# Commutative Algebra

WENCHAO ZHANG

Bar-Ilan University

*Email:* whzecomjm@foxmail.com

*June 23, 2020*

## Prologue

This Note is originated from a manuscript scanned note when I study Atiyah's book at SUSTC. After some corrections and update, I am trying to rearrange all those issues, including scanned version at SUSTC, texmacs file at SUSTC, scanned version at BIU, and a supplementary notes in 2019. On June 3, 2020, I manage to combine them all into this specific Texmacs file.

More precisely, I changed several times on this file from December 9 2013. We will called that version 1.0. Then on April 10, 2014, I updated some items and corrected some typos. That is version 2. Now this version, we will name it as version 3.

In version 3, I updated all necessary places before chapter 5.

## Table of contents

# 1 Rings and Ideals

In this chapter, we will review some basic definitions and properties of rings. We will discuss about prime ideal, maximal ideal and basic operations between ideals. At the end of the chapter, we will introduce Grothendieck's schemes languages (cf. Exercises of Chapter 1 in Atiyah's book).

## 1.1 Rings and ring homomorphisms

We assume all rings are commutative except for a specific requirement for certain content.

**Definition 1.1. (ring)** *A ring $A$ is a set with two binary operations (addition and multiplication) such that*

1. *$A$ is an abelian additive group,*
2. *Multiplication is associative and distributive over addition,*
3. *There exists $1 \in A$, such that $x1 = 1x = x$ for all $x \in A$,*
4. *(commutative) all elements are commutative.*

**Definition 1.2. (ring homomorphism)** *In a word, A ring homomorphism is a map between two rings, which respects addition, multiplication and the identity element.*

## 1.2 Ideals and quotient rings

**Definition 1.3. (ideal)** *An ideal $\alpha$ is an additive subgroup of a ring $A$, which satisfies $A\alpha \subseteq \alpha$.*

The multiples $ax$ of an element $x \in A$ form a *principal ideal* denoted by $(x)$ or $Ax$.

**Remark 1.4.** Since the quotient group $A/\alpha$ inherits a uniquely defined multiplication from $A$ which makes it into a ring, called the *quotient ring $A/\alpha$*.

**Remark 1.5.** The mapping $\varphi: A \rightarrow A/\alpha$ taking $x \in A$ into $x + \alpha$ is a surjective ring homomorphism.

**Proposition 1.6.** *There is a one-to-one order-preserving correspondence between the ideals $b$ of ring $A$ which contains $\alpha$, and the ideals $\bar{b}$ of $A/\alpha$, given by $b = \varphi^{-1}(\bar{b})$, where $\varphi: A \to A/\alpha$.*

**Note 1.7.** 上述命题说明环$R$中包含理想 $\alpha$ 的理想与‘模去’$\alpha$ 的理想是一对一的，并且对应的关系就是 $\varphi^{-1}$.

## 1.3 Zero-divisors, nilpotent elements, units

**Definition 1.8. (zero-divisor)** *A zero-divisors in a ring $A$ is an element $x$, if there exists $0 \neq y \in A$, such that $xy = 0$.*

0 is always a zero-divisor, so we usually consider non-zero zero-divisors in a ring.

**Definition 1.9. (integral domain)** *A nontrivial ring with non nonzero zero-divisors is called an integral domain.*

**Definition 1.10. (nilpotent)** *An element $x \in A$ is called nilpotent if $x^n = 0$ for some integer $n > 0$.*

A nilpotent element is a zero-divisor but not conversely. We call an element $u$ a *unit* of ring if it is invertible in the ring, i.e. there exists $x \in A$, s.t. $ux = xu = 1$.

**Remark 1.11.** All units in a (commutative) ring forms a multiplicative Abelian group.

**Proposition 1.12. (ring as field)** *Let $A$ be a nonzero ring, the following are equivalent (TFAE):*

- *$A$ is a field;*
- *The only ideals of $A$ are $(0) =: 0$ and $(1) = A$;*
- *Every ring homomorphism of $A$ into a non-zero ring $B$ is* ***injective****.*

## 1.4 Prime ideals and Maximal Ideals

**Definition 1.13.** *A ideal $\wp$ in $A$ is prime if $\wp \neq (1)$ and if $xy \in \wp \Rightarrow x \in \wp$ or $y \in \wp$.*

**Proposition 1.14.** *$A$ is an integral domain $\Leftrightarrow$ 0 is prime in $A$.*

**Proof.** "$\Rightarrow$" If $A$ is an integral domain, then there is no nonzero zero-divisor. That is to say, for any $x, y \in A$, with $xy = 0$, it follows that $x = 0$ or $y = 0$. This defined exactly 0 is a prime ideal.

"$\Leftarrow$" If 0 is prime in $A$, then for any $xy = 0$, it follows $x = 0$ or $y = 0$. This means that there is no nonzero zero-divisors in $A$, hence $A$ is an integral domain. □

**Corollary 1.15.** *An ideal $\wp$ in $A$ is prime if and only if $A / \wp$ is a integral domain.*

**Proof.** Consider a ring homomorphism $f: A \rightarrow A / \wp$, with $a \mapsto \bar{a}$. Note that $a \in \wp \Leftrightarrow \bar{a} = 0$, hence 0 is prime in $A / \wp$. By Proposition 1.14, it equivalent to $A / \wp$ is an integral domain. Vice verse. □

**Proposition 1.16.** *If $f: A \rightarrow B$ is a ring homomorphism, $\wp$ is a prime ideal of $B$, then $f^{-1}(\wp)$ is also a prime ideal of $A$.*

**Proof.** $A / f^{-1}(\wp) \cong B / \wp$, because $B / \wp$ has no nonzero zero divisor hence $A / f^{-1}(\wp)$ has no zero divisor either. Hence, $f^{-1}(\wp)$ is prime. □

**Remark 1.17.** The inverse image of a maximal ideal is not always maximal. However, if $f$ is *surjective*, then the inverse image of a maximal ideal is also maximal.

Note that if $f$ is not surjective, then there could be an ideal larger than the inverse image. Here is an example. Consider and embedding homomorphism $f: \mathbb{Z} \rightarrow \mathbb{Q}$, $\mathfrak{m} = (0)$ is a maximal ideal of $\mathbb{Q}$, but not a maximal ideal of $\mathbb{Z}$.

**Theorem 1.18.** **(Krull's theorem (1929))** *Every ring with an identity element $A$ has at least one maximal ideal.*

**Corollary 1.19.** *If $\alpha \neq (1)$ is an ideal of $A$, then there exists a maximal ideal of $A$ contains $\alpha$.*

**Corollary 1.20.** *Every non-unit of $A$ is contained in a maximal ideal.*

**Remark 1.21.** In a commutative ring with unity, all maximal ideals are prime.

**Proof.** If $R$ is a maximal ideal of $A$, then $A / R$ contains no proper ideal by Proposition 1.6. We just need to show $A / R$ is an integral domain because of Corollary 1.15. Hence every element in $A / R$ is a unit, otherwise it will generate a proper principal ideal of $A / R$. Thus $A / R$ is a field, hence a integral domain. □

From this remark, we obtain a similar result of Corollary 1.15 for the relation between a maximal ideal and field.

**Proposition 1.22.** *An ideal $\mathfrak{m}$ in $A$ is maximal if and only if $A/\mathfrak{m}$ is a field.*

We seldom consider the minimal ideals except 0 ideal. In fact we have following proposition on the minimal prime ideals with respect to inclusion.

**Proposition 1.23.** *A nontrivial commutative ring $A$ has minimal prime ideals with respect to inclusion.*

**Proof.** Let $\Sigma$ be the set of all prime ideals of $A \neq 0$. Order $\Sigma$ by division. $\Sigma$ is not empty, since $0 \in \Sigma$. To apply Zorn's Lemma, we must know that every chain in $\Sigma$ has an upper bound with respect to division in $\Sigma$. Let $\wp_i$ $(i \in I)$ be a chain of prime ideals of $\Sigma$, such that each pair of indices $i, j$ we have either $\wp_i | \wp_j$(i.e. $\wp_i \supset \wp_j$) or $\wp_j | \wp_i$. Let $\mathfrak{P} = \cap_{i \in I} \wp_i$. Then $\mathfrak{P}$ is a prime ideal (How to Prove? Find a contradiction to division of each two prime ideals) and $\mathfrak{P} | \wp_i$, i.e. $\mathfrak{P}$ is a upper bound of chains with respect to division. But for inclusion, we have minimal elements for any prime ideals chain. □

**Definition 1.24. (local ring)** *A ring with only one maximal ideal is called local ring. The field $k = A/m$ is called the residue field of $A$. A ring with only a finite number of maximal ideals is called semi-local.*

**Proposition 1.25.**

*i. Let $A$ be a ring and $\mathfrak{m} \neq (1)$ an ideal of $A$ s.t. every $x \in A - \mathfrak{m}$ is a unit in $A$. then $A$ is a local ring and $m$ is maximal;*

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

**Example 1.26.** The ideal $\mathfrak{m}$ of all polynomial in $A = k[x_1, \dots, x_n]$ with zero constant term is maximal.

**Definition 1.27. (PID)** *A principal ideal domain is an integral domain in which every ideal is principal.*

**Proposition 1.28.** *All nonzero prime ideal of a PID is maximal.*

**Proof.** Suppose $(p)$ is a nonzero prime ideal of the PID $A$. If there exists an ideal $(q) \supseteq (p)$, then $p \in (p) \subseteq (q)$, hence there exists $a \in A$, s.t. $p = qa$. Since $p \in (p)$, we have either $q \in (p)$ or $a \in (p)$.

If $q \in (p)$, then it follows that $(q) \subseteq (p)$, and hence $(q) = (p)$.

If $a \in (p)$, then there exists $b \in A$, s.t. $a = pb$, and hence $p = qa = qpb = pqb$. Since $A$ is a domain and $p \neq 0$, we have $1 = qb$. This yields that $q$ is a unit, and hence $(q) = A$.

In summary, we observe that whenever $(p) \subseteq (q) \subseteq A$, we have either $(p) = (q)$ or $(q) = A$. Thus $(p)$ is a maximal ideal of $A$. □

## 1.5 Nilradical and Jacobson radical of rings

**Proposition 1.29.** *The set $\mathfrak{N}$ of all nilpotent element in a ring $A$ form an ideal, and $A/\mathfrak{N}$ has no nonzero nilpotent element.*

**Definition 1.30. (nilradical)** *The ideal of all nilpotent elements is called the nilradical of $A$.*

**Proposition 1.31.** *The nilradical of $A$ is **intersection of all prime ideals** of $A$.*

**Definition 1.32. (Jacobson radical)** *The Jacobson radical $\mathfrak{R}$ of $A$ is defined to be the intersection of all maximal ideals of $A$.*

**Proposition 1.33.** $x \in \mathfrak{R} \Leftrightarrow \forall y \in A, 1 - xy$ *is a unit in $A$.*

**Example 1.34.** If $A$ is a commutative ring with 1, $f(x) = a_0 + a_1 x + \cdots + a_n x^n \in A[x]$. Then

1. $f$ is a unit in $A[x] \Longleftrightarrow a_0$ is a unit in $A$ and $a_1, \ldots, a_n$ are nilpotent in $A$.

2. $f$ is nilpotent $\Longleftrightarrow a_0, a_1, \ldots, a_n$ are nilpotent.

3. $f$ is an zero-divisor $\Longleftrightarrow \exists 0 \neq a \in A$, s.t. $af = 0$.

4. The nilradical and Jacobson radical of $A[x]$ are the same.

## 1.6 Operations on ideals

The addition and multiplication of ideals are defined as follows:

**Definition 1.35. (addition and multiplication of ideals)**

- $\mathfrak{a} + \mathfrak{b} := (\mathfrak{a}, \mathfrak{b})$, *then* $\mathfrak{a} + \mathfrak{a} = (\mathfrak{a}, \mathfrak{a}) = \mathfrak{a}$.

- *$a \cap b$ with respect to inclusion of sets is an ideal.*

- *$ab := \{\sum x_1 x_2; \forall x_1 \in a, \forall x_2 \in b\}$ (finite sum) is generated by all product $x_1 x_2$.*

- *$a^n = \prod a$.*

Since the intersection of any family of ideals is an ideal, the ideal of $A$ form a complete lattice with respect to inclusion.

**Definition 1.36. (coprime)** *If two primes $a, b$ satisfy $a + b = (1)$, then we call they are coprime.*

**Proposition 1.37.** *Note that $ab \subseteq a \cap b$. If $a, b$ are coprime ideals, then $ab = a \cap b$.*

**Proof.** Note that for any $\alpha_1, \alpha_2 \in a$, $\beta_1, \beta_2 \in b$, then $\alpha_1 \beta_1 + \alpha_2 \beta_2 \subseteq a \cap b + a \cap b = a \cap b$. For any finite sum of product of $\alpha_i \beta_i$ is then inside $a \cap b$. Thus $ab \subseteq a \cap b$.

$(a + b)(a \cap b) = a\,(a \cap b) + b\,(a \cap b) \subseteq ab + ab = ab$, if $a + b = (1)$, then $a \cap b \subseteq ab$. On the other hand, $ab \subseteq a \cap b$. Hence, $ab = a \cap b$. □

**Definition 1.38. (direct product)** *$A = \Pi_{i=1}^n A_i$ is the set of all sequences $x = (x_1, x_2, \ldots, x_n)$ with $x_i \in A_i\,(1 \leqslant i \leqslant n)$ and component-wise addition and multiplication.*

The direct product of commutative ring with 1 are a commutative ring with identity $(1, 1, \cdots, 1)$.

Let $A$ be a ring and $\alpha_1, \alpha_2, \ldots, \alpha_n$ ideals of $A$. Define a homomorphism

$$\begin{aligned} \phi\colon \quad A &\longrightarrow \prod_{i=1}^{n} (A/\alpha_i) \\ x &\longmapsto (x + \alpha_1, x + \alpha_2, \ldots, x + \alpha_n) \end{aligned}$$

This is a way to map a commutative ring with 1 to the direct product of several quotient rings, which is stemmed from the idea from ancient Chinese method, say Chinese reminder theorem.

We have a proposition as follows:

**Proposition 1.39.**

*i. If $\alpha_i, \alpha_j (\forall i \neq j)$ are mutually coprime, then $\Pi \alpha_i = \cap \alpha_i$;*

*ii. $\phi$ is surjective $\Leftrightarrow$ $\alpha_i, \alpha_j (\forall i \neq j)$ are mutually coprime;*

*iii.* $\phi$ *is injective* $\Leftrightarrow \cap \alpha_i = 0$.

**Proposition 1.40.**

1. *Let* $\wp_1, \ldots, \wp_n$ *be prime ideals of* $A$ *and let* $a$ *be an ideal contained in* $\cup_{i=1}^n \wp_i$, *then there exists* $i$, *such that* $a \subset \wp_i$.

2. *Let* $a_1, a_2, \ldots, a_n$ *be ideals of* $A$ *and let* $\wp$ *be a prime ideal containing* $\cap_{i=1}^n a_i$, *then there exists* $i$, *such that* $\wp \supset a_i$. *In particular, if* $\wp = \cap_{i=1}^n a_i$, *then there exists* $i$ *such that* $\wp = a_i$.

**Definition 1.41. (ideal quotient, annihilator)** *If* $a$,$b$ *are ideals of* $A$, *then ideal quotient is* $(a\colon b) = \{x \in A{:}x b \subset a\}$, *which is an ideal. In particular,* $(0\colon b)$ *is called the annihilator of* $b$ *and is also denoted as* $\operatorname{Ann}(b)$.

**Remark 1.42.** In this notation, we have the set of all zero-divisors $D$ in $A$ is $D = \bigcup_{x \neq 0} \operatorname{Ann}(x)$, where $\operatorname{Ann}(x) = \operatorname{Ann}((x))$.

**Definition 1.43. (radical)** *If* $a$ *is any ideal of* $A$, *then radical of* $a$ *is*

$$r(a) = \{x \in A\colon x^n \in a \,\text{for some}\, n > 0\}$$

**Proposition 1.44.** *The radical of ideal* $a$ *is the* **intersection of the prime ideals which contains** $a$.

**Definition 1.45. (torsion element)** *An element* $x$ *is a torsion element if* $\operatorname{Ann}(x) \neq 0$.

**Proposition 1.46.** $D := \text{set of zero divisors of } A = \cup_{x \neq 0} \operatorname{Ann}(x) = \cup_{x \neq 0} r(\operatorname{Ann}(x))$.

**Proposition 1.47.** *Let* $a, b$ *be ideal of a ring* $A$ *such that* $r(a)$, $r(b)$ *are coprime, the* $a, b$ *are coprime.*

**Exercise 1.1. (Properties of radical)**

i. $r(a) \supseteq a$;

ii. $r(r(a)) = r(a)$;

iii. $r(a b) = r(a \cap b) = r(a) \cap r(b)$;

iv. $r(a) = (1) \Leftrightarrow a = (1)$;

v. $r(a + b) = r(r(a) + r(b))$;

vi. $r(\wp^n) = \wp$, $\forall n > 0$.

## 1.7 Extension and contraction of ideal

**Definition 1.48. (extension and contraction of ideal)** *Let $f$: $A \to B$ is a ring homomorphism, the extension $a^e$ of an ideal $a$ in $A$ is the ideal $Bf(a)$; the contraction $b^c$ of an ideal of $B$ is inverse image of $b$, i.e. $f^{-1}(b)$ (naturally defined, which is always an ideal of $A$).*

**Remark 1.49.** $f(a)$ is not necessarily an ideal of $B$, so we have to define extension of ideal. If $b$ is prime, then so is $b^c$, but $b^e$ may not be prime ($f{:}\,\mathbb{Z}\to\mathbb{Q}, b\neq 0, b^e=\mathbb{Q}$).

**Example 1.50.** $f{:}\,\mathbb{Z}\to\mathbb{Z}[i]$. $\mathbb{Z}[i]$ is a PID and the situation is as follows:

i. $(2)^e=((1+i)^2)$ is a square of a prime in $\mathbb{Z}[i]$.

ii. If $p\equiv 1(\bmod 4)$, then $(p)^e$ is the product of two distinct prime ideals. $(5)^e=(2+i)(2-i)$.

iii. If $p\equiv 3(\bmod 4)$, then $(p)^e$ is prime in $\mathbb{Z}[i]$.

**Note 1.51.** If $p\equiv 1(\bmod 4)$, then it can be expressed as sum of two integer squares, e.g. $97=9^2+4^2$.

**Proposition 1.52.**

*i.* $a\subset a^{ec}, b\supset b^{ce}$*;*

*ii.* $b^c=b^{cec}, a^e=a^{ece}$;

## 1.8 Construction of an algebraic closure of a field (E. Artin)

Let $K$ be a field and let $\Sigma\subseteq K[x]$ be the set of all irreducible monic polynomial. For each $f\in\Sigma$, define $A$ to be the polynomial ring generated by indeterminate $x_f$. Let $a$ be the ideal of $A$ generated by the polynomials $f(x_f)$ for all $f\in\Sigma$, i.e., $A=K[x_{f_1},\ldots,x_{f_i},\ldots]$, $a=(f_1(x_{f_1}),\ldots,f_i(x_{f_i}),\ldots)$.

Suppose $a=A$, then there are $f_1,\ldots,f_n\in\Sigma$ and $g_1,g_2,\ldots,g_n\in A$. such that

$$g_1f_1(x_{f_1})+g_2f_2(x_{f_2})+\ldots+g_nf_n(x_{f_n})=1 \tag{1.1}$$

Let $K'$ be a field containing $K$ and roots $\alpha_i$ of $f_i$, then letting $x_{f_i}=\alpha_i$ in [1.1], we yield $0=1$ in $K'$, Hence we may assume $a$ a proper ideal of $A$.

Let $m$ be a maximal ideal of $A$ containing $a$, and let $K_1 = A/m$. Then $K_1$ is an extension field of $K$ in which each $f \in \Sigma$ has a root. Repeat the process with $K_1$ in place of $K$, obtaining $K_2$, and so on. Let $L = \cup_{n=1}^{\infty} K_n$. Then $L$ is a field in which each $f \in \Sigma$ splits completely into linear factors. Let $\bar{K}$ be the set of all elements of $L$ which are algebraic over $K$. Then $\bar{K}$ is an algebraic closure of $K$.

## 1.9 The prime spectrum of rings

**Definition 1.53. (prime spectrum)** *Let $A$ be a ring and $X$ be the set of all prime ideals on $A$. For each subset $E \subset A$, Let $V(E)$ denote the set of all prime ideals contains $E$. Then*

*i. If $\alpha$ is an ideal generated by $E$, then $V(\alpha) = V(E) = V(r(\alpha))$;*

*ii. $V(0) = X, V(1) = \varnothing$;*

*iii. $V(\bigcup_{i \in I} E_i) = \bigcap_{i \in I}(V(E_i))$;*

*iv. $\forall a, b$ are ideals, $V(a \cap b) = V(ab) = V(a) \cup V(b)$.*

*The resulting topology is called the* ***Zariski topology****. The topological space $X(A, V)$ is called the* ***prime spectrum*** *of $A$ and written by* **Spec($A$)**. *The set $V(E)$ are all closed sets.*

There exists another view of prime spectrum, $X_f = X - V(f)$ are open set and form a basis of open sets for the Zariski topology.

**Proposition 1.54.** *$X = \mathrm{Spec}(A)$ is quasi-compact.*

***Proof.*** *Let $\Lambda$ be an indexing set and $\{U_\lambda\}_{\lambda \in \Lambda}$ be an open cover for* Spec($A$). *For every $\lambda \in \Lambda$, then $U_\lambda = \mathrm{Spec}(A) - V(f_\lambda) = X_{f_\lambda}$. Hence, we have*

$$\begin{aligned}
\mathrm{Spec}(A) &= \bigcup_{\lambda \in \Lambda} U_\lambda \\
&= \bigcup_{\lambda \in \Lambda} (X - V(f_\lambda)) \\
&= X - \bigcap_{\lambda \in \Lambda} V(f_\lambda) \\
&= X - V\Big(\bigcup_{\lambda \in \Lambda} f_\lambda\Big) \\
&= X - V(\alpha)
\end{aligned}$$

*where $\alpha$ is the ideal generated by the union. It follows that $V(\alpha) = \varnothing$. i.e. $A = \alpha$. Then $\{f_\lambda\}$ generate $A$. we can write $1 = \sum_{\lambda=1}^{n} a_\lambda f_\lambda$ for finite sum. Working backwards, $X$ is quasi-compact.* □

**Remark 1.55.** *If we have infinite ideals generate the unit ideal, then there must have a finite number of those ideals such that they generate the unit ideal.* we have used this statement at [1.1] in 1.8.

**Proposition 1.56.** Spec($A$) *is irreducible if and only if the nilradical is a prime ideal of $A$.*

***Proof.*** *Suppose that* Spec($A$) *is not irreducible. Choose nonempty open sets $U, V$ such that $U \cap V = \varnothing$. Then there exists $f, g$ for which $\varnothing \neq X_f \subset U, \varnothing \neq X_g \subset V$, then $X_{fg} = X_f \cap X_g = \varnothing$. hence $fg$ is nilpotent, since nilradical is prime, then $f$ or $g$ must have one which is nilpotent, i.e. $X_f = \varnothing$ or $X_g = \varnothing$. The contradiction shows that* Spec($A$) *is irreducible.*

*Suppose the nilradical is not a prime ideal, then there are $fg \in \mathfrak{N}$, but $f$, $g \notin \mathfrak{N}$. Hence $X_f$ and $X_g$ are nonempty sets, and $X_f \cap X_g = X_{fg} = \varnothing$. Hence,* Spec($A$) *is not irreducible.* □

***Note* 1.57.** *A topological space is irreducible if $X \neq \varnothing$ and if every pair of non-empty open sets in $X$ intersect, or equivalently if every non-empty open set is dense in $X$.*

**Proposition 1.58. (Category of Spectrums)** *Let $\phi: A \to B$ be a ring homomorphism. $X =$* Spec($A$)*, $Y =$* Spec($B$)*. Since for any prime ideal $q \in Y$, then $\phi^{-1}(q)$ is a prime ideal of $A$, i.e. a prime ideal of $X$. Hence, $\phi$ induces a morphism $\phi^*: Y \to X$.*

# 2 Modules

**Definition 2.1. (Module)** *An **A-module** $M$ is an additive abelian group on which $A$ acts linearly. More precisely, it's a pair $(M,\mu)$ such that $M$ is an abelian group and $\mu$ is a linear mapping of $A\times M\rightarrow M$, s.t. $\mu(a,x)=ax$, the following axioms are satisfied:* $\forall a,b\in A$ *and* $x,y\in M$,

$$a(x+y)=ax+ay, (a+b)x=ax+bx, (ab)x=a(bx), 1x=x.$$

**Note. (Generators of Modules)** The generators of modules can be viewed as generators of *additive abelian group* with adding the multiplication.

**Note 2.2.** $A$-模是一个带$A$线性乘法的加法群，或是带环同态 $A\rightarrow\mathrm{End}(M)$ 的加法群。

**Example 2.3.**

1. An ideal of $A$ is an $A$-module.
2. For a field $k$, a $k$-module is a vector space.
3. A $\mathbb{Z}$-module is an Abelian group.
4. If $A=k[x]$, with $k$ a field, then $A$-module is a $k$-vector space with a linear transformation.
5. Let $G$ be a finite group, $A=k[G]$ be a group algebra of $G$ over field $k$. Then an $A$-module is a $k$-representation of $G$.

**Definition 2.4. (module homomorphism)** *Let $M$, $M$ be $A$-module, then the map $f\colon M\rightarrow N$ is an $A$-module homomorphism if*

$$f(x+y)=f(x)+f(y), f(ax)=af(x) \qquad \forall a\in A,\ x,y\in M.$$

*The set of all $A$-module homomorphisms from $M$ to $N$ can be viewed as an $A$-module as well. Define*

$$(f+g)(x)=f(x)+g(x), \quad (af)(x)=af(x), \quad \forall x\in M.$$

*This $A$-module is denoted by* $\mathrm{Hom}_A(M,N)$ *or simply* $\mathrm{Hom}(M,N)$.

**Note 2.5.** 所有的$A$-模同态的集合是$A$-模，正如所有的群同态的集合也是群。

## 2.1 Submodules and quotient modules

Let $f\colon M\rightarrow N$ be an $A$-module homomorphism, the kernel of $f$ is a submodule of $M$. The image of $f$, $\mathrm{Im}(f)=f(M)$ is a submodule of $N$. We define cokernel of $f$ as $\mathrm{Coker}(f)=N/\mathrm{Im}(f)$, which is a quotient module of $N$.

### 2.1.1 Operations on submodules

**Note 2.6.** 理想是模，理想的运算可以推广到模中；
模同时又是一种特殊的加法群，故又能继承一些加法群的性质。

Since modules are Abelian groups first, submodule inherits properties of subgroup, hence we have some isomorphism theorems for submodules, such as:

**Proposition 2.7.**

*i. If $L \supseteq M \supseteq N$ are $A$-modules, then $(L/N)/(M/N) \cong L/M$;*

*ii. If $M_1, M_2$ are submodules of $M$, then $(M_1 + M_2)/M_1 \cong M_2/(M_1 \cap M_2)$.*

Since ideals is a special submodules, there are some definitions from ideals can be applied to submodules, such as quotient and annihilator.

We can not define directly the product of two submodules, but can define the product of a submodule and an ideal of $A$, which is a $A$-module as well.

**Definition 2.8.** *Let $N$ and $P$ are $A$-modules, then $(N:P) = \{a \in A: aP \subset N\}$, which is an ideal of $A$. Similarly, we have definition of $\operatorname{Ann}(N)$.*

**Definition 2.9. (faithful)** *An $A$-module $M$ is faithful if $\operatorname{Ann}(M) = 0$.*

### 2.1.2 Direct sum and product

**Note 2.10.** 直和与直积的‘表面’区别在于前者是有限的后者是无限的。

**Definition 2.11.** *A free $A$-module is the one which is isomorphic to an $A$-module of form $\oplus_{i\in I} M_i$, with $M_i \cong A$.*

A finitely generated free $A$-module is isomorphic to $A \oplus \cdots \oplus A = A^n$.

**Note 2.12.** 有限生成的$A$-模可以分解为有限个理想，或者同构于$A^n$的一个商模。

**Proposition 2.13.** *$M$ is a finitely generated $A$-module if and only if $M$ is isomorphic to a quotient of $A^n$ for some integer $n > 0$.*

**Proposition 2.14.** *Let $M$ be a finitely generated $A$-module, $a$ be an ideal of $A$, and $\phi$ be an $A$-module homomorphism of $M$ such that $\phi(M) \subseteq aM$. Then $\phi$ satisfies an equation of the following form*

$$\phi^n + \alpha_1 \phi^{n-1} + \cdots + \alpha_n = 0$$

*where $\alpha_i$ are in $a$.*

*In particular, if $aM = M$, then there exists $x \equiv 1 (\operatorname{mod} a)$ such that $xM = 0$.*

**Note 2.15.** If $A$ is a PID, then we may call $a$ an integer element over $A$. (类似于代数数论中整元素的定理)

**Theorem 2.16. (Nakayama Lemma)** *Let $M$ be a finitely generated $A$-module, $\alpha$ is an ideal of $A$ which is contained in $\mathfrak{R}$. If $\alpha M = M$, then $M = 0$.*

**Proof. (sketch)** From Proposition 2.14, there exists $x \equiv 1 (\mathrm{mod}\, \Re)$, s.t. $xM = 0$. On the other hand, $x$ is a unit by 1.33. Thus $M = x^{-1} x M = 0$ □

**Corollary 2.17.** *Let $M$ be a finitely generated $A$-module, $N$ a submodule of $M$, and $a \subseteq \Re$ an ideal of $A$. If $M = aM + N$, then $M = N$.*

**Proof. (sketch)** $a(M/N) = (aM + N)/N$, then by Nakayama lemma. □

## 2.2 Exact sequences

**Definition 2.18. (exact sequence)** *A sequence of $A$-module and $A$-homomorphism*

$$\cdots \to M_{i-1} \xrightarrow{f_i} M_i \xrightarrow{f_{i+1}} M_{i+1} \to \cdots$$

*is said to be exact at $M_i$ if $\mathrm{Im}(f_i) = \mathrm{Ker}(f_{i+1})$. The sequence is called to be exact if it is exact at each $M_i$.*

**Remark.** $0 \to M' \xrightarrow{f} M \xrightarrow{g} M'' \to 0$ is exact (i.e. $\mathrm{Im}(f) = \ker(g)$) $\Leftrightarrow$ $f$ is injective, $g$ is surjective, and $g$ induces an isomorphism of $\mathrm{Coker}(f) = M/f(M') \cong M''$. This type of sequence is called a *short exact sequence*. Any long exact sequence can be split up into short sequences. In fact, let $N_i := \mathrm{Im}(f_i) = \mathrm{Ker}(f_{i+1})$. Then we have

$$0 \to N_i \to M \to N_{i+1} \to 0, \qquad (\forall i)$$

**Proposition 2.19.**

i. *Let $M' \xrightarrow{f} M \xrightarrow{g} M'' \longrightarrow 0$ is exact $\Leftrightarrow$ $\forall A$-module $N$, the sequence*

$$0 \longrightarrow \mathrm{Hom}(M'', N) \xrightarrow{\bar{g}} \mathrm{Hom}(M, N) \xrightarrow{\bar{f}} \mathrm{Hom}(M', N)$$

*is exact.*

ii. *Let $0 \longrightarrow M' \xrightarrow{f} M \xrightarrow{g} M''$ is exact $\Leftrightarrow$ $\forall A$-module $N$, the sequence*

$$0 \longrightarrow \mathrm{Hom}(N, M') \xrightarrow{\bar{f}} \mathrm{Hom}(N, M) \xrightarrow{\bar{g}} \mathrm{Hom}(N, M'')$$

*is exact.*

**Definition 2.20. (additive function of exact sequence)** *A additive function $\lambda$ on class of $A$-module with values in $\mathbb{Z}$ will map a short exact sequence into $\lambda(M')$,$\lambda(M)$,$\lambda(M'')$, s.t. $\lambda(M') - \lambda(M) + \lambda(M'') = 0$.*

**Example 2.21.** Let $A$ be a field $k$, and let $C$ be the class of all finite-dimensional $k$-vector spaces $V$. Then $\lambda: V \to \dim V$ is an additive function on $C$.

**Proposition 2.22.** *Let $0 \to M_0 \to M_1 \to \cdots \to M_n \to 0$ be an exact sequence of $A$-module in which all the modules $M_i$ and the kernels of all homomorphisms belong to $C$. Then for any additive function $\lambda$ on $C$ we have*

$$\sum_{i=0}^{n} (-1)^i \lambda(M_i) = 0.$$

## 2.3 Tensor product of Modules

**Definition 2.23. (bilinear)** *Let $M$, $N$, $P$ be three $A$-modules. A mapping $f: M \times N \to P$ is said to be $A$-bilinear if $\forall x \in M$, $y \mapsto f(x, y)$ of $N$ into $P$ is $A$-linear, and for any $y \in N$, $x \mapsto f(x, y)$ of $M$ into $P$ is $A$-linear.*

**Definition 2.24. (tensor product)** *Let $M$ $N$ be two $A$-modules, then tensor product of $M$ and $N$ over $A$, $M \otimes_A N$ is an $A$-module together with an bilinear map:*

$$\otimes: M \times N \longrightarrow M \otimes_A N$$

*which is universal in the following sense:*

*$\forall$ $A$-module $P$ and every bilinear map $f: M \times N \to P$, there is a unique isomorphism*

$$\tilde{f}: M \otimes_A N \to P$$

*such that $\tilde{f} \circ \otimes = f$.*

**Proposition 2.25. (Canonical isomorphisms)** *Let $M$ $N$ $P$ be $A$-modules, then there exist unique isomorphisms:*

1. *$M \otimes N \to N \otimes M$, $x \otimes y \longmapsto y \otimes x$;*
2. *$(M \otimes N) \otimes P \to M \otimes (N \otimes P) \to M \otimes N \otimes P$, $(x \otimes y) \otimes z \longmapsto x \otimes (y \otimes z) \longmapsto x \otimes y \otimes z$;*
3. *$(M \oplus N) \otimes P \to (M \otimes P) \oplus (N \otimes P)$,$(x, y) \otimes z \longmapsto (x \otimes z, y \otimes z)$;*
4. *$A \otimes M \to M$, $a \otimes x \longmapsto ax$.*

Let $f: A \rightarrow B$ be a ring homomorphism, $M$ an $A$-module, then $M_B = B \otimes_A M$ is an $A$-module, (since $ax$ is defined by $f(a)x$ in $B$, hence $B$ can be regarded as $A$-module) What's more, $M_B$ can be regarded as $B$-module, s.t. $b(b' \otimes x) = bb' \otimes x, \forall b, b' \in B$, $x \in M$. $M_b$ is said to be obtained from $M$ by extension of scalars.

**Note 2.26.** 上述结论可以看作是模的扩展和收缩概念的推广，参见 Section 1.7。

**Proposition 2.27.** *If $M$ is a finitely generated $A$-module, then $M_B$ is a finitely generated $B$-module.*

## 2.4 Exactness of tensor product

Let $f: M \times N \rightarrow P$ be an $A$-bilinear mapping, then we have a canonical isomorphism:

$$\mathrm{Hom}(M \otimes N, P) \cong \mathrm{Hom}(M, \mathrm{Hom}(N, P))$$

i.e.

$$\mathrm{Hom}(T(M), P) \cong \mathrm{Hom}(M, U(P))$$

hence, the functor $T$ is left adjoint of $U$, and $U$ is the right adjoint of $T$.

**Proposition 2.28. (Left adjoint is right exact)** *Let $M' \xrightarrow{f} M \xrightarrow{g} M'' \longrightarrow 0$ be exact sequence of $A$-modules and homomorphism and let $N$ be any $A$-module, then the sequence*

$$M' \otimes N \xrightarrow{f \otimes 1} M \otimes N \xrightarrow{g \otimes 1} M'' \otimes N \longrightarrow 0$$

*is exact.*

**Definition. (flat module)** *The functor $T_N: M \rightarrow M \otimes_A N$ is not always exact (for short exact sequences). If* ***$T_N$ is exact****, that's to say, if tensoring with $N$ makes all exact sequences into exact sequences, then $N$ is said to be a flat $A$-module.*

**Note 2.29.** 因为张量积是左伴随的，因此是右正合的；

如果拥有了平坦性，则也是左正合的，故是短正合的。

**Theorem 2.30. (absolutely flat)** *A ring $A$ is absolutely flat if every $A$-module is flat. TFAE:*

*i. $A$ is absolutely flat;*

*ii. Every principal ideal is idempotent;*

*iii. Every finitely generated ideal is a direct summand(component of direct sum) of $A$.*

**Remark.**

- A Bolean ring is absolutely flat.
- Every homomorphism image of an absolutely flat ring is absolutely flat.
- A absolutely flat local ring is a field.
- Every non-unit in an absolutely flat ring is zero-divisor.

## 2.5 Algebras

**Definition 2.31. (algebra)** *A ring $B$ equipped with $A$-module structure is said to be $A$-algebra, or ring $B$ together with a ring homomorphism $f: A \to B$.*

**Note 2.32.** $A$-algebra = ring + $A$-module = ring + ring homomorphism

**Example.** Every ring is a $\mathbb{Z}$-algebra. A $k$-algebra is a ring containing $k$ as its subring.

**Remark.** An $A$-algebra $B$ is **finite** if $B$ is a finitely generated $A$-module, i.e. $B = Aa_1 + \ldots + Aa_n$.

$B$ is **finitely generated** (or finite type) if $\exists x_i \in B, 1 \leqslant i \leqslant n$, s.t. every element in $B$ can be written as a polynomial in $x_i$ with coefficients in $f(A)$, or equivalently, if there is an $A$-algebra homomorphism from $A[x_1, \ldots, x_n]$ onto $B$.

A ring is called finitely generated if it is finitely generated as a $\mathbb{Z}$-algebra.

**Note 2.33.** 代数是有限的比有限生成的更强。比如 $k[X]$ 是有限生成的 $k$-代数，但不是有限的。

## 2.6 Tensor product of algebras

Let $B, C$ be two $A$-algebras, $f: A \to B$, $g: A \to C$. Since $B, C$ are A-modules, we have $D = B \otimes_A C$ which is an $A$-module. Then consider the mapping $B \times C \times B \times C \to D$ defined by $(b, c, b', c') \mapsto bb' \otimes cc'$. Therefore $D = B \otimes_A C$ with

$$D \times D \to D$$

$$(b, c, b', c') \longmapsto bb' \otimes cc'$$

## 2.7 Direct limits

**Definition. (directed set, direct system)** *A partially ordered set $I$ is said to be a directed set if $\forall i, j \in I$, there exists $k \in I$, s.t. $i \leqslant k$ and $j \leqslant k$. i.e. $I$ has an upper boundary.*

*Let $A$ be a ring, $I$ be a directed set and $(M_i)_{i\in I}$ is a family of $A$-modules. Let $\mu_{ij}$: $M_i \to M_j$ $(\forall i \leqslant j \in I)$ be an $A$-homomorphism, and suppose the following axioms are satisfied:*

- *i.* *$\mu_{ii}$ is identity mapping of $M_i$, $\forall i \in I$.*
- *ii.* *$\mu_{ik} = \mu_{jk} \circ \mu_{ij}$ wherever $i \leqslant j \leqslant k$*

*Then $(M_i, \mu_{ij})$ are said to form a direct system $\mathcal{M}$ over the directed set $I$.*

**Definition. (direct limit)** *Let $C = \oplus_{i\in I} M_i$ and $D$ be submodule of $C$ generated by all elements of then form $x_i - \mu_{ij}(x_i)$, where $i \leqslant j \in I$, $x_i \in M_i$. Then module $M$ is called to be direct limit of $M_i$, which can be written as $M = \varinjlim M_i$.*

**Proposition 2.34.** *Tensor product and direct limit are commutative,i.e. $\varinjlim (M_i \otimes N) \cong \left(\varinjlim M_i\right) \otimes N$*

# 3 Rings and Modules of fractions

**Definition 3.1. (ring of fractions)** *Let $A$ be a ring, $S$ is a multiplicatively closed set of $A$, define an equivalence relation "$\equiv$" on $A \times S$ as follows:*

$$(a, s) \equiv (b, t) \Leftrightarrow (a t - b s) u = 0 \,\text{for some}\, u \in S$$

*Let $a / s$ denote the equivalence of $(a, s)$ and let $S^{-1}A$ denote the set of equivalence classes.*

*We can put a ring structure on $S^{-1}A$ b defining addition and multiplication in the same way as in elementary algebra. The ring $S^{-1}A$ is called the ring of fractions of $A$ with respect to $S$.*

**Example.**

- i. Let $\wp$ be a prime ideal of $A$, then $S = A - \wp$ is a multiplicatively closed set, and we write $A_\wp$ for $S^{-1}A$ in this case. $A_\wp$ is a local ring and this process is so called localization at $\wp$.
- ii. Let $\alpha$ be any ideal of $A$, then $S = 1 + \alpha = \{1 + x : x \in \alpha\}$ is a multiplicative closed set.
- iii. Let $f \in A$ and let $S = \{f^n\}_{n \geqslant 0}$, we write $A_f$ for this case.

**Proposition 3.2. (universal properties)** *Let $g: A \to B$ be a ring homomorphism such that $g(s)$ is a unit in $B$ for all $s \in S$. Then there exists a unique ring homomorphism $h: S^{-1}A \to B$ such that $g = h \circ f$, where $f: A \to S^{-1}A$.*

**Proposition 3.3.** *The operation $S^{-1}$ is exact.*

**Proposition 3.4.** *Let $M$ be an $A$-module, then $S^{-1}M \cong S^{-1}A \otimes_A M$, with a uniquely isomorphism: $f((a/s) \otimes m) = am/s$, $(\forall a \in A, m \in M, s \in S)$.*

**Corollary 3.5.** *$S^{-1}A$ is a flat $A$-module.*

## 3.1 Local properties

**Remark 3.6.** From $A$ to $A_\wp$ cuts out all prime ideals except those contained in $\wp$; from $A$ to $A/\wp$ cuts out all prime ideals except those containing $\wp$.

**Note 3.7.** *$A_\wp$ 是对$A$的放大（使用部分分母），而 $A/\wp$ 是对 $A$ 分割缩小。*

**Definition 3.8. (local property)** *A property $P$ of a ring $A$ (or an $A$-module $M$) is said to be a local property if*

*A(or M) has property $P$ $\Leftrightarrow$ $A_\wp(\text{or } M_\wp)$ also has property $P$ for any $\wp$.*

**Theorem 3.9. (local properties)** *The following properties are local properties:*

- *$M = 0$ (then $M_\wp = 0$,$M_m = 0$);*
- *flatness of A-module;*
- *injection and surjection of homomorphism of A-module;*
- *Integral closed is a local property of domain.*

**Proposition 3.10.** *Let $M$ be a finitely generated $A$-module, $S$ a multiplicatively closed set of $A$. Then*

$$S^{-1}(\mathrm{Ann}(M)) = \mathrm{Ann}(S^{-1}M)$$

# 4 Primary Decomposition

This chapter is intended to study a method to represent an ideal as the intersection of everal primary ideals.

**Definition 4.1. (primary)** *An ideal $q$ in a ring $A$ is primary if $q \neq A$ and if $xy \in q \Rightarrow x \in q$ or $y^n \in q$, for some $n$.*

*In other words, $\Leftrightarrow$ every zero-divisor in $A/q \neq 0$ is nilpotent.*

**Remark 4.2.** Every prime ideal is primary. Contraction of a primary ideal is primary.

**Proposition 4.3.** *Let $q$ be a primary ideal of $A$ then $r(q)$ is the smallest prime ideal containing $q$. For notation, if $r(q) = \wp$, then $q$ is said to be $\wp$-primary.*

**Proposition 4.4.** *If $r(\alpha)$ is maximal, then $\alpha$ is primary. In particular, the power of a maximal ideal $m$ are $m$-primary.*

**Note 4.5.** 素理想的幂不一定是准素的，但极大理想的幂一定是准素的。

**Definition. (primary decomposition)** *A primary decomposition of an ideal $\alpha$ in $A$ is an expression of $\alpha$ as a finite intersection of primary ideals, say $\alpha = \bigcap_{i=1}^{n} q_i$. We shall say $\alpha$ is decomposable if it has a primary decomposition.*

**Theorem 4.6. (first uniqueness theorem)** *Let $\alpha$ be a decomposable ideal and let $\alpha = \bigcap_{i=1}^{n} q_i$ be a minimal primary decomposition of $\alpha$. Let $\wp_i = r(q_i)(1 \leqslant i \leqslant n)$. Then the $\wp_i$ are precisely the prime ideals which occur in the set of ideal $r(a \colon x)$ $(x \in A)$, and hence are independent of the particular decomposition of $\alpha$.*

**Remark.** The prime ideals $\wp_i$ in Theorem 4.6 are said to be belong to $\alpha$, or to be associated with $\alpha$. Hence, $\alpha$ is primary iff. it has only one associated prime ideal.

**Definition 4.7.** *The minimal elements (respect to inclusion) of the set $\{\wp_1, \wp_2, \ldots, \wp_n\}$ are called the minimal or isolated prime ideals belonging to $\alpha$. The others are called embedded prime ideals.*

*A set $\Sigma$ of prime ideas belonging to $\alpha$ is said to be isolated if it satisfies the following condition: if $\wp'$ is a prime ideal belonging to $\alpha$ and $\wp' \subset \wp(\exists \wp \in \Sigma)$, then $\wp' \in \Sigma$.*

**Theorem 4.8. (2nd uniqueness theorem)** *Let $\alpha$ be a decomposable ideal and let $\alpha = \bigcap_{i=1}^{n} q_i$ be a minimal primary decomposition of $\alpha$, and let $\{\wp_{i_1}, \ldots, \wp_{i_m}\}$ be an isolated set of prime ideals of $\alpha$. Then $q_{i_1} \cap \ldots \cap q_{i_m}$ is independent of the decomposition.*

In particular,

**Corollary 4.9.** *The isolated primary components(i.e. the primary component $q_i$ corresponding to minimal prime ideal $\wp_i$) are uniquely determined by $\alpha$.*

# 5 Integral Dependence and Valuations

## 5.1 The going-up theorem

**Theorem 5.1.** *Let $A \subset B$ be rings, $B$ integral over $A$, and let $\wp$ be a prime ideal of $A$, then there exists a prime ideal $q$ in $B$ such that $q \cap A = \wp$.*

Then we have following going-up theorem:

**Theorem 5.2. (Going-up theorem)** *Let $A \subset B$ be ring, $B$ integral over $A$, and let $\wp_1 \subset \wp_2 \subset \ldots \subset \wp_n$ be a chain of prime ideals of $A$ and $q_1 \subset q_2 \subset \ldots \subset q_m$ be a chain of prime ideals of $B$ such that $q_i \cap A = \wp_i\,(1 \leqslant i \leqslant m)$. Then the chain $q_1 \subset q_2 \subset \ldots \subset q_m$ can be extended to a chain $q_1 \subset q_2 \subset \ldots \subset q_n$, such that $q_i \cap A = \wp_i\,(1 \leqslant i \leqslant n)$.*

## 5.2 The going-down theorem

**Proposition 5.3.** *Let $A \subset B$ be rings, $C$ the integral closure of $A$ in $B$. Let $S$ be a multiplicatively closed set of $A$. Then $S^{-1}C$ is the integral closure of $S^{-1}A$ in $S^{-1}B$.*

**Theorem 5.4. (Going-down theorem)** *Let $A \subset B$ be integral domains, $A$ integrally closed, $B$ integral over $A$. Let $\wp_1 \supset \wp_2 \supset \ldots \supset \wp_n$ be a chain of prime ideals of $A$ and let $q_1 \supset \ldots \supset q_m$ be a chain of prime ideals of $B$, s.t. $q_i \cap A = \wp_i\,(1 \leqslant i \leqslant m)$. Then the chain can be extended to a chain $q_1 \supset \ldots \supset q_n$, where $q_i \cap A = \wp_i\,(1 \leqslant i \leqslant n)$.*

## 5.3 Valuation rings

**Definition. (valuation ring)** *Let $B$ be an integral domain, $K$ its field of fractions. $B$ is a valuation ring of $K$ if $\forall x \neq 0$, then either $x \in B$ or $x^{-1} \in B$ (or both).*

**Proposition 5.5.** *Let $B$ be a valuation ring, then*

*i. $B$ is a local ring;*

*ii. If $B'$ is a ring s.t. $B \subset B' \subset K$, then $B'$ is also a valuation ring of $K$;*

*iii. $B$ is integrally closed.*

The following theorem solves how to find a local ring:

Let $K$ be a field, $\Omega$ an algebraically closed field. Let $\Sigma$ be set of all pairs $(A, f)$, where A is subring of $K$ and $f$ is a homomorphism of $A$ into $\Omega$. We partially order the set as follows:

$$(A, f) \leqslant (A', f') \Leftrightarrow A \subset A' \text{and } f'|_A = f$$

**Theorem 5.6.** *Let $(B, g)$ be the maximal element of $\Sigma$, then $B$ is a valuation ring of $K$.*

**Corollary 5.7.** *Let $A$ be the subring of $K$, then the integral closure $\bar{A}$ of $A$ in $K$ is the intersection of all valuation rings of $K$ which contain $A$.*

**Corollary 5.8.** *Let $K$ be a field and $B$ a finitely generated $k$-algebra. If $B$ is a field then it's a finite algebraic extension of $K$.*

# 6 Chain Conditions

**Remark 6.1.** Stationary sequence is equivalent to the existence of maximal(or minimal) elements.

**Proposition 6.2.** *Let $0 \longrightarrow M' \xrightarrow{f} M \xrightarrow{g} M'' \longrightarrow 0$ be an exact sequence of $A$-modules, then*

- *$M$ is Noetherian $\Leftrightarrow$ $M'$ and $M''$ are Noetherian;*
- *$M$ is Artinian $\Leftrightarrow$ $M'$ and $M''$ are Artinian.*

**Corollary 6.3.** *If $M_i$ are Noetherian (resp. Artinian) $A$-modules, so is $\oplus_{i=1}^{n} M_i$.*

***Proof.*** *By induction and the exact sequence: $0 \to M_n \to \oplus_{i=1}^{n} M_i \to \oplus_{i=1}^{n-1} M_i \to 0$.* □

**Proposition 6.4.** *Let $A$ be a Noetherian (resp. Artinian) ring,*

- *If $M$ is a finitely generated $A$-module, then $M$ is Noetherian (resp. Artinian)*
- *$\alpha$ is an ideal of $A$, then $A/\alpha$ is Noetherian (resp. Artinian)*

## 6.1 Composition series

**A chain of submodules** of a module $M$ is a sequence $(M_i)$ of submodules of $M$, such that $M = M_0 \supset M_1 \supset \ldots \supset M_n = 0$(strict inclusions). A composition series is a maximal chain, that is one in which on extra submodules can be inserted, i.e. $M_{i-1}/M_i$ are simple. Every composition series of a module $M$ have the same length.

A module which has a composition series is called a module of finite length, the length of composition series $l(M)$ is called the length of $M$. The length $l(M)$ is an additive function on the class of all $A$-modules with finite length.

**Theorem 6.5.** *$M$ has a composition series $\Leftrightarrow$ $M$ satisfies both a.c.c. and d.c.c.*

**Proposition 6.6.** *For $k$-vector space $V$, TFAE:*

- *i. finite dimension;*
- *ii. finite length;*
- *iii. a.c.c*
- *iv. d.c.c*

**Corollary 6.7.** *Let $A$ be a ring in which $0 = m_1 m_2 ... m_n$ (not necessary distinct maximal ideals), then $A$ is Noetherian iff. $A$ is Artinian.*

# 7 Noetherian rings

**Proposition 7.1.** *If $A$ is a Noetherian ring and $\phi$ is a homomorphism of $A$* ***onto*** *a ring $B$, then $B$ is Noetherian.*

**Proposition 7.2.** *If $A$ is a Noetherian ring and $S$ is any multiplicatively closed set, then $S^{-1}A$ is Noetherian. In particular, $A_\wp$ is Noetherian if $A$ is Noetherian.*

## 7.1 Primary decomposition in Noetherian rings

**Definition. (Irreducible)** *An ideal $\alpha$ is said to be irreducible if $\alpha = b \cap c \Rightarrow \alpha = b$ or $\alpha = c$.*

**Lemma 7.3.** *$A$ is a Noetherian ring,*

- *i. every ideal is a finite intersection of irreducible ideals;*
- *ii. every irreducible ideal is primary.*

**Theorem 7.4.** *In a Noetherian ring $A$, every ideal has a primary decomposition.*

**Proposition 7.5.** *In a Noetherian ring $A$, every ideal $\alpha$ contains a power of its radical,i.e. $(r(\alpha))^m \subset \alpha$. Hence, nilradical of $A$ is nilpotent.*

**Proposition 7.6.** *Let $\alpha \neq (1)$ be an ideal of a Noetherian ring, then the prime ideals which belong to $\alpha$ are precisely the prime ideals which occur in the set of ideals $(a\colon x)(\forall x \in A)$.*

# 8 Artin rings

**Theorem 8.1.** *In an Artin ring $A$ every prime ideal is maximal. What's more, it has only finite number of maximal ideals.*

**Proposition 8.2.** *In an Artin ring the nilradical is nilpotent.*

**Theorem 8.3.** *A ring $A$ is Artin $\Leftrightarrow$ $A$ is Noetherian and $\dim A = 0 \Leftrightarrow A$ is Noetherian and $\operatorname{Spec}(A)$ is discrete.*

**Proposition 8.4.** *Let $A$ be a Noetherian local ring, then exactly one of following two statements is true:*

*i.* $m^n \neq m^{n+1} (\forall n)$;

*ii.* $m^n = 0 (\exists n)$, *in which case $A$ is an Artin local ring.*

**Theorem 8.5. (structure theorem for Artin rings)** *An Artin ring $A$ is uniquely (up to isomorphism) a finite direct product of Artin local rings.*

**Theorem 8.6.** *Let $A$ be an Artin local ring, $k = A/m$ its residue field, then TFAE:*

*i. every ideal of $A$ is principal;*

*ii. the maximal ideal $m$ is principal;*

*iii.* $\dim_k(m/m^2) \leqslant 1$.

# 9 Discrete valuation rings and Dedekind domains

## 9.1 Discrete valuation rings

Let $k$ be a field, $K^* = k - \{0\}$ the multiplicative group of $k$. A discrete valuation on $k$ is a mapping $v$ of $K^*$ onto $\mathbb{Z}$, such that

- $v(xy) = v(x) + v(y),$ i.e. $v$ is homomorphism;
- $v(x + y) \geqslant \min(v(x), v(y))$

The set **containing 0 and all $x \in K^*$ such that $v(x) \geqslant 0$** is a ring, called the valuation ring of $v$.

The valuation ring of $v$ is a valuation ring of field $k$, and sometimes we define $v(0) = +\infty$.

**Example.** $k = \mathbb{Q}$, take a fixed prime $p$, then any $0 \neq x \in \mathbb{Q}$ can be written as $p^a y$, where $a \in \mathbb{Z}$ and both numerator and denominator of $y$ are prime to $p$. Define $v_p(x) = a$, then valuation ring of $v_p$ is local ring $\mathbb{Z}_{(p)}$.

**Definition.** *An domain $A$ is a discrete valuation ring if there is a discrete valuation $v$ of its field of fractions $k$, s.t. $A$ is the valuation ring of $v$.*

**Remark.** A DVD is a Noetherian domain with dimension 1 and it is a local ring.

**Theorem 9.1.** *Let $A$ be a Noetherian local domain of dimension 1, $k = A/m$ is residue field. TFAE:*

*i. $A$ is a DVD;*

*ii. $A$ is integrally closed;*

*iii. $m$ is principal ideal;*

*iv. $\dim_k(m/m^2) = 1$;*

*v. every nonzero ideal is a power of $m$;*

*vi. $\exists x \in A$, s.t. every nonzero ideal is of the form $(x^k), k \geqslant 0$.*

## 9.2 Dedekind domains

**Note 9.2.** A field is a PID but not a Dedekind Domain.

**Theorem 9.3.** *Let $A$ be a Noetherian domain of dimension $1$, Then TFAE:*

*i.* *$A$ is integrally closed, i.e. Dedekind;*

*ii.* *every primary ideal of $A$ is a prime power;*

*iii.* *every local ring $A_{\wp}(\wp \neq 0)$ is a DVD.*

**Corollary 9.4.** *In a Dedekind domain every non-zero ideal has a unique factorization as product of prime ideals.*

### 9.2.1 Fractional ideals

**Theorem 9.5.** *The invertible of fractional ideal is a local property.*

1. *$M$ is invertible;*
2. *$M$ is finitely generated and $\forall \wp$, $M_{\wp}$ is invertible;*
3. *$M$ is finitely generated and $\forall m$, $M_m$ is invertible.*

**Proposition 9.6.** *Let $A$ be a domain, then $A$ is a Dedekind domain $\Leftrightarrow$ every nonzero fractional ideal of $A$ is invertible.*

**Definition.** *Let $K^*$ denote the multiplicative group of $k$ (field of fractions), $\forall u \in K^*$ defined a fractional ideal $(u)$, and the mapping $u \longmapsto (u)$ is a homomorphism $\phi$: $K^* \rightarrow I$.*

*The image $P$ of $\phi$ is the group of PIDs, the quotient group $H = I / P$ is so called the ideal class group of $A$. The kernel $U$ of $\phi$ is the group of units of $A$.*

$U$ is a finitely generated abelian group. The elements of finite order in $U$ are just the roots of unity which lie in $k$, and they form a finite cyclic group $W$; $U / W$ is there are $n$ distinct embeddings $K \rightarrow C$(the field of complex numbers). The number of generators of $U / W$ is then $r_1 + r_2 - 1$.

We have an exact sequence:

$$1 \rightarrow U \rightarrow K^* \rightarrow I \rightarrow H \rightarrow 1$$

**Proposition 9.7.** *Let $k$ is an algebraic number field, $A = O_K$(Hence, is Dedekind), then order$(H) < +\infty$, $h = \mathrm{order}(H)$ is the class number of the field $k$. TFAE:*

*i.* *$h = 1$;*

*ii.* *I=P;*

*iii. A is PID*

*iv. A is UFD*

# 10 Completions

在交换代数中，我们有两种方法简化环的结构，一是局部化，其次是完备化。
局部化的两个重要性质是保持正合性和诺特性。当局限于有限生成模时，同样的结论断言对完备化也是正确的。

完备化还拥有一个重要结论是 Krull 定理。这一定理鉴定出环中进过完备化所零化的部分。Krull引理和完备化的正合性都是著名的 Artin-Rees 引理的简单结论。

## 10.1 Topologies and completions

**Lemma 10.1.** *Let $H$ be the intersections of all neighbourhoods of 0 in $G$, then*

1. *$H$ is a subgroup;*
2. *$H$ is closure of $\{0\}$;*
3. *$G/H$ is Hausdorff;*
4. *$G$ is Hausdorff $\Leftrightarrow H=0$*

**Remark 10.2.**

完备化的方法有两种，一是Cauchy序列，另一种是使用反向极限。

**Proposition 10.3.** *If $0\to\{A_n\}\to\{B_n\}\to\{C_n\}\to 0$ is an exact sequence of inverse system, then*

$$0\to\varprojlim A_n\to\varprojlim B_n\to\varprojlim C_n$$

*is always exact.*

*In particular, $A_n$ is surjective system, then $0\to\varprojlim A_n\to\varprojlim B_n\to\varprojlim C_n\to 0$ is exact.*

## 10.2 Graded rings and modules

**Definition.** *A graded ring is a ring $A$ together with a family $(A_n)_{n\geqslant 0}$ of subgroups of the additive group of $A$, such that $A=\oplus_{n=0}^{n}A_n$ and $A_mA_n\subset A_{n+m}$ $(\forall m,n\geqslant 0)$.*

**Proposition 10.4.** *For a graded ring $A$, TFAE:*

1. *$A$ is a Noetherian ring;*
2. *$A_0$ is Noetherian and $A$ is finitely generated as an $A_0$-algebra.*

**Theorem 10.5. (Artin-Rees Lemma)** *Let $A$ be a Noetherian ring, $M$ a finitely generated $A$-module, $(M_n)$ a stable $\alpha$-filtration of $M$. If $M'$ is a submodule of $M$, then $(M' \cap M_n)$ is a stable $\alpha$-filtration of $M'$.*

**Theorem 10.6. (Krull Theorem)** *Let $A$ be a Noetherian ring, $M$ a finitely generated $A$-module, and $\hat{M}$ the $\alpha$-completion of $M$. Then the kernel $E = \bigcap_{n=1}^{n} \alpha^n M$ of $M \rightarrow \hat{M}$ consists of those $x \in M$ annihilated by some element of $1 + \alpha$.*

### 10.3 The associated graded ring

**Definition.** *Let $A$ be ring and $\alpha$ an ideal of $A$, define $G(A) = G_\alpha(A) = \oplus_{n=0}^{n} \alpha^n / \alpha^{n+1}$. This is a graded ring called the associated graded ring.*

*Similarly, if $M$ is an $A$-module, $(M_n)$ is an $\alpha$-filtration of $M$, define $G(M) = \oplus_{n=0}^{n} M_n / M_{n+1}$, which is a graded $G(A)$-module in a natural way.*

**Theorem 10.7.** *Let $A$ be Noetherian ring, $\alpha$ an ideal of $A$, then*

- *$G_\alpha(A)$ is Noetherian;*
- *$G_\alpha(A) \cong G_{\hat{\alpha}}(\hat{A})$ as graded ring.*

# 11 Dimension theory

## 11.1 Dimension theory of Noetherian local ring

Let $A$ be a Noetherian local ring, $m$ its maximal ideal. Let $\delta(A) =$ least number of generators of an $m$-primary ideal of $A$.

**Theorem 11.1. (Dimension theorem)** *For any Notherian local ring $A$, TFAE:*

1. *the maximal length of chains of prime ideals of $A$;*
2. *the degree of the characteristic polynomial $\chi_m(n) = l(A/m^n)$;*

3. *the least number of generators of an $m$-primary ideal of $A$.*

*i.e.* $\delta(A) = d(A) = \dim(A) < +\infty$.

**Remark.** $\text{height}(\wp) = \dim A_{\wp}$; $\text{depth}(\wp) = \dim A/\wp$.

**Theorem 11.2. (Krull's principal ideal theorem)** *Let $A$ be a Noetherian ring and let $x$ be an element of $A$ which is neither a zero-divisor nor a unit. Then every minimal prime ideal $\wp$ of $(x)$ has height* $1$.

**Corollary 11.3.** *Let $\hat{A}$ be the $m$-adic completion of $A$, then* $\dim A = \dim \hat{A}$.

## 11.2 Regular local ring

**Theorem 11.4.** *Let $A$ be a Noetherian local ring of dimension $d$, $m$ its maximal ideal, $k = A/m$. Then TFAE (which are definitions of regular local ring)*

1. $G_m(A) \cong k[t_1, \ldots, t_d]$*;*
2. $\dim(m/m^2) = d$;
3. *$m$ can be generated by $d$ elements.*

A regular local rings is an integrally closed integral domain.

# Index