_1, \dots, m_n . Since $\phi(M) \subseteq \mathfrak{a}M$, for each i ,

$$\phi(m_i) = \sum_{j=1}^n a_{ij} m_j$$

with $a_{ij} \in \mathfrak{a}$. Let $A = (a_{ij})$ be the $n \times n$ matrix over \mathfrak{a} representing ϕ in this basis.

Consider the A -module homomorphism $\Phi : M^n \rightarrow M^n$ given by $\Phi = \phi \cdot I - A$, where I is the identity. By the Cayley-Hamilton theorem for modules, the characteristic polynomial $f(x) = x^n + a_1 x^{n-1} + \dots + a_n$ with $a_i \in \mathfrak{a}$ annihilates ϕ :

$$f(\phi) = \phi^n + a_1 \phi^{n-1} + \dots + a_n = 0$$

as endomorphisms of M . \square

Corollary 2.5.6. Let M be a finitely generated A -module and $\mathfrak{a} \triangleleft A$ such that $\mathfrak{a}M = M$. Then there exists $x \in A$ with $x \equiv 1 \pmod{\mathfrak{a}}$ such that $xM = 0$.

Proof. Take $\phi = \text{id}$. There exists $1 + a_1 + a_2 + \dots + a_n = 0$ since Theorem 2.5.5, let $x = 1 + a_1 + a_2 + \dots + a_n$. \square

Theorem 2.5.7 (Nakayama's lemma). Let M be a finitely generated A -module and $\mathfrak{a} \triangleleft A$, if $\mathfrak{a} \subseteq \mathfrak{R}$, then $\mathfrak{a}M = M$ implies $M = 0$.

Proof. By Corollary 2.5.6, if $\mathfrak{a}M = M$ and $\mathfrak{a} \subseteq \mathfrak{R}$, then there exists $x \in A$ with $x \equiv 1 \pmod{\mathfrak{a}}$ such that $xM = 0$. That is, $x = 1 + a$ for some $a \in \mathfrak{a}$, and $xM = 0$.

But $1 + a$ is a unit in A (since $a \in \mathfrak{R}$ and Proposition 1.5.5). Therefore, x is invertible, so $xM = 0$ implies $M = 0$. \square

Corollary 2.5.8. Let M be a finitely generated A -module, N is a submodule of M , $\mathfrak{a} \triangleleft A$, if $\mathfrak{a} \subseteq \mathfrak{R}$, then $M = \mathfrak{a}M + N$ implies $N = M$.

Proof. Consider the quotient module M/N . Since $M = \mathfrak{a}M + N$, we have

$$M/N = (\mathfrak{a}M + N)/N \cong \mathfrak{a}M/(\mathfrak{a}M \cap N) \subseteq \mathfrak{a}(M/N)$$

so $M/N = \mathfrak{a}(M/N)$. By Theorem 2.5.7, since $\mathfrak{a} \subseteq \mathfrak{R}$ and M/N is finitely generated, it follows that $M/N = 0$, i.e., $M = N$. \square

References

- [AM18] Michael F Atiyah and Ian Grant Macdonald. *Introduction to commutative algebra*. CRC Press, 2018.
- [聂灵沼 21] 聂灵沼. 代数学引论. 高等教育出版社, 2021.