Commutative Algebra

Icey Swan

My notes for commutative algebra, based on the textbook Introduction to commutative algebra by M.F. Atiyah and I.G. Macdonald, Addison-Wesley.

March 19, 2024

Contents

1. Ring

1.1. Rings & Ring Homomorphisms

Definition 1.1.1 (Ring) A is a non-empty set with binary operators '$+$ ' and ' $\cdot$ '. Then A is a ring if

1. $(A, +)$ is an abelian group
2. $(A, \cdot)$ is a semigroup
3. $\forall a, b, c \in A$, $a \cdot (b + c) = a \cdot b + a \cdot c$ and $(a + b) \cdot c = a \cdot c + b \cdot c$

If, in addition, $\exists 1_A \in A$ such that $1_A \cdot a = a \cdot 1_A = a$ for all $a \in A$, then A is a ring with identity. If also $a \cdot b = b \cdot a$ for all $a, b \in A$, then A is commutative.

Remark

Throughout these notes, ring means commutative ring with identity.

Example.

1. $M_n(\mathbb{R}) = \left\{ \left(a_{ij}\right)_{n \times n} : a_{ij} \in \mathbb{R} \right\}$, and the operations are defined as usual matrix addition and multiplication. Then $(M_n(\mathbb{R}), +)$ is an abelian group and $(M_n(\mathbb{R}), \cdot)$ is a semigroup, but not commutative.
2. $k[x] = \left\{ f(x) = \sum_{i=0}^{n} a_i x^i : a_i \in k, n \in \mathbb{N} \right\}$, then $k[x]$ is a commutative ring with identity.
3. $k[x_1, ..., x_n]$ is a ring.

Definition 1.1.2 (Homomorphism) Let A, B be two rings. A map $\varphi : A \to B$ is called a homomorphism if

1. $\varphi(a + b) = \varphi(a) + \varphi(b)$
2. $\varphi(ab) = \varphi(a) \cdot \varphi(b)$
3. $\varphi(1_A) = 1_B$

Remark

If $f : A \to B, g : B \to C$ are ring homomorphisms, then $g \circ f : A \to C$ is a homomorphism.

Example. Let φ be a homomorphism between two rings A, B, we define

$$\ker \varphi = \{a \in A : \varphi(a) = 0\} \tag{1.1}$$

Obviously, $\ker\varphi$ is an ideal of A, and

$$\forall b \in A, a \in \ker\varphi, \Rightarrow \varphi(b \cdot a) = \varphi(b) \cdot \varphi(a) = \varphi(b) \cdot 0 = 0 \tag{1.2}$$

1.2. Ideals and Quotient Rings

Definition 1.2.1 (Ideal) Let $\mathfrak{a} \subset A$. If $\mathfrak{a}$ is a subgroup of $(A, +)$ and $\forall a \in A, b \in \mathfrak{a}$, $a \cdot b \in \mathfrak{a}$, then $\mathfrak{a}$ is an ideal of A.

Definition 1.2.2 (Quotient) Let $\mathfrak{a}$ is an ideal of ring A, then $A/\mathfrak{a}$ is a ring defined as follows:

$$A/\mathfrak{a} = \{a + \mathfrak{a} : a \in A\} \tag{1.3}$$

where the $a + \mathfrak{a}$ is the equivalence class of a, or residue class of a.

Remark

Let $\mathfrak{a}$ be an ideal of A, there is a surjective homomorphism

$$\varphi : A \to A/\mathfrak{a}, \quad \varphi(a) = a + \mathfrak{a} \tag{1.4}$$

Proposition 1.2.3 Let $\mathfrak{a}$ be an ideal of A. The ideals of $A/\mathfrak{a}$ are in one-to-one correspondence with the ideals $\mathfrak{b}$ of A such that $\mathfrak{a} \subset \mathfrak{b}$, by

$$\mathfrak{b} \mapsto \mathfrak{b}/\mathfrak{a} = \{b + \mathfrak{a} : b \in \mathfrak{b}\}. \tag{1.5}$$

1.3. Zero-divisors, Nilpotents and units

Definition 1.3.1 (Zero-divisor) x is a zero-divisor of A if $\exists y \neq 0 \in A$, s.t. $x \cdot y = 0$

A ring A with $1 \neq 0$ and no non-zero zero-divisors is called an integral domain.

Definition 1.3.2 (Nilpotent) x is a nilpotent of A if $\exists n \in \mathbb{Z}_+$, s.t. $x^n = 0 (n > 0)$

Remark

A nilpotent element is a zero-divisor unless $A = 0$, but not conversely in general.

Definition 1.3.3 (Unit) x is a unit of A if $\exists 1 y \in A$, s.t. $x \cdot y = 1_A$

Remark

The element y is then uniquely determined by x and is written x^{-1}. The units of A form a multiplicative abelian group.

Definition 1.3.4 (Principal) An ideal $\mathfrak{a}$ is principal if $\exists a \in A$ such that $\mathfrak{a} = (a) = \{ab : b \in A\}$.

Definition 1.3.5 (Field) A is a field if $\forall a \neq 0 \in A$ is unit.

In other words, A is a field $\Leftrightarrow$ 0 is the only non-unit.

Proposition 1.3.6 Let $A \neq 0$ be a ring. Then the following are equivalent:
1. A is a field
2. The only ideals in A are 0 and (1)
3. For every non-zero ring B, every ring homomorphism $\varphi : A \to B$ is injective.

Proof. $1 \Rightarrow 2$: Let $\mathfrak{a} \neq 0$ be an ideal of A. For any $0 \neq x \in \mathfrak{a}$, x is a unit. Hence $\mathfrak{a} \supset (x) = (1)$, so $\mathfrak{a} = (1)$.

$2 \Rightarrow 3$: Let $\varphi : A \to B$ be a homomorphism. Since $B \neq 0$, $\ker(\varphi) \neq (1)$. Hence $\ker(\varphi) = 0$, so φ is injective.

$3 \Rightarrow 1$: Let $x \in A$ be a non-unit. Then $(x) \neq (1)$, so $B = A/(x)$ is non-zero. The quotient map $\varphi : A \to B, \quad a \mapsto a + (x)$ is injective by (3), hence $(x) = \ker(\varphi) = 0$. Therefore every non-zero element of A is a unit, so A is a field. $\square$

1.4. Prime ideals and maximal ideals

Definition 1.4.1 (Prime ideal) An ideal $\mathfrak{p} \subset A$ is prime ideal if

$$\mathfrak{p} \neq (1) \land (xy \in \mathfrak{p} \Rightarrow x \in \mathfrak{p} \lor y \in \mathfrak{p}) \tag{1.6}$$

Definition 1.4.2 (Maximal ideal) An ideal $\mathfrak{m} \subset A$ is maximal ideal if

$$\mathfrak{m} \neq (1) \land (\mathfrak{m} \subset \mathfrak{a} \subset A \Rightarrow \mathfrak{a} = \mathfrak{m} \text{ or } \mathfrak{a} = A) \tag{1.7}$$

Remark

1. $\mathfrak{p}$ is prime $\Rightarrow A/\mathfrak{p}$ is an integral domain
2. $\mathfrak{m}$ is maximal $\Rightarrow A/\mathfrak{m}$ is a field

Hence a maximal ideal is prime ideal, but not conversely. The 0 is prime $\Leftrightarrow A$ is an integral domain.

Prime ideals are fundamental to the whole of commutative algebra. The following theorem and corollaries ensure that there is always a sufficient supply of them.

Theorem 1.4.3 $\forall A \neq 0$ is a ring has at least one maximal ideal.

Corollary 1.4.3.1 If $\mathfrak{a} \neq (1)$ is an ideal of A, then $\exists \mathfrak{m}$ is a maximal ideal of A s.t. $\mathfrak{a} \subset \mathfrak{m}$.

Corollary 1.4.3.2 Every non-unit $a \in A$ belongs to some maximal ideal of A.

Proof. Since a is not a unit, $(a) \neq (1)$. By the previous corollary, there is a maximal ideal $\mathfrak{m}$ such that $(a) \subset \mathfrak{m}$. Hence $a \in \mathfrak{m}$. □

Proposition 1.4.4

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

Definition 1.4.5 (Local ring) A ring A is a local ring if A has a unique maximal ideal.

1.5. Nilradical and Jacobson radical

Proposition 1.5.1 The set $\mathfrak{N}$ of all nilpotent elements in A is an ideal, and $A/\mathfrak{N}$ has no non-zero nilpotent elements.

Proof. Let $\mathfrak{N} = \{x : x \text{ is nilpotent element in } A\}$, then

$$\begin{gathered} \forall a \in A, ax \in \mathfrak{N}, (x^n = 0 \Rightarrow (ax)^n = a^n x^n = 0 \in \mathfrak{N}) \\ \forall x, y \in \mathfrak{N}, x^m = 0, y^n = 0 \Rightarrow (x+y)^{m+n+1} = 0 \in \mathfrak{N} \Rightarrow x + y \in \mathfrak{N} \end{gathered} \tag{1.8}$$

Hence $\mathfrak{N}$ is an ideal of A. If $\overline{x} = x + \mathfrak{N}$ is nilpotent in $A/\mathfrak{N}$, then $\overline{x}^n = 0$ for some $n > 0$, so $x^n \in \mathfrak{N}$. Hence $(x^n)^m = 0$ for some $m > 0$, and therefore $x^{nm} = 0$. Thus $x \in \mathfrak{N}$ and $\overline{x} = 0$. □

Definition 1.5.2 (Nilradical) The ideal $\mathfrak{N}$ is called the nilradical of A.

Proof. Let $\mathfrak{N}' = \cap\, \mathfrak{p}$, where $\mathfrak{p}$ runs over all prime ideals of A. If $f \in A$ is nilpotent, then $f^n = 0 \in \mathfrak{p}$ for every prime ideal $\mathfrak{p}$, hence $f \in \mathfrak{p}$ for every $\mathfrak{p}$ and $f \in \mathfrak{N}'$.

Conversely, suppose f is not nilpotent. Let $S = \{1, f, f^2, \ldots\}$. Then $0 \notin S$. By the standard maximal ideal argument applied to ideals disjoint from S, there is a prime ideal $\mathfrak{p}$ with $\mathfrak{p} \cap S = \varnothing$. Hence $f \notin \mathfrak{p}$, so $f \notin \mathfrak{N}'$. □

Proposition 1.5.3 Let $\mathfrak{N}$ be the nilradical of A. Then $\mathfrak{N} = \cap\, \mathfrak{p}$, where $\mathfrak{p}$ runs over all prime ideals of A.

Definition 1.5.4 (Jacobson radical) The Jacobson radical $\mathfrak{R}$ of A is defined to be $\mathfrak{R} = \cap\, \mathfrak{m}$, where $\mathfrak{m}$ is the maximal ideal of A.

Proposition 1.5.5 $x \in \mathfrak{R} \Leftrightarrow 1 - xy$ is a unit in $A, \forall y \in A$

Proof. [$\Rightarrow$] Suppose $1 - xy$ is not unit in A, then $\exists \mathfrak{m}$, s.t. $1 - xy \in \mathfrak{m}$ by Corollary 1.4.3.2 , but $\mathfrak{R} = \cap\, \mathfrak{m}$. Hence $xy \in \mathfrak{m} \Rightarrow 1 \in \mathfrak{m}$, which is a contradiction.

[$\Leftarrow$] Suppose $x \notin \mathfrak{R}$. Then $\exists \mathfrak{m}$ maximal such that $x \notin \mathfrak{m}$. Since $\mathfrak{m}$ is maximal,

$$\mathfrak{m} \subset (x) + \mathfrak{m} = (1) \Rightarrow \exists y \in A, z \in \mathfrak{m}, \text{s.t. } xy + z = 1 \Rightarrow z = 1 - xy \Rightarrow \mathfrak{m} = (1), \tag{1.9}$$

so $1 - xy \in \mathfrak{m}$ is not a unit. This contradicts the hypothesis. □

1.6. Operations on Ideals

1. Sum: $\mathfrak{a} + \mathfrak{b} = \{x + y : x \in \mathfrak{a}, y \in \mathfrak{b}\}$ is an ideal.
2. Intersection: $\mathfrak{a} \cap \mathfrak{b} = \{z : z \in \mathfrak{a} \cap \mathfrak{b}\}$ is an ideal.
3. Product: $\mathfrak{a} \cdot \mathfrak{b} = \{\sum x_i y_i : x_i \in \mathfrak{a}, y_i \in \mathfrak{b}\}$ is an ideal.

The three operations so far defined are commutative and associative. Also there is a distributive law

$$\mathfrak{a} \cdot (\mathfrak{b} + \mathfrak{c}) = \mathfrak{a} \cdot \mathfrak{b} + \mathfrak{a} \cdot \mathfrak{c} \tag{1.10}$$

Proof. ($\subset$) Let $z \in \mathfrak{a}(\mathfrak{b} + \mathfrak{c}) \Rightarrow z = \sum a_i(b_i + c_i) = \sum a_i b_i + \sum a_i c_i \in \mathfrak{ab} + \mathfrak{ac}$

($\supset$) obviously. □

Definition 1.6.1 (Coprime) $\mathfrak{a}, \mathfrak{b}$ are said to be coprime if $\mathfrak{a} + \mathfrak{b} = (1)$, equivalently if $\exists x \in \mathfrak{a}, y \in \mathfrak{b}$ such that $x + y = 1$.

Remark

Thus for coprime ideals we have $\mathfrak{a} \cap \mathfrak{b} = \mathfrak{a} \cdot \mathfrak{b}$.

Proof. Since $\mathfrak{a}\cdot\mathfrak{b}\subset\mathfrak{a}\cap\mathfrak{b}$ is clear, only prove the reverse inclusion. Choose $x\in\mathfrak{a}, y\in\mathfrak{b}$ with $x+y=1$. If $z\in\mathfrak{a}\cap\mathfrak{b}$, then $z=z(x+y)=zx+zy\in\mathfrak{a}\mathfrak{b}$. ☐

4. Direct Product: Let $A_1, \ldots A_n$ be rings, put $A=\prod_{i=1}^n A_i$. Then A is a ring and

$$\begin{aligned} +: A\times A\to A, &\quad (x_1,\ldots,x_n),(y_1,\ldots,y_n)\mapsto(x_1+y_1,\ldots,x_n+y_n) \\ \cdot: A\times A\to A, &\quad (x_1,\ldots,x_n),(y_1,\ldots,y_n)\mapsto(x_1y_1,\ldots,x_ny_n) \end{aligned} \tag{1.11}$$

we call A is a the direct product of A_i and $P_i: A\to A_i, (x_1,\ldots,x_n)\mapsto x_i$ is a surjective homomorphism

Proposition 1.6.2 Let A be a ring and let $\mathfrak{a}_i$ be ideals of A.

$$\varphi: A\to\prod A/\mathfrak{a}_i,\quad x\mapsto(x+\mathfrak{a}_1,\ldots,x+\mathfrak{a}_n) \tag{1.12}$$

then
1. If $\mathfrak{a}_i+\mathfrak{a}_j=(1)(i\neq j)\Rightarrow\prod\mathfrak{a}_i=\cap\,\mathfrak{a}_i$
2. φ is surjective $\Leftrightarrow\mathfrak{a}_i+\mathfrak{a}_j=(1)$
3. φ is injective $\Leftrightarrow\cap\,\mathfrak{a}_i=0$

Proof. (3). $\{0\}=\ker(\varphi)=\varphi^{-1}(0,\ldots,0)=\{x\in A: x\in\mathfrak{a}_k, k=1,\ldots,n\}=\cap\,\mathfrak{a}_i$ ☐

5. Union: If $\mathfrak{a}_1,\mathfrak{a}_2$ are ideals of A, then $\mathfrak{a}_1\cup\mathfrak{a}_2$ isn't ideal in general.

Proposition 1.6.3
1. Let $\mathfrak{p}_1,\ldots,\mathfrak{p}_n$ be prime ideals, $\mathfrak{a}$ be an ideal and $\mathfrak{a}\subset\cup_{i=1}^n\mathfrak{p}_i$, then $\mathfrak{a}\subset\mathfrak{p}_i$ for some i
2. Let $\mathfrak{a}_1,\ldots,\mathfrak{a}_n$ be ideals, $\mathfrak{p}$ be prime ideal and $\mathfrak{p}\supset\cap_{i=1}^n\mathfrak{a}_i$, then $\mathfrak{p}\supset\mathfrak{a}_i$ for some i

6. Quotient:

$$\begin{aligned} (\mathfrak{a}:\mathfrak{b})&=\{x\in A, x\mathfrak{b}\subset\mathfrak{a}\}, \\ \operatorname{Ann}(\mathfrak{b})=(0:\mathfrak{b})&=\{x\in A: x\mathfrak{b}=0\} \end{aligned} \tag{1.13}$$

Specially, if $\mathfrak{b}=(x)$ is principal, then $(\mathfrak{a}:\mathfrak{b})=(\mathfrak{a}:x)$. Let D be the set of zero-divisors in A; then $D=\cup_{x\neq 0}\operatorname{Ann}(x)$.

7. Radical

$$r(\mathfrak{a})=\{x\in A:\exists n>0,\text{s.t. } x^n\in\mathfrak{a}\}, \tag{1.14}$$

obviously, we can get $\mathfrak{a}\subset r(\mathfrak{a})$

Proposition 1.6.4 $r(\mathfrak{a})=\cap\,\mathfrak{p}$, where $\mathfrak{p}$ runs over all prime ideals of A such that $\mathfrak{a}\subset\mathfrak{p}$.

Proof. Apply Proposition 1.5.3 to $A/\mathfrak{a}$. The prime ideals of $A/\mathfrak{a}$ correspond to prime ideals $\mathfrak{p}$ of A containing $\mathfrak{a}$, and the nilradical of $A/\mathfrak{a}$ is $r(\mathfrak{a})/\mathfrak{a}$. ☐

Proposition 1.6.5 D is the set of zero-divisors of A, then $D = \cup_{x\neq 0} r(\mathrm{Ann}(x))$.

Proof. $D = r(D) = r\left(\cup_{x\neq 0} \mathrm{Ann}(x)\right) = \cup_{x\neq 0} r(\mathrm{Ann}(x))$ □

Proposition 1.6.6 Let $\mathfrak{a}, \mathfrak{b}$ be ideals in ring A, s.t. $r(\mathfrak{a}) + r(\mathfrak{b}) = (1) \Rightarrow \mathfrak{a} + \mathfrak{b} = (1)$

Proof. $r(\mathfrak{a} + \mathfrak{b}) = r(r(\mathfrak{a}) + r(\mathfrak{b})) = r(1) \Rightarrow \mathfrak{a} + \mathfrak{b} = (1)$ □

8. Extension and contraction

Let $f : A \to B$ is a homomorphism, $\mathfrak{a} \subset A, \mathfrak{b} \subset B$ is ideals then

$$\mathfrak{b}^c = f^{-1}(\mathfrak{b}) = \{a \in A : f(a) \in \mathfrak{b}\} \tag{1.15}$$

is a ideal of A, called contraction, but

$$f(\mathfrak{a}) = \{b \in B : \exists a \in \mathfrak{a}, \text{s.t. } f(a) = b\} \tag{1.16}$$

is not ideal of B in general. We let $\mathfrak{a}^e =< f(\mathfrak{a}) >$ is the ideal of B, called extension.

Proposition 1.6.7 Let $f : A \to B$ is a homomorphism, $\mathfrak{a} \subset A, \mathfrak{b} \subset B$ is ideals then

1. $\mathfrak{a} \subset \mathfrak{a}^{ec}, \mathfrak{b} \supset \mathfrak{b}^{ce}$
2. $\mathfrak{a}^e = \mathfrak{a}^{ece}, \mathfrak{b}^c = \mathfrak{b}^{cec}$
3. If C is the set of contracted ideals in A and E is the set of extended ideals in B, then

$$C = \{\mathfrak{a} : \mathfrak{a}^{ec} = \mathfrak{a}\}, E = \{\mathfrak{b} : \mathfrak{b}^{ce} = \mathfrak{b}\} \tag{1.17}$$

and $\varphi : \mathfrak{a} \to \mathfrak{a}^e$ is a bijection, where inverse map is $\varphi^{-1} : \mathfrak{b} \to \mathfrak{b}^c$

2. Modules

2.1. Modules and module homomorphisms

Definition 2.1.1 (Module) Let A be a ring, M be an abelian group. M is a A-module if exist map

$$\varphi : A \times M \to M \tag{2.1}$$

s.t $\forall a, b \in A, m_1, m_2 \in M$

1. $\varphi(a, m_1 + m_2) = \varphi(a, m_1) + \varphi(a, m_2)$
2. $\varphi(a + b, m) = \varphi(a, m) + \varphi(b, m)$
3. $\varphi(ab, m) = \varphi(a, \varphi(b, m))$
4. $\varphi(1_A, m) = m$

Remark

For express, we write $\varphi(a, m) = a \cdot m$, where $a \in A, m \in M$.

Definition 2.1.2 (Homomorphism) Let M, N be A-modules. $f : M \to N$ is a homomorphism if

$$f(m_1 + m_2) = f(m_1) + f(m_2), \quad f(am) = af(m), \forall a \in A, m, m_1, m_2 \in M \tag{2.2}$$

Definition 2.1.3 (Hom) Let M, N be A-modules, set

$$\mathrm{Hom}_A(M, N) = \{f : M \to N : f \text{ is a homomorphism}\} \tag{2.3}$$

Proposition 2.1.4 $\mathrm{Hom}_A(M, N)$ is a A-module

Proof. $\forall f_1, f_2 \in \mathrm{Hom}_A(M, N), x \in M, a \in A$, then

$$(f_1 + f_2)(x) = f_1(x) + f_2(x), \quad (af)(x) = af(x) \tag{2.4}$$

□

For any A-module M, there is a natural isomorphism $\mathrm{Hom}_A(A, M) \cong M$.

2.2. Submodule and quotient module

Definition 2.2.1 (Submodule) A submodule M' of M if $M' \subset M$ is subgroup and M' is A-module.

Definition 2.2.2 (Quotient module) Let M' be a submodule of M, then

$$M/M' = \{m + M' : m \in M\} \tag{2.5}$$

is a quotient module.

Obviously, we get a natural surjective homomorphism $\pi : M \to M/M', \quad m \mapsto m + M'$.

Example. If $f : M \to N$ is an A-module homomorphism, then

$$\begin{gathered} \ker(f) = \{x \in M : f(x) = 0\} \text{ is submodule of M} \\ \mathrm{Im}(f) = f(M) \text{ is submodule of N} \\ \mathrm{Coker}(f) = N/\mathrm{Im}(f) \text{ is quotient module of N} \end{gathered} \tag{2.6}$$

If $M' \subset M$ is submodule, s.t. $M' \subset \ker(f)$, let

$$\overline{f} = M/M' \to N, \quad \overline{x} \mapsto \overline{f}(\overline{x}) = f(x) \tag{2.7}$$

we get $\ker\left(\overline{f}\right) = \ker(f)/M'$, if we set $M' = \ker(f)$, we can get $M/\ker(f) \cong \mathrm{Im}(f)$.

2.3. Operations on submodule

1. Sum

$$\sum_{i \in I} M_i = \left\{m = \sum x_i : x_i \in M_i, x_i = 0 \text{ except for finitely many } i\right\} \tag{2.8}$$

is a submodule.

2. Intersection

$$\cap_{i \in I} M_i = \{m : m \in M_i, \forall i \in I\} \tag{2.9}$$

is a submodule. Thus the submodules of M form a complete lattice with respect to inclusion.

Proposition 2.3.1

1. If $L \supset M \supset N$ are A-module, then $(L/N)/(M/N) \cong L/M$.
2. If M_1, M_2 are submodule of M. then $(M_1 + M_2)/M_1 \cong M_2/(M_1 \cap M_2)$

Proof.

1. set

$$f : L/N \to L/M, \quad f(l + N) = l + M \tag{2.10}$$

we can simarly proof f is well-define and $\ker(f) = M/N$. Hence

$$(L/N)/\ker(f) = \mathrm{Im}(f) \Rightarrow (L/N)/(M/N) = L/M \tag{2.11}$$

2. set $g : M_2 \to (M_1 + M_2)/M_1$, like 1., g is surjective, and $\ker(g) = M_1 \cap M_2$.

$\square$

3. Quotient: Let M_1, M_2 are submodule of M, then

$$(M_1 : M_2) = \{r \in A : rM_2 \subset M_1\} \tag{2.12}$$

is an ideal of A. In particular, $\mathrm{Ann}(M) = (0 : M) = \{a \in A : aM = 0\}$ is called the annihilator of M.

If $\mathfrak{a} \subset \mathrm{Ann}(M)$, we can regard M as a $A/\mathfrak{a}$-module, then

$$f : A/\mathfrak{a} \times M \to M, \quad (\overline{a}, m) \mapsto am \tag{2.13}$$

where $\overline{a} = a + \mathfrak{a}$.

A-module is faithful if $\mathrm{Ann}(M) = 0$. If $\mathrm{Ann}(M) = \mathfrak{a}$, then M is faithful as $A/\mathfrak{a}$-module.

4. Direct Sum: Set M_i is A-module, then $\oplus\, M$ is a A-module (and abelian group), $|I| < \infty$,

$$\begin{gathered} (x_1, ...x_n) + (y_1, ...y_n) = (x_1 + y_1, ...x_n + y_n) \in \oplus\, M_i \\ a(x_1, ...x_n) = (ax_1, ...ax_n) \in \oplus\, M_i \end{gathered} \tag{2.14}$$

where almost all $x_i = 0$ except finitely many i. If we drop the restriction on the number of non-zero components, we get the direct product $\prod M_i$.

Remark

In other words, the direct sum is the direct product of A-modules with the restriction that only finitely many components are non-zero. They are the same if $|I| < \infty$.

If set

$$\mathfrak{a} =< (0, ..., 0, 1, 0, ..., 0) >= \{(0, ..., 0, a_i, 0, ..., 0) : a_i \in A_i\} \tag{2.15}$$

the ring A considered as A-module as: $A = \oplus_{i \in I}\, \mathfrak{a}_i$

Remark

Give a module decomposition $A = \oplus_{i=1}^n\, \mathfrak{a}_i$ of A as a direct sum of ideals, we have

$$A \cong \prod_{i=1}^n (A/\mathfrak{b}_i), \tag{2.16}$$

where $\mathfrak{b}_i = \oplus_{j \neq i}\, \mathfrak{a}_j$. Each ideal $\mathfrak{a}_i$ is a ring (isomorphic to $A/\mathfrak{b}_i$). The identity element $e_i \in \mathfrak{a}_i$ is an idempotent in A, and $\mathfrak{a}_i = (e_i)$.

Definition 2.3.2 (f.g. module) M is a finite generated A-module, if

$$x_1, ...x_n \in M, \text{s.t. } M = \sum_{i=1}^n Ax_i \left(\text{i.e. } \forall m \in M, \exists a_i \in A, \text{s.t. } m = \sum_{i=1}^n a_i x_i. \right) \tag{2.17}$$

Definition 2.3.3 (f.g. free module) M is a f.g. free A-module if $M = \oplus_{i=1}^{n} A_i$, where each $A_i \cong A$ as an A-module.

Proposition 2.3.4 M is f.g. A-module $\Leftrightarrow M \cong A^n/K$, where K is a submodule of A^n and $n > 0$.

Proof. [=>]Suppose $x_1, ..., x_n$ is generators of M,

$$\varphi : A^n \to M, \quad (a_1, ...a_n) \mapsto \sum_{i=1}^{n} a_i x_i \tag{2.18}$$

so φ is surjective, hence $M \cong A^n / \ker(\varphi)$

[<=] Obviously. □

Definition 2.3.5 (endomorphism) Let M be a A-module, $\varphi : M \to M$ is an endomorphism of M if φ is a homomorphism.

$\mathrm{End}_A(M) = \{\varphi : \varphi \text{ is endmomorphism of } M\}$

Proposition 2.3.6 Let M be a f.g. A-module, $\mathfrak{a}$ is ideal of A, and $\varphi : M \to M$ be an A-module endomorphism, such that. $\varphi(M) \subset \mathfrak{a}M$, then φ is satisfied the following

$$\varphi^n + a_1\varphi^{n-1} + ... + a_n = 0, \quad a_i \in \mathfrak{a} \tag{2.19}$$

Corollary 2.3.6.1 Let M be f.g. A-module, and $\mathfrak{a}$ is ideal of A, s.t. $\mathfrak{a}M = M$, then $\exists x = 1 \bmod \mathfrak{a}$, s.t. $x \cdot M = 0$

Proof. Let $\varphi = \mathrm{id}, x = 1 + a_1 + ... + a_n \Rightarrow x \cdot M = 0$ by Proposition 2.3.6 □

Lemma 2.3.7 (Nakayama) Let M be f.g. A-module, $\mathfrak{a}$ is ideal of A and $\mathfrak{a} \subset \mathfrak{R}$. Then $\mathfrak{a}M = M \Rightarrow M = 0$.

Proof. By Corollary 2.3.6.1, we have $xM = 0 (\forall x = 1 \bmod \mathfrak{R})$, hence x is a unit of A, so $M = x^{-1}xM = 0$ □

Corollary 2.3.7.1 Let M be f.g. A-module, N is submodule of M, $\mathfrak{a} \subset \mathfrak{R}$ is ideal, then $M = \mathfrak{a}M + N \Rightarrow M = N$.

Proof. Apply Lemma 2.3.7 to M/N, we get

$$M/N = (\mathfrak{a}M + N)/N = \mathfrak{a}(M/N) \Rightarrow M = N \tag{2.20}$$

□

Proposition 2.3.8 A is local ring, $\mathfrak{m}$ is the maximal ideal of A, $A/\mathfrak{m}$ is the residue field of A.

M is f.g. A-module, $\mathfrak{m}M$ is submodule of M, $M/\mathfrak{m}M$ is $A/\mathfrak{m}$-module. We have natural homomorphism

$$\varphi : M \to M/\mathfrak{m}M, \quad x \mapsto \varphi(x) = x + \mathfrak{m}M \tag{2.21}$$

Let $x_1, ...x_n \in M$, s.t. $\{\varphi(x_i)\}_{i=1}^n$ are basis of $M/\mathfrak{m}M$, then $x_1, ...x_n$ generator M.

Proof. Let N be the submodule of M generated be $\{x_1, ..., x_n\}$, then

$$N \xrightarrow{\tau} M \xrightarrow{\varphi} M/\mathfrak{m}M, \quad x \mapsto x \mapsto x + \mathfrak{m}M \tag{2.22}$$

$\varphi \circ \tau$ is surjective homomorphism, so $N + \mathfrak{m}M \cong M \Rightarrow M \cong N$ by Corollary 2.3.7.1 □

2.4. Exact sequences

Definition 2.4.1 (Exact sequence) A sequence of A-modules and homomorphisms

$$... \to M_{i-1} \xrightarrow{f_i} M_i \xrightarrow{f_{i+1}} M_{i+1} \to ... \tag{2.23}$$

is exact at M_i, if $\mathrm{Im}(f_i) = \ker(f_{i+1})$. The sequence is exact if it is exact at every M_i. In particular,

$$\begin{aligned} 0 \to M' \xrightarrow{f} M & \text{ is exact} \Leftrightarrow f \text{ is injective} \\ M \xrightarrow{g} M'' \to 0 & \text{ is exact} \Leftrightarrow g \text{ is surjective} \\ 0 \to M' \xrightarrow{f} M \xrightarrow{g} M'' \to 0 & \text{ is exact} \Leftrightarrow f \text{ is injective}, g \text{ is surjective}, \wedge \mathrm{Im}(f) = \ker(g) \end{aligned} \tag{2.24}$$

and g induces a isomorphism of $\mathrm{Coker}(f) = M/f(M')$ onto M''

A sequence of type Equation (2.24) is called short exact sequence. Any long exact sequence Equation (2.23) can be split up into short exact sequence, if $N_i = \mathrm{Im}(f_i) = \ker(f_{i+1})$, we have short exact sequence

$$0 \to N_i \to M_i \to N_{i+1} \to 0, \quad \forall i \tag{2.25}$$

Proposition 2.4.2

1. Let a sequence of A-modules and homomorphisms,

$$M' \xrightarrow{u} M \xrightarrow{v} M'' \to 0 \tag{2.26}$$

then the sequence Equation (2.26) is exact $\Leftrightarrow \forall N$, the sequence

$$0 \to \mathrm{Hom}(M'', N) \xrightarrow{\overline{v}} \mathrm{Hom}(M, N) \xrightarrow{\overline{u}} \mathrm{Hom}(M', N) \tag{2.27}$$

is exact.

2. Let a sequence of A-module and homo-

$$0 \to N' \xrightarrow{u} N \xrightarrow{v} N'' \tag{2.28}$$

then the sequence Equation (2.28) is exact $\Leftrightarrow \forall M$ the sequence

$$0 \to \mathrm{Hom}(M, N') \xrightarrow{\overline{u}} \mathrm{Hom}(M, N) \xrightarrow{\overline{v}} \mathrm{Hom}(M, N'') \tag{2.29}$$

is exact.

Proposition 2.4.3 Let

$$\begin{tikzcd}
0 \arrow[r] & M' \arrow[r, "u"] \arrow[d, "f'"] & M \arrow[r, "v"] \arrow[d, "f"] & M'' \arrow[r] \arrow[d, "f''"] & 0 \\
0 \arrow[r] & N' \arrow[r, "u'"] & N \arrow[r, "v'"] & N'' \arrow[r] & 0
\end{tikzcd}$$

be a commutative diagram of A-modules and homomorphisms, with the rows exact. Then there exists an exact sequence

$$0 \to \ker(f') \xrightarrow{\overline{u}} \ker(f) \xrightarrow{\overline{v}} \ker(f'') \xrightarrow{d} \mathrm{Coker}(f') \xrightarrow{\overline{u}'} \mathrm{Coker}(f) \xrightarrow{\overline{v}'} \mathrm{Coker}(f'') \tag{2.30}$$

in which $\overline{u}, \overline{v}$ are restrictions of u, v, and $\overline{u}', \overline{v}'$ are induced by u', v'.

Proof. Define the connecting homomorphism $d : \ker(f'') \to \mathrm{Coker}(f')$. For $x'' \in \ker(f'')$, choose $x \in M$ with $v(x) = x''$. Then

$$v'(f(x)) = f''(v(x)) = f''(x'') = 0, \tag{2.31}$$

so $f(x) \in \ker(v') = \mathrm{Im}(u')$. Since u' is injective, there is a unique $y' \in N'$ such that $u'(y') = f(x)$. Set

$$d(x'') = y' + \mathrm{Im}(f') \in \mathrm{Coker}(f'). \tag{2.32}$$

This is well-defined: if x is replaced by $x + u(m')$, then y' is replaced by $y' + f'(m')$, which gives the same class in $\mathrm{Coker}(f')$.

Exactness at $\ker(f')$ and $\ker(f)$ follows by restricting the exact top row. For exactness at $\ker(f'')$, if $x'' = v(x)$ with $f(x) = 0$, then $d(x'') = 0$. Conversely, if $d(x'') = 0$, choose x, y'

as above and write $y' = f'(m')$. Then $f(x - u(m')) = 0$ and $v(x - u(m')) = x''$, so $x'' \in \operatorname{Im}(\overline{v})$.

For exactness at $\operatorname{Coker}(f')$, the image of d is contained in $\ker(\overline{u}')$ by construction. Conversely, if $y' + \operatorname{Im}(f') \in \ker(\overline{u}')$, then $u'(y') = f(x)$ for some $x \in M$. Thus $f''(v(x)) = v'(f(x)) = v'u'(y') = 0$, so $v(x) \in \ker(f'')$ and $d(v(x)) = y' + \operatorname{Im}(f')$. Exactness at $\operatorname{Coker}(f)$ and $\operatorname{Coker}(f'')$ follows from exactness of the bottom row. □

Remark

Proposition 2.4.3 is a special case of the exact homology sequence of homological algebra.

Definition 2.4.4 Let C be a class of A-modules and λ be a function on C, the function λ is additive, if

$$\forall \text{ exact sequence } 0 \to M' \to M \to M'' \to 0 \Rightarrow \lambda(M') - \lambda(M) + \lambda(M'') = 0 \tag{2.33}$$

Example. Let A be a field over $\mathbb{K}$, C be the class of all finite-dim $\mathbb{K}$-vertor space, the $V \to \dim(V)$ is an additive function on C.

Proposition 2.4.5 Let $0 \to M_0 \to M_1 \to \ldots \to M_m \to 0$ be an exact sequence of A-modules, in which all the modules M_i and the kernels of all the homomorphisms belong to C. Then for any additive function λ on C, we have

$$\sum_{i=0}^{m} (-1)^i \lambda(M_i) = 0 \tag{2.34}$$

.

Proof. Split the sequence into short exact sequences

$$0 \to N_i \to M_i \to N_{i+1} \to 0, \quad \text{where } (N_0 = N_{n+1} = 0) \tag{2.35}$$

then we get $\lambda(M_i) = \lambda(N_i) + \lambda(N_{i+1})$. Now take the alternative sum of the $\lambda(M_i)$. □

2.5. Tensor product of modules

Definition 2.5.1 (Tensor product) We construct an A-module T, called the tensor product of M and N, with the property that for every A-module P, the A-bilinear maps $M \times N \to P$ are in natural one-to-one correspondence with the A-linear maps $T \to P$.

Proposition 2.5.2 Let M, N, T be A-module, then there exist a pair (T, g), where $g : M \times N \to T$ is bilinear map, with the following properties

$$\begin{gathered}\forall \text{ A-module } P, f: M\times N\to P \text{ is bilinear map}\\ \exists 1 f': T\to P \text{ is linear map, s.t. } f = f'\circ g.\end{gathered} \tag{2.36}$$

Moreover, if $(T,g),(T',g')$ are two pair with this property, then $\exists 1$ isomorphism

$$\tau: T\to T' \text{ s.t. } \tau\circ g = g' \tag{2.37}$$

Corollary 2.5.2.1 Let $x_i\in M, y_i\in N$, s.t. $\sum x_i\otimes y_i = 0\in M\otimes N$, then exist f.g. submodule M_0 of M, N_0 of N, s.t. $\sum x_i\otimes y_i = 0\in M_0\otimes N_0$

Proof. Let C denote the free A-module $A^{M\times N}$, and let D be the submodule generated by the usual bilinearity relations. If

$$\sum x_i\otimes y_i = 0 \Rightarrow \sum x_i\otimes y_i\in D\Rightarrow \sum x_i\otimes y_i \text{ is finite sum of generator of } D \tag{2.38}$$

The displayed relation uses only finitely many generators of D, hence only finitely many elements of M and N. Let M_0 and N_0 be the submodules generated by those elements. Then $\sum x_i\otimes y_i = 0$ already in $M_0\otimes N_0$. □

In particular, if M, N are f.g. A-module, so is $M\otimes N$.

Proposition 2.5.3 Let M, N, P be A-module, then exists unique isomorphism, s.t.

$$M\otimes N\to N\otimes M,\quad x\otimes y\mapsto y\otimes x \tag{2.39}$$

$$\begin{gathered}(M\otimes N)\otimes P\to M\otimes(N\otimes P)\to M\otimes N\otimes P\\ (x\otimes y)\otimes z\mapsto x\otimes(y\otimes z)\mapsto x\otimes y\otimes z\end{gathered} \tag{2.40}$$

$$(M\oplus N)\otimes P\to(M\otimes P)\oplus(N\otimes P),\quad (x,y)\otimes z\mapsto(x\otimes z, y\otimes z) \tag{2.41}$$

$$A\otimes M\to M,\quad a\otimes x\mapsto ax \tag{2.42}$$

2.6. Restriction and extension of scalars

Definition 2.6.1 Let $f: A\to B$ be a ring homomorphism and let N be a B-module. Then N has an A-module structure defined as

$$\forall a\in A, x\in N,\quad (a,x)\mapsto f(a)\cdot x \tag{2.43}$$

This A-module is said to be obtained from N by restriction of scalars. In particular, f defines in this way an A-module structure on B.

Proposition 2.6.2 Suppose N is f.g. B-module and B is f.g. A-module, then N is f.g. as an A-module.

Proof. Let $y_1, ..., y_n$ generate N over B and $x_1, ..., x_n$ generate B as an A-module, then the product $x_i y_j$ generate N over A. □

Now let M be an A-module. Since, as we have just seen, B can be regarded as an A-module, we can form the A-module $M_B = B \otimes_A M$. In fact M_B carries a B-module structure s.t.

$$b(b' \otimes x) = bb' \otimes x, \quad \forall b, b' \in B, x \in M. \tag{2.44}$$

The B-module M_B is said to be obtained from M by extension of scalars.

Proposition 2.6.3 If M is f.g. as an A-module, then M_B is f.g. B-module.

Proof. If $x_1, ..., x_m$ generate M over A, then $\forall x \in M, \exists a_i \in A$, s.t. $x = \sum_{i=1}^m a_i x_i$, then

$$b \otimes x = b \otimes \left(\sum a_i x_i\right) = \sum b \otimes a_i x_i = \sum (b a_i) \otimes x_i = \sum b a_i (1 \otimes x_i) \in M_B, \tag{2.45}$$

where $b \in B, 1 \otimes x_i \in B$. Hence we get $1 \otimes x_i$ generate M_B over B. □

2.7. Exactness properties of the tensor product

Proposition 2.7.1

$$\mathrm{Hom}_A(M \otimes_A N, P) \cong \mathrm{Hom}_A(M, \mathrm{Hom}_A(N, P)) \tag{2.46}$$

Proof.

Let $f : M \times N \to P$ be an A-bilinear map. For each $x \in M$, the map $y \mapsto f(x, y)$ is A-linear from N to P, and the assignment $x \mapsto (y \mapsto f(x, y))$ is A-linear from M to $\mathrm{Hom}_A(N, P)$. Conversely, every A-linear map $\varphi : M \to \mathrm{Hom}_A(N, P)$ defines an A-bilinear map $(x, y) \mapsto \varphi(x)(y)$.

Thus the set of A-bilinear maps $M \times N \to P$ is naturally in one-to-one correspondence with $\mathrm{Hom}_A(M, \mathrm{Hom}_A(N, P))$. By the universal property of the tensor product, it is also naturally in one-to-one correspondence with $\mathrm{Hom}_A(M \otimes_A N, P)$. □

Proposition 2.7.2 let

$$M' \xrightarrow{f} M \xrightarrow{g} M'' \to 0 \tag{2.47}$$

be an exact sequence of A-modules and homomorphisms, let N be any A-module. Then the sequence

$$M' \otimes N \xrightarrow{f \otimes \mathrm{id}} M \otimes N \xrightarrow{g \otimes \mathrm{id}} M'' \otimes N \to 0 \tag{2.48}$$

is exact.

Proof. Let E denote Equation (2.47), let $E \otimes N$ denote Equation (2.48), and let P be any A-module. Then $\mathrm{Hom}_A(N, P)$ is an A-module.

Since E is exact, $\mathrm{Hom}(E, \mathrm{Hom}_A(N, P))$ is exact by Proposition 2.4.2. Hence $\mathrm{Hom}(E \otimes N, P)$ is exact by Proposition 2.7.1. By Proposition 2.4.2 again, it follows that $E \otimes N$ is exact. □

Proposition 2.7.3 The following is equivalent for an A-module N.
1. N is flat
2. If $0 \to M' \to M \to M'' \to 0$ is exact, the tensor sequence
$$0 \to M' \otimes N \to M \otimes N \to M'' \otimes N \to 0 \text{ is exact.} \tag{2.49}$$
3. If $f : M' \to M$ is injective $\Rightarrow f \otimes \mathrm{id} : M' \otimes N \to M \otimes N$ is injective.
4. If $f : M' \to M$ is injective, and M, M' is f.g., then $f \otimes \mathrm{id} : M' \otimes N \to M \otimes N$ is injective.

2.8. Algebras

Definition 2.8.1 Let $f : A \to B$ be a ring homomorphism. For $a \in A, b \in B$, define $ab = f(a)b$.

Then this makes B into an A-module compatible with its ring structure. The ring B is said to be an A-algebra.

Remark

1. In particular, if $A = \mathbb{K}$ is a field and $B \neq 0$, then $f : \mathbb{K} \to B$ is injective and therefore $\mathbb{K}$ can be canonically identified with its image in B. Thus a $\mathbb{K}$-algebra is effectively a ring containing $\mathbb{K}$ as a subring.
2. Let A be any ring. Since A has an identity element, there is a unique homomorphism from $\mathbb{Z}$ into A, $n \mapsto n \cdot 1$. Thus every ring is automatically a $\mathbb{Z}$-algebra.

2.9. Tensor product of algebras

Definition 2.9.1 Let B, C be two A-algebra, $f : A \to B, g : A \to C$ are homo-. Since B, C are A-module, so $D = B \otimes_A C$ is an A-module. We shall define a multiplication on D. Consider the map
$$B \times C \times B \times C \to D, \quad (b, c, b', c') \mapsto bb' \otimes cc' \tag{2.50}$$

This is A-linear in each factor, so by Proposition 2.7.1, which induce an A-module homo-

$$B \otimes C \otimes B \otimes C \to D \tag{2.51}$$

hence by Proposition 2.5.3, an A-module homomorphism $D \otimes D \to D$, and this in turn by Proposition 2.5.2 corresponds to an A-bilinear map

$$\mu : D \times D \to D \tag{2.52}$$

where is

$$\mu(b \otimes c, b' \otimes c') = bb' \otimes cc' \Rightarrow \mu\left(\sum_i (b_i \otimes c_i), \sum_j \left(b'_j \otimes c'_j\right)\right) = \sum_{i,j} \left(b_i b'_j \otimes c_i c'_j\right) \tag{2.53}$$

3. Rings and Modules of fractions

Let A is a ring, $S \subset A$, s.t. $1 \in S$, and $\forall a, b \in S, ab \in S$, then

$$\begin{gathered} A \times S : (a_1, s_1) \sim (a_2, s_2) \Leftrightarrow \exists t \in S, \text{s.t. } t(a_1 s_2 - a_2 s_1) = 0. \\ A \times S / \sim = \left\{ \frac{a}{s} : a \in A, s \in S \right\} = S^{-1} A \end{gathered} \tag{3.1}$$

we put a ring structure on $S^{-1}A$ defined by

$$\begin{gathered} S^{-1}A \times S^{-1}A \to S^{-1}A \\ \frac{a_1}{s_1} + \frac{a_2}{s_2} = \frac{a_1 s_2 + a_2 s_1}{s_1 s_2}, \quad \frac{a_1}{s_1} \cdot \frac{a_2}{s_2} = \frac{a_1 a_2}{s_1 s_2} \end{gathered} \tag{3.2}$$

we also have a ring homomorphism $f : A \to S^{-1}A, f(x) = \frac{x}{1}$. This is not injective in general.

> **Remark**
>
> If A is an integral domain and $S = A - \{0\}$, then $S^{-1}A$ is the field of fractions of A.

Definition 3.1 (Ring of fraction) The ring $S^{-1}A$ is called the ring of fractions of A with respect S.

It has an universal property.

Proposition 3.2 (Universal Property) Let $g : A \to B$ be a ring homo-, s.t. $\forall s \in S, g(s)$ is a unit in B, Then

$$\exists 1 h : S^{-1}A \to B, \text{s.t. } g = h \circ f. \tag{3.3}$$

Proof. [Uniqueness] Let h satisfies the conditions, then $h(\frac{a}{1}) = h \circ f(a) = g(a) (\forall a \in A)$, then if $s \in S$, we get

$$\begin{gathered} h(1/s) = h((s/1)^{-1}) = [h(s/1)]^{-1} = [g(s)]^{-1} \\ \Rightarrow h(a/s) = h(a/1) h(1/s) = g(a) g(s)^{-1} \end{gathered} \tag{3.4}$$

$\Rightarrow h$ is uniquely determined by g.

[Existence] Let $h(a/s) = g(a)[g(s)]^{-1} \Rightarrow h$ is a ring homomorphism. Suppose $\frac{a}{s} = \frac{a'}{s'}$, then

$$\exists t \in S, \text{s.t. } (as' - a's)t = 0 \Rightarrow (g(a)g(s') - g(a')g(s))g(t) = 0 \tag{3.5}$$

Since $g(t)$ is a unit, so $g(a)[g(s)]^{-1} = g(a')[g(s')]^{-1}$. □

Proposition 3.3 The ring $S^{-1}A$ and homo- $f : A \to S^{-1}A$ have the follow properties.

1. $s \in S \Rightarrow f(s)$ is a unit in $S^{-1}A$

2. $f(a) = 0 \Rightarrow as = 0$ for some $s \in S$
3. Every element of $S^{-1}A$ is the form $f(a)f(s)^{-1}$ where $a \in A, s \in S$.

Conversely, there three properties determined $S^{-1}A$ up to isomorphism.

Corollary 3.3.1 If $g : A \to B$ is ring homo-, s.t.
1. $s \in S \Rightarrow g(s)$ is a unit in B
2. $g(a) = 0 \Rightarrow as = 0$ for some $s \in S$
3. Every element of B is the form $g(a)g(s)^{-1}$

Then there is a unique isomorphism $h : S^{-1}A \to B, h(a/s) = g(a)g(s)^{-1}$

Proof. By Proposition 3.3, we have to show that

$$h : S^{-1}A \to B, h(a/s) = g(a)g(s)^{-1} \tag{3.6}$$

is isomorphism, By (3), we get h is surjective, Now, just to prove h is injective.

$$h(a/s) = 0 \Rightarrow g(a) = 0 \Rightarrow ta = 0 \text{ for some } t \in S \Rightarrow \frac{a}{s} = 0 \in S^{-1}A \tag{3.7}$$

Hence h is injective, so h is isomorphism. □

Proposition 3.4 The operation S^{-1} is exact, i.e.

$$M' \xrightarrow{f} M \xrightarrow{g} M'' \text{ exact} \Rightarrow S^{-1}M' \xrightarrow{S^{-1}f} S^{-1}M \xrightarrow{S^{-1}g} S^{-1}M'' \text{ exact} \tag{3.8}$$

Proof. Only need to prove $\mathrm{Im}(S^{-1}f) = \ker(S^{-1}g)$,

[$\subset$]

$$M' \xrightarrow{f} M \xrightarrow{g} M'' \text{ exact} \Rightarrow g \circ f = 0 \Rightarrow S^{-1}g \circ S^{-1}f = S^{-1}(0) = 0 \tag{3.9}$$

$\Rightarrow \mathrm{Im}(S^{-1}f) \subset \ker(S^{-1}g)$

[$\supset$] Let $m/s \in \ker(S^{-1}g) \Rightarrow \frac{g(m)}{s} = 0 \in S^{-1}M \Rightarrow \exists t \in S$, s.t. $t \cdot g(m) = 0 \in M''$

But $tg(m) = g(tm)$ since g is an A-module homomorphism, so $tm \in \ker(g) = \mathrm{Im}(f)$, hence $tm = f(m')$ for some $m' \in M'$.

We have $\frac{m}{s} = t\frac{m}{ts} = \frac{f(m')}{ts} \in \mathrm{Im}(S^{-1}f) \Rightarrow \ker(S^{-1}g) \subset \mathrm{Im}(S^{-1}f)$ □

Corollary 3.4.1 If N, P are submodule of M, M is A-module, then
1. $S^{-1}(N + P) = S^{-1}N + S^{-1}P$
2. $S^{-1}(N \cap P) = S^{-1}N \cap S^{-1}P$
3. the $S^{-1}A$-module $S^{-1}(M/N)$ and $S^{-1}M/S^{-1}N$ are isomorphism.

Proof. Just prove (3). Apply S^{-1} to the exact sequence $0 \to N \to M \to M/N \to 0$ □

Proposition 3.5 Let M be an A-module. Then the $S^{-1}A$-modules $S^{-1}M$ and $S^{-1}A \otimes_A M$ are isomorphic; more precisely, there exists a unique $f : S^{-1}A \otimes_A M \to S^{-1}M$ such that

$$f\left(\frac{a}{s} \otimes m\right) = \frac{am}{s}, \quad \forall a \in A, m \in M, s \in S \tag{3.10}$$

Proof. Let bilinear mapping

$$\varphi : S^{-1}A \times M \to S^{-1}M, \quad \left(\frac{a}{s}, m\right) \mapsto \frac{am}{s} \tag{3.11}$$

therefore by the universal property of tensor products, φ induces an A-homomorphism

$$f : S^{-1}A \otimes_A M \to S^{-1}M, \quad f\left(\frac{a}{s} \otimes m\right) = \frac{am}{s} \tag{3.12}$$

Clearly, f is surjective, and it's uniquely defined by Equation (3.11). Now to prove f is injective. Let $\sum_i \frac{a_i}{s_i} \otimes m_i \in S^{-1}A \otimes M$. If $s = \prod_i s_i \in S$ and $t_i = \prod_{j \neq i} s_j$, we have

$$\sum_i \frac{a_i}{s_i} \otimes m_i = \sum_i \frac{a_i t_i}{s} \otimes m_i = \sum_i \frac{1}{s} \otimes a_i t_i m_i = \frac{1}{s} \otimes \sum_i a_i t_i m_i, \tag{3.13}$$

so that every element of $S^{-1}A \otimes M$ is of the form $\left(\frac{1}{s}\right) \otimes m$.

$$f\left(\left(\frac{1}{s}\right) \otimes m\right) = 0 \Rightarrow \frac{m}{s} = 0 \Rightarrow tm = 0 \tag{3.14}$$

for some $t \in S$, and therefore

$$\frac{1}{s} \otimes m = \frac{t}{st} \otimes m = \frac{1}{st} \otimes tm = \frac{1}{st} \otimes 0 = 0. \tag{3.15}$$

Hence f is injective. □

Corollary 3.5.1 $S^{-1}A$ is flat A-module.

Proof. Just because Proposition 3.4 and Proposition 3.5 and

$$\forall M' \to M \to M'' \text{ exact} \Rightarrow S^{-1}A \otimes M' \to S^{-1}A \otimes M \to S^{-1}A \otimes M'' \text{ exact.} \tag{3.16}$$

□

Proposition 3.6 If M, N are A-module, $\exists 1 S^{-1}A$-module f is isomorphism

$$f : S^{-1}M \otimes_{S^{-1}A} S^{-1}N \to S^{-1}(M \otimes_A N), \quad f\left(\left(\frac{m}{s}\right) \otimes \left(\frac{n}{t}\right)\right) = \frac{m \otimes n}{st} \tag{3.17}$$

In particular, if $\mathfrak{p}$ is any prime ideal, then $M_{\mathfrak{p}} \otimes_{A_{\mathfrak{p}}} N_{\mathfrak{p}} \cong (M \otimes_A N)_{\mathfrak{p}}$ as $A_{\mathfrak{p}}$-modules.

Proof. by Proposition 3.5, we have $S^{-1}A \otimes M \cong S^{-1}M$, so

$$S^{-1}M \otimes_{S^{-1}A} S^{-1}N \cong S^{-1}(M \otimes_A N) \tag{3.18}$$

Hence we have an isomorphism

$$f : S^{-1}M \otimes_{S^{-1}A} S^{-1}N \to S^{-1}(M \otimes_A N), \quad f\left(\left(\frac{m}{s}\right) \otimes \left(\frac{n}{t}\right)\right) = \frac{m \otimes n}{st} \tag{3.19}$$

□

3.1. Local properties

Definition 3.1.1 (Local properties) A property P of a ring A(or A-module M) is said to be a local property if the following is true A(or M) has $P \Leftrightarrow A_{\mathfrak{p}}$ has $P, \forall \mathfrak{p}$ is prime ideal of A.

The following propositions give example of local properties.

Proposition 3.1.2 Let M is an A-module, then the following are equivalent
1. $M = 0$
2. $M_{\mathfrak{p}} = 0$ for all prime ideal $\mathfrak{p}$ of A
3. $M_{\mathfrak{m}} = 0$ for all maximal ideal $\mathfrak{m}$ of A

Proof. $1 \Rightarrow 2 \Rightarrow 3$ is obviously, now to prove $3 \Rightarrow 1$.

Suppose 3 satified and $M \neq 0$, let $x \in M, x \neq 0$ and $\mathfrak{a} = \operatorname{Ann}(x) \Rightarrow \mathfrak{a} \neq (1)$ is ideal $\Rightarrow a \subset \mathfrak{m}$, consider $\frac{x}{1} \in M_{\mathfrak{m}} \Rightarrow \frac{x}{1} = 0 \Rightarrow x$ is killed by some elements of $A - \mathfrak{m}$, but this is impossible, so $M = 0$ □

Proposition 3.1.3 Let $\varphi : M \to N$ be an A-homo, then the following are equivalent
1. φ is injective
2. $\varphi_{\mathfrak{p}} : M_{\mathfrak{p}} \to N_{\mathfrak{p}}$ is injective for each prime ideal $(\mathfrak{p})$
3. $\varphi_{\mathfrak{m}} : M_{\mathfrak{m}} \to N_{\mathfrak{m}}$ is injective for each maximal ideal $(\mathfrak{m})$

Similarly, with injective replaced by surjective.

Proof. $(1) \Rightarrow (2)$ $0 \to M \to N$ is exact $\Rightarrow 0 \to M_{\mathfrak{p}} \to N_{\mathfrak{p}}$ is exact, hence $\varphi_{\mathfrak{p}}$ is injective.

$(2) \Rightarrow (3)$ Obviously

$(3) \Rightarrow (1)$ Let $M' = \ker(\varphi) \Rightarrow 0 \to M' \to M \to N$ is exact, so $0 \to M'_{\mathfrak{m}} \to M_{\mathfrak{m}} \to N_{\mathfrak{m}}$ is exact by Proposition 3.4, and $M'_{\mathfrak{m}} \cong \ker(\varphi_{\mathfrak{m}}) = 0$. Since $\varphi_{\mathfrak{m}}$ is injective, $M'_{\mathfrak{m}} = 0$ for every maximal ideal $\mathfrak{m}$. Hence $M' = 0$ by Proposition 3.1.2, so φ is injective. □

Flatness is a local property.

Proposition 3.1.4 $\forall$ A-module M the following are equivalent

1. M is flat A-module
2. $M_{\mathfrak{p}}$ is flat $A_{\mathfrak{p}}$-module for prime ideal $\mathfrak{p}$
3. $M_{\mathfrak{m}}$ is flat $A_{\mathfrak{m}}$-module for maximal ideal $\mathfrak{m}$

3.2. Extended and Contracted ideals in ring of fractions

Definition 3.2.1 Let A is a ring, S is a multiplicative closed subset of A,

$$\begin{aligned} f : A \to S^{-1}A, \quad a \mapsto \frac{a}{1} \text{ is a natural homo} \\ C := \{\mathfrak{a} \subset A : \exists \mathfrak{b} \subset S^{-1}A \text{ is an ideal, s.t. } f^{-1}(\mathfrak{b}) = \mathfrak{a}\} \\ E := \{\mathfrak{b} \subset S^{-1}A : \exists \mathfrak{a} \subset A \text{ is an ideal, s.t. } \mathfrak{b} = S^{-1}f(\mathfrak{a})\} \end{aligned} \tag{3.20}$$

Example. If $\mathfrak{a} \subset A$ is an ideal and $\mathfrak{a} \cap S \neq \varnothing$, then $S^{-1}\mathfrak{a} = S^{-1}A$.

Proposition 3.2.2

1. Every ideal in $S^{-1}A$ is an extended ideal.
2. If $\mathfrak{a} \subset A$ is an ideal, then $\mathfrak{a}^{ec} = \cup_{s \in S} (\mathfrak{a} : s)$. Hence $\mathfrak{a}^e = (1) \Leftrightarrow \mathfrak{a} \cap S \neq \varnothing$.
3. The prime ideals of $S^{-1}A$ are in one-to-one correspondence with the prime ideals of A which do not meet S.

$$\overline{P}_c = \{\overline{\mathfrak{p}} \in S^{-1}A\} \xrightarrow{1-1} P = \{\mathfrak{p} \subset A \wedge \mathfrak{p} \cap S = \varnothing\} \tag{3.21}$$

4. The operation S^{-1} commutes with finite sums, products, intersections, and radicals of ideals.

Proof. (1) Let $\mathfrak{b}$ be an ideal of $S^{-1}A$ and let $\mathfrak{a} = \mathfrak{b}^c$. If $\frac{a}{s} \in \mathfrak{b}$, then $\frac{a}{1} = \left(\frac{s}{1}\right)\left(\frac{a}{s}\right) \in \mathfrak{b}$, so $a \in \mathfrak{a}$ and $\frac{a}{s} \in \mathfrak{a}^e$. Thus $\mathfrak{b} \subset \mathfrak{a}^e$, and the reverse inclusion is immediate.

(2) For $x \in A$,

$$x \in \mathfrak{a}^{ec} \Leftrightarrow \frac{x}{1} \in S^{-1}\mathfrak{a} \Leftrightarrow \exists s \in S, \text{s.t. } sx \in \mathfrak{a} \Leftrightarrow x \in \cup_{s \in S} (\mathfrak{a} : s). \tag{3.22}$$

Also $\mathfrak{a}^e = (1)$ iff $1 \in S^{-1}\mathfrak{a}$ iff $\exists s \in S$ such that $s \in \mathfrak{a}$.

(3) If $\mathfrak{p}$ is prime and $\mathfrak{p} \cap S = \varnothing$, then $S^{-1}\mathfrak{p}$ is prime in $S^{-1}A$, and its contraction is $\mathfrak{p}$ by (2). Conversely, if $\mathfrak{q}$ is prime in $S^{-1}A$, then $\mathfrak{q}^c$ is prime in A and is disjoint from S, because every $\frac{s}{1}$ is a unit in $S^{-1}A$. By (1), extension and contraction are inverse on these prime ideals.

(4) Sums and products follow directly from the definitions. Intersections follow from exactness of localization applied to $0 \to \mathfrak{a} \cap \mathfrak{b} \to \mathfrak{a} \oplus \mathfrak{b} \to \mathfrak{a} + \mathfrak{b} \to 0$, where the middle map is $(x, y) \mapsto x - y$. For radicals, $\frac{x}{s} \in r(S^{-1}\mathfrak{a})$ iff $\left(\frac{x}{s}\right)^n \in S^{-1}\mathfrak{a}$ for some $n > 0$, iff $\frac{x^n}{t} \in S^{-1}\mathfrak{a}$ for some

$t \in S$, iff $ux^n \in \mathfrak{a}$ for some $u \in S$, which is equivalent to $ux \in r(\mathfrak{a})$ for some $u \in S$. Hence $r(S^{-1}\mathfrak{a}) = S^{-1}r(\mathfrak{a})$. □

Remark

If $\mathfrak{a}, \mathfrak{b}$ are ideal of A, the formula $S^{-1}(\mathfrak{a} : \mathfrak{b}) = (S^{-1}\mathfrak{a} : S^{-1}\mathfrak{b})$ is true provided $\mathfrak{b}$ is f.g.

Corollary 3.2.2.1 If $\mathfrak{N}$ is the nilradical of A, then $S^{-1}\mathfrak{N}$ is the nilradical of $S^{-1}A$.

Corollary 3.2.2.2 If $\mathfrak{p}$ is a prime ideal of A, the prime ideals of the local ring $A_\mathfrak{p}$ are in one-to-one correspondence with prime ideals of A contained in $\mathfrak{p}$, i.e.

$$\overline{P}_c = \{\overline{\mathfrak{p}} \in A_\mathfrak{p}\} \xrightarrow{1-1} P = \{\mathfrak{p}' \subset A \text{ is prime and } \mathfrak{p}' \subset \mathfrak{p}\} \tag{3.23}$$

Proof. Let $S = A - \mathfrak{p}$ in Proposition 3.2.2 (3) □

Proposition 3.2.3 Let M be a f.g. A-module and let S be a multiplicatively closed subset of A. Then $S^{-1}(\text{Ann}(M)) = \text{Ann}(S^{-1}M)$.

Proof. If it is true for submodules M, N, then it is true for $M + N$ because

$$\begin{aligned} S^{-1}(\text{Ann}(M+N)) &= S^{-1}(\text{Ann}(M) \cap \text{Ann}(N)) = S^{-1}(\text{Ann}(M)) \cap S^{-1}(\text{Ann}(N)) \\ &= \text{Ann}(S^{-1}M) \cap \text{Ann}(S^{-1}N) = \text{Ann}(S^{-1}(M+N)) \end{aligned} \tag{3.24}$$

Hence it is enough to prove the result for a cyclic module $M = (x)$. Then $M \cong A/\mathfrak{a}$ where $\mathfrak{a} = \text{Ann}(x)$, and

$$S^{-1}M = S^{-1}A/S^{-1}\mathfrak{a} \Rightarrow \text{Ann}(S^{-1}M) = S^{-1}\mathfrak{a} = S^{-1}(\text{Ann}(M)) \tag{3.25}$$

□

Corollary 3.2.3.1 If N, P are submodule of A-module, P is f.g., then $S^{-1}(N : P) = (S^{-1}N : S^{-1}P)$

Proof. $(N : P) = \text{Ann}((N + P)/N)$ by Proposition 3.2.3 □

Proposition 3.2.4 Let $f : A \to B$ be a homo $\mathfrak{p} \subset A, \mathfrak{q} \subset B$ be prime ideal, then

$$\mathfrak{p} = \mathfrak{q}^c \Leftrightarrow \mathfrak{p}^{ec} = \mathfrak{p} \tag{3.26}$$

Proof. [$\Rightarrow$] by prop:1.17

[$\Leftarrow$] If $\mathfrak{p}^{ec} = \mathfrak{p}$, let $S = f(A - \mathfrak{p}) \subset B \Rightarrow \mathfrak{p}^e \cap A = \varnothing \Rightarrow \mathfrak{p}^{ec}$ is a proper ideal in $S^{-1}B$ by Proposition 3.2.2 and $\mathfrak{p}^{ec} = \mathfrak{m}$, where $\mathfrak{m}$ is maximal of $S^{-1}B$. If $\mathfrak{q} = \mathfrak{m}^c \Rightarrow \mathfrak{q}$ is prime, because $\mathfrak{q} \supset \mathfrak{p}^e, \mathfrak{q} \cap S = \varnothing \Rightarrow \mathfrak{q}^c = \mathfrak{p}$. $\square$

4. Primary Decomposition

Definition 4.1 (Primary) A proper ideal $\mathfrak{q}$ of a ring A is primary if

$$\forall x, y \in A, xy \in \mathfrak{q} \Rightarrow x \in \mathfrak{q} \text{ or } y^n \in \mathfrak{q} \text{ for some } n > 0. \tag{4.1}$$

Remark

Prime ideal is primary. In other words

$$\mathfrak{q} \text{ is primary} \Leftrightarrow A/\mathfrak{q} \neq 0 \text{ and } \forall \text{ zero-divisor} \in A/\mathfrak{q} \text{ is nilpotent} \tag{4.2}$$

Remark

The contraction of a primary ideal is primary, i.e. if $f : A \to B$ and $\mathfrak{q}$ is a primary ideal in B, then $A/\mathfrak{q}^c$ is isomorphic to a subring of $B/\mathfrak{q}$.

Proposition 4.2 Let $\mathfrak{q}$ be a primary in A, the $r(\mathfrak{q})$ is the smallest prime ideal containing $\mathfrak{q}$

Proof. (Smallest) By definition, $r(\mathfrak{q})$ is contained in every prime ideal containing $\mathfrak{q}$.

(Prime) Suppose $xy \in r(\mathfrak{q})$ and $y \notin r(\mathfrak{q})$. Then $(xy)^n = x^n y^n \in \mathfrak{q}$ for some $n > 0$. Since $y^n \notin r(\mathfrak{q})$, in particular no power of y^n lies in $\mathfrak{q}$. Because $\mathfrak{q}$ is primary, we must have $x^n \in \mathfrak{q}$, so $x \in r(\mathfrak{q})$. Hence $r(\mathfrak{q})$ is prime. □

Definition 4.3 (p-primary) if $\mathfrak{p} = r(\mathfrak{q})$, then $\mathfrak{q}$ is said to $\mathfrak{p}$-primary

Proposition 4.4 If $r(\mathfrak{a})$ is maximal, then $\mathfrak{a}$ is primary.

Proof.

$$\pi : A \to A/\mathfrak{a}, \quad r(\mathfrak{a}) = \mathfrak{m} \mapsto \overline{\mathfrak{m}} = \mathfrak{m} + \mathfrak{a} \tag{4.3}$$

$r(\mathfrak{a})$ is maximal $\Rightarrow \overline{\mathfrak{m}}$ is maximal of $A/\mathfrak{a}$

Because $\overline{\mathfrak{m}} \subset \mathfrak{N}(A/\mathfrak{a}) = \cap\, \overline{\mathfrak{p}}(\text{where } \overline{\mathfrak{p}} \text{ is prime}) \Rightarrow A/\mathfrak{a}$ has only one prime ideal $\overline{\mathfrak{m}} \Rightarrow \forall r + \mathfrak{a} \in A/\mathfrak{a}$

$$\begin{cases} r + \mathfrak{a} \in \overline{\mathfrak{m}} \Rightarrow r + \mathfrak{a} \text{ is nilpotent in } A/\mathfrak{a} \\ r + \mathfrak{a} \notin \overline{\mathfrak{m}} \Rightarrow r + \mathfrak{a} \text{ is unit of } A/\mathfrak{a} \end{cases} \tag{4.4}$$

Every zero-divisor in $A/\mathfrak{a}$ is not a unit, hence is nilpotent in $A/\mathfrak{a}$. Therefore $\mathfrak{a}$ is primary. □

Lemma 4.5 If $\mathfrak{q}_i (i \in \{1, ...n\})$ are $\mathfrak{p}$-primary, hence $\mathfrak{q} = \cap_{i=1}^n \mathfrak{q}_i$ is $\mathfrak{p}$-primary.

Proof. We know $r(\mathfrak{q}) = r(\cap_{i=1}^n \mathfrak{q}_i) = \cap_{i=1}^n r(\mathfrak{q}_i) = \mathfrak{p}$.

Let $x \cdot y \in \mathfrak{q}$ and $x \notin \mathfrak{q}$. Choose i such that $x \notin \mathfrak{q}_i$. Since $xy \in \mathfrak{q}_i$ and $\mathfrak{q}_i$ is primary, we have $y \in \mathfrak{p}$. Thus for every j, some power of y lies in $\mathfrak{q}_j$. Choosing one exponent large enough for all j, we get $y^N \in \cap_{j=1}^n \mathfrak{q}_j = \mathfrak{q}$. □

Lemma 4.6 Let $\mathfrak{q}$ be a $\mathfrak{p}$-primary, $x \in A$, then

1. if $x \in \mathfrak{q} \Rightarrow (\mathfrak{q} : x) = (1)$
2. if $x \notin \mathfrak{q} \Rightarrow (\mathfrak{q} : x)$ is $\mathfrak{p}$-primary and therefore $r(\mathfrak{q} : x) = \mathfrak{p}$
3. if $x \notin \mathfrak{p} \Rightarrow (\mathfrak{q} : x) = \mathfrak{q}$

Proof. (1), (3) are clear; now prove (2).

Since $\mathfrak{q} \subset (\mathfrak{q} : x)$, we have $\mathfrak{p} = r(\mathfrak{q}) \subset r(\mathfrak{q} : x)$. If $y \in (\mathfrak{q} : x)$, then $xy \in \mathfrak{q}$ and $x \notin \mathfrak{q}$, so $y \in \mathfrak{p}$. Hence $(\mathfrak{q} : x) \subset \mathfrak{p}$ and $r(\mathfrak{q} : x) = \mathfrak{p}$.

To see that $(\mathfrak{q} : x)$ is primary, suppose $yz \in (\mathfrak{q} : x)$ and $z \notin (\mathfrak{q} : x)$. Then $xyz \in \mathfrak{q}$ and $xz \notin \mathfrak{q}$. Since $\mathfrak{q}$ is primary, $y^n \in \mathfrak{q} \subset (\mathfrak{q} : x)$ for some $n > 0$. □

Definition 4.7 A primary decomposition of $\mathfrak{a}$ is

$$\mathfrak{a} = \cap_{i=1}^n \mathfrak{q}_i, \quad \text{where } \mathfrak{q}_i \text{ is primary ideal.} \tag{4.5}$$

Definition 4.8 We call Equation (4.5) minimal if

1. $\mathfrak{p}_i = r(\mathfrak{q}_i)$ are all distinct
2. $\cap_{j \neq i} \mathfrak{q}_j \not\subset \mathfrak{q}_i$ for every i

Theorem 4.9 (1st uniqueness theorem) Let $\mathfrak{a}$ be a decomposable ideal and $\mathfrak{a} = \cap_{i=1}^n \mathfrak{q}_i$ be a minimal primary decomposition of $\mathfrak{a}$. Let $\mathfrak{p}_i = r(\mathfrak{q}_i)(1 \leq i \leq n)$.

Then the $\mathfrak{p}_i$ are precisely the prime ideals which occur among the ideals $r(\mathfrak{a} : x)$ for $x \in A$, and hence are independent of the particular decomposition of $\mathfrak{a}$.

Proof. Let $x \in A$. Since $(\cap_i \mathfrak{q}_i : x) = \cap_{i(\mathfrak{q}_i : x)}$, by Lemma 4.6 we have

$$r(\mathfrak{a} : x) = \cap_{x \notin \mathfrak{q}_i} \mathfrak{p}_i, \tag{4.6}$$

with factors for which $x \in \mathfrak{q}_i$ omitted. If this radical is prime, Proposition 1.6.3 implies it is one of the $\mathfrak{p}_i$.

Conversely, since the decomposition is minimal, for each i there exists $x_i \in \cap_{j \neq i} \mathfrak{q}_j$ with $x_i \notin \mathfrak{q}_i$. Then

$$r(\mathfrak{a}:x_i)=\cap_{j=1}^{n} r\left(\mathfrak{q}_j:x_i\right)=\mathfrak{p}_i \tag{4.7}$$

□

Definition 4.10 (Associated) Assume Equation (4.5) is a minimal primary decomposition of $\mathfrak{a}$. The primes $\mathfrak{p}_i=r(\mathfrak{q}_i)$ are said to belong to $\mathfrak{a}$, or to be associated with $\mathfrak{a}$.

Example. Let $\mathfrak{a}=(x^2,xy)\in A=k[x,y]$. Then $\mathfrak{a}=\mathfrak{p}_1\cap\mathfrak{p}_2^2$, where $\mathfrak{p}_1=(x)$ and $\mathfrak{p}_2=(x,y)$. The ideal $\mathfrak{p}_2^2$ is primary, so $\mathfrak{p}_1,\mathfrak{p}_2$ are prime ideals. In this example, $\mathfrak{p}_1\subset\mathfrak{p}_2$, we have $r(\mathfrak{a})=\mathfrak{p}_1\cap\mathfrak{p}_2=\mathfrak{p}_1$, but $\mathfrak{a}$ is not primary.

Definition 4.11 (Minimal and embedded) The minimal elements of $\{\mathfrak{p}_i\}$ are called the minimal prime ideals belonging to $\mathfrak{a}$.

The ideal $\mathfrak{a}$ is primary $\Leftrightarrow$ $\mathfrak{a}$ has only one associated prime ideal.

The minimal elements of the set $\{\mathfrak{p}_\mathrm{i}\}_{i=1}^n$ are called the minimal or isolated prime ideals belonging to $\mathfrak{a}$.

The others are called embedded prime ideals.

Remark

In the example above, $\mathfrak{p}_2=(x,y)$ is embedded.

Proposition 4.12 Let $\mathfrak{a}$ be a decomposable ideal. Then any prime ideal $\mathfrak{p}\supset\mathfrak{a}$ contains a minimal prime ideal belonging to $\mathfrak{a}$.

Proof.

$$\mathfrak{p}\supset\mathfrak{a}=\cap_{i=1}^n\mathfrak{q}_i,\quad \mathfrak{p}=r(\mathfrak{q})\supset\cap_{i=1}^n r(\mathfrak{q}_i)=\cap_{i=1}^n\mathfrak{p}_i, \tag{4.8}$$

by Proposition 1.6.3, we have $\exists$ some $i\in\{1,\dots,n\}$, s.t. $\mathfrak{p}_i\subset\mathfrak{p}$. □

Proposition 4.13 Let $\mathfrak{a}$ be a decomposable ideal with minimal primary decomposition $\mathfrak{a}=\cap_{i=1}^n\mathfrak{q}_i$, and let $\mathfrak{p}_i=r(\mathfrak{q}_i)$. Then

$$\cup_{i=1}^n\mathfrak{p}_i=\{x\in A:(\mathfrak{a}:x)\neq\mathfrak{a}\} \tag{4.9}$$

In particular, if $\mathfrak{a}=(0)$, then $D=\{x\in A:(0:x)\neq 0\}$ is the set of zero-divisors. Then D is the union of all prime ideals belonging to (0).

Proof. It is enough to prove the case $\mathfrak{a}=(0)$ after passing to $A/\mathfrak{a}$. Suppose first that $x\in\cup_i\mathfrak{p}_i$. Then for some i, $x\in r(\mathfrak{q}_i)$, so $x^N\in\mathfrak{q}_i$ for some N. By minimality choose $y\in\cap_{j\neq i}\mathfrak{q}_j$ with

$y \notin \mathfrak{q}_i$. For N minimal such that $x^N y \in \mathfrak{q}_i$, the element $x^{N-1}y$ is not in $\mathfrak{a}$ but is killed by x modulo $\mathfrak{a}$. Hence $(\mathfrak{a} : x) \neq \mathfrak{a}$.

Conversely, if $(\mathfrak{a} : x) \neq \mathfrak{a}$, choose $y \in (\mathfrak{a} : x)$ with $y \notin \mathfrak{a}$. Then $xy \in \mathfrak{q}_i$ for all i, while $y \notin \mathfrak{q}_i$ for some i. Since $\mathfrak{q}_i$ is primary, $x \in r(\mathfrak{q}_i) = \mathfrak{p}_i$.

For the quotient formulation, if $\mathfrak{a}$ is decomposable, then $0 \subset A/\mathfrak{a}$ is decomposable and

$$(0) = \cap_{i=1}^{n} \bar{\mathfrak{q}}_i, \quad \bar{\mathfrak{q}} = \pi(\mathfrak{q}_i) \text{ is primary} \tag{4.10}$$

where $\pi : A \to A/\mathfrak{a},, x \mapsto x + \mathfrak{a}$ is the natural homomorphism.

The result above applied in $A/\mathfrak{a}$ gives the stated equality. $\square$

Proposition 4.14 Let A is a ring, S is multiplicative closed subset, let $\mathfrak{q}$ be a $\mathfrak{p}$-primary ideal, then
1. If $S \cap \mathfrak{p} \neq \varnothing \Rightarrow S^{-1}\mathfrak{q} = S^{-1}A$
2. If $S \cap \mathfrak{p} = \varnothing \Rightarrow S^{-1}\mathfrak{q}$ is a $S^{-1}\mathfrak{p}$-primary ideal and $\left(S^{-1}\mathfrak{q}\right)^c = \mathfrak{q}$.

Proof. If $S \cap \mathfrak{p} \neq \varnothing$, choose $s \in S \cap \mathfrak{p}$. Since $\mathfrak{p} = r(\mathfrak{q})$, some power $s^n \in \mathfrak{q}$. Thus $\frac{s^n}{1}$ is both a unit and an element of $S^{-1}\mathfrak{q}$, so $S^{-1}\mathfrak{q} = S^{-1}A$.

Now suppose $S \cap \mathfrak{p} = \varnothing$. By Proposition 3.2.2, $r\left(S^{-1}\mathfrak{q}\right) = S^{-1}r(\mathfrak{q}) = S^{-1}\mathfrak{p}$, which is prime. If $\left(\frac{x}{s}\right)\left(\frac{y}{t}\right) \in S^{-1}\mathfrak{q}$ and $\frac{x}{s} \notin S^{-1}\mathfrak{q}$, then for some $u \in S$, $uxy \in \mathfrak{q}$. Also $\frac{x}{s} \notin S^{-1}\mathfrak{q}$ means no element of S sends x into $\mathfrak{q}$, so $ux \notin \mathfrak{q}$. Since $\mathfrak{q}$ is primary, $y^n \in \mathfrak{q}$ for some $n > 0$, hence $\left(\frac{y}{t}\right)^n \in S^{-1}\mathfrak{q}$. Thus $S^{-1}\mathfrak{q}$ is primary.

Finally, if $x \in \left(S^{-1}\mathfrak{q}\right)^c$, then $\frac{x}{1} \in S^{-1}\mathfrak{q}$, so $sx \in \mathfrak{q}$ for some $s \in S$. Since $s \notin \mathfrak{p}$, Lemma 4.6 gives $(\mathfrak{q} : s) = \mathfrak{q}$, hence $x \in \mathfrak{q}$. The reverse inclusion is immediate. $\square$

Remark

$\mathfrak{q}^{ec} = \left(S^{-1}\mathfrak{q}\right)^c := S(\mathfrak{q})$

Proposition 4.15 Let S be a multiplicatively closed subset and let $\mathfrak{a}$ be decomposable. Let $\mathfrak{a} = \cap_{i=1}^{n} \mathfrak{q}_i$ be a minimal primary decomposition and let $\mathfrak{p}_i = r(\mathfrak{q}_i)$. Suppose that the $\mathfrak{q}_i$ are numbered such that

$$\begin{cases} S \cap \mathfrak{p}_i = \varnothing & i \leq m \\ S \cap \mathfrak{p}_i \neq \varnothing & i > m \end{cases} \tag{4.11}$$

Then $S^{-1}\mathfrak{a} = \cap_{i=1}^{m} S^{-1}\mathfrak{q}_i$ and $S(\mathfrak{a}) = \left(S^{-1}\mathfrak{a}\right)^c = \cap_{i=1}^{m} \mathfrak{q}_i$. This decomposition is minimal after omitting any redundant unit components.

Proof. By Proposition 3.2.2, localization commutes with finite intersections, so

$$S^{-1}\mathfrak{a} = \cap_{i=1}^{n} S^{-1}\mathfrak{q}_i. \tag{4.12}$$

If $S \cap \mathfrak{p}_i \neq \varnothing$, then $S^{-1}\mathfrak{q}_i = S^{-1}A$ by the previous proposition, so those factors may be omitted. If $S \cap \mathfrak{p}_i = \varnothing$, then $S^{-1}\mathfrak{q}_i$ is $S^{-1}\mathfrak{p}_i$-primary and its contraction is $\mathfrak{q}_i$. Therefore

$$\left(S^{-1}\mathfrak{a}\right)^c = \cap_{i=1}^m \left(S^{-1}\mathfrak{q}_i\right)^c = \cap_{i=1}^m \mathfrak{q}_i. \tag{4.13}$$

The associated primes that remain are exactly the $\mathfrak{p}_i$ disjoint from S, so minimality follows from the first uniqueness theorem. □

Definition 4.16 A set $\sum$ of prime ideals belonging to $\mathfrak{a}$ is isolated if whenever $\mathfrak{p}'$ belongs to $\mathfrak{a}$, $\mathfrak{p}' \subset \mathfrak{p}$, and $\mathfrak{p} \in \sum$, then $\mathfrak{p}' \in \sum$.

Theorem 4.17 (2nd uniqueness theorem) Let $\mathfrak{a}$ be a decomposable ideal,

$$\mathfrak{a} = \cap_{i=1}^n \mathfrak{q}_i \text{ is a minimal primary decomposition}, \mathfrak{p}_i = r(\mathfrak{q}_i), \tag{4.14}$$

Let $\left\{\mathfrak{p}_{i_1}, \ldots, \mathfrak{p}_{i_k}\right\}$ be an isolated set of prime ideals belonging to $\mathfrak{a}$. Then $\cap_{j=1}^k \mathfrak{q}_{i_j}$ is independent of Equation (4.14).

Proof. Let $\sum = \left\{\mathfrak{p}_{i_1}, \ldots, \mathfrak{p}_{i_k}\right\}$ and set

$$S = A - \cup_{\mathfrak{p} \in \sum} \mathfrak{p}. \tag{4.15}$$

Since each $\mathfrak{p}$ is prime, S is multiplicatively closed. For $\mathfrak{p} \in \sum$, clearly $S \cap \mathfrak{p} = \varnothing$. If $\mathfrak{p}_j \notin \sum$, then $\mathfrak{p}_j$ is not contained in the union of the primes in $\sum$; otherwise prime avoidance would give $\mathfrak{p}_j \subset \mathfrak{p}$ for some $\mathfrak{p} \in \sum$, and the isolated property would force $\mathfrak{p}_j \in \sum$. Hence $S \cap \mathfrak{p}_j \neq \varnothing$.

Applying the previous proposition with this S gives

$$\left(S^{-1}\mathfrak{a}\right)^c = \cap_{\mathfrak{p}_i \in \sum} \mathfrak{q}_i. \tag{4.16}$$

The left side depends only on $\mathfrak{a}$ and $\sum$, not on the chosen minimal primary decomposition. Therefore the displayed intersection is independent of Equation (4.14). □