COMMUTATIVE ALGEBRA

BOWEN LIU

Abstract. It's a lecture note I typed for seminar organized by CUHKSZ and SDU, which is about commutative algebra. This note will only contains main definitions, propositions and theorems without proof. Readers can refer to Atiyah's Introduction to commutative algebra for detailed proof. Furthermore, this note will contain some solutions to the exercises we discussed in the seminar.

Contents

1. Rings and Ideals

1.1. Rings and ring homomorphism.

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

(1) A is an abelian group with respect to addition.
(2) The multiplication is associative and distributive over addition.

We shall consider only rings which are commutative:

(3) The multiplication is commutative.

and have the identity element

(4) There exists $1 \in A$ such that $x1 = 1x = x$ for all $x \in A$.

In this note we only consider about commutative rings with an identity element. In particular, identity element may be zero. In this case the ring only has one element 0, is called zero ring.

Definition 1.1.2 (morphism of rings)**.** A ring homomorphism is a mapping f of a ring A into a ring B such that

(1) f is a homomorphism of abelian groups.
(2) $f(xy) = f(x)f(y)$ for all $x, y \in A$.
(3) $f(1_A) = 1_B$.

Remark 1.1.1. Since f is a group homomorphism, we must have $f(0) = 0$, but if we only require $f(xy) = f(x)f(y)$, we may not have $f(1_A) = 1_B$. Indeed,

$$f(1_A) = f(1_A \cdot 1_A) = f(1_A)f(1_A) \implies f(1_A)(1_S - f(1_A)) = 0$$

In a general ring $xy = 0$ won't implies $x = 0$ or $y = 0$.

Definition 1.1.3 (subring)**.** A subset S of a ring A is a subring of A if S is closed under addition and multiplication and contains the identity element of A.

Remark 1.1.2. You may wonder why don't we define a subring as follows: A subset S of a ring A is a subring of A if S itself is a ring with respect to the addition and multiplication of A? In fact, these two definitions are a little different. For a ring A, there may exist a subset B such that B is a ring with respect to the addition and multiplication of A, but $1_B \neq 1_A$. For example: Let $A = R_1 \times R_2$ and $B = R_1 \times \{0\}$. Then $1_A = (1_{R_1}, 1_{R_2})$ but $1_B = (1_{R_1}, 0)$, where R_1, R_2 are two rings.

1.2. Ideals, quotient rings.

Definition 1.2.1 (ideals)**.** An ideal $\mathfrak{a}$ of a ring A is a subset of A which is an additive subgroup and is such that $A\mathfrak{a} \subseteq \mathfrak{a}$.

Definition 1.2.2 (quotient rings)**.** Let $\mathfrak{a} \subseteq A$ be an ideal of a ring A. The quotient group inherits a uniquely defined multiplication from A which makes it into a ring, called quotient ring.

1.3. Zero divisors, nilpotent elements and units.

Proposition 1.3.1. Let A be a ring $\neq 0$. Then the following statements are equivalent.

(1) A is a field.
(2) The only ideals in A are 0 and (1).
(3) Every homomorphism of A into a non-zero ring B is injective.

1.4. Prime ideals and maximal ideals.

Proposition 1.4.1. Let A be a ring.

(1) An ideal $\mathfrak{p}$ is prime if and only if $A/\mathfrak{p}$ is an integral domain.
(2) An ideal $\mathfrak{m}$ is maximal if and only if $A/\mathfrak{m}$ is a field.

Proposition 1.4.2. Let $f\colon A \to B$ be a ring homomorphism. For a prime ideal $\mathfrak{p}$ in B, $f^{-1}(\mathfrak{p})$ is a prime ideal in A, and there is an isomorphism

$$A/f^{-1}(\mathfrak{p}) \cong B/\mathfrak{p}$$

as rings.

However, the pullback of maximal ideal may not be a maximal ideal.

Example 1.4.1. Let $A = \mathbb{Z}, B = \mathbb{Q}$ and $f\colon \mathbb{Z} \to \mathbb{Q}$ be inclusion map. Consider zero ideal in $\mathbb{Q}$, it's a maximal ideal, since $\mathbb{Q}$ is a field, but zero ideal in $\mathbb{Z}$ is not maximal.

Definition 1.4.1 (local ring)**.** A ring with exactly one maximal ideal is called a local ring.

Proposition 1.4.3.

(1) Let A be a ring and $\mathfrak{m} \neq (1)$ be an ideal of A such that every $x \in A \setminus \mathfrak{m}$ is a unit in A. Then A is a local ring and $\mathfrak{m}$ is its maximal ideal.
(2) Let A be a ring and $\mathfrak{m}$ be a maximal ideal such that every element of $1 + \mathfrak{m}$ is a unit in A. Then A is a local ring.

1.5. Nilradical and Jacobson radical.

Definition 1.5.1 (nilradical)**.** Let A be a ring. The set of $\mathfrak{N}$ of all nilpotent elements in a ring A is an ideal, called the nilradical of A.

Proposition 1.5.1. The nilradical of a ring A is the intersection of all the prime ideals of A.

Definition 1.5.2 (Jacobson radical)**.** The Jacobson radical $\mathfrak{R}$ of a ring A is defined to be the intersection of all the maximal ideals of A.

Proposition 1.5.2. Let A be a ring. $x \in \mathfrak{R}$ if and only if $1 - xy$ is a unit in A for all $y \in A$.

1.6. **Operations on ideals.**

Definition 1.6.1 (coprime)**.** Two ideals $\mathfrak{a}, \mathfrak{b}$ are said to be coprime if $\mathfrak{a}+\mathfrak{b} = (1)$.

Proposition 1.6.1 (Chinese remainder theorem)**.** Let A be a ring and $\mathfrak{a}_1, \dots, \mathfrak{a}_n$ be ideals of A. Consider the following ring homomorphism

$$\begin{aligned}\phi\colon A &\to \prod_{i=1}^{n}(A/\mathfrak{a}_i)\\ x &\mapsto (x+\mathfrak{a}_1, \dots, x+\mathfrak{a}_n)\end{aligned}$$

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

Proposition 1.6.2. Let $\mathfrak{p}_1, \dots, \mathfrak{p}_n$ be prime ideals and $\mathfrak{a}$ be an ideal contained in $\bigcup_{i=1}^n \mathfrak{p}_i$. Then $\mathfrak{a} \subseteq \mathfrak{p}_i$ for some i.

Proof. Prove it by induction on n in the form

$$\mathfrak{a} \subsetneq \mathfrak{p}_i (1 \leq i \leq n) \implies \mathfrak{a} \subsetneq \bigcup_{i=1}^{n} \mathfrak{p}_i$$

It's clear when $n = 1$. If $n > 1$ and the result is true for $n-1$. Assume $\mathfrak{a} \not\subseteq \mathfrak{p}_i$ for each i, then by induction for each i there exists $x_i \in \mathfrak{a}$ such that $x_i \notin \mathfrak{p}_j$ when $i \neq j$. If for some i we have $x_i \notin \mathfrak{p}_i$, then we're done. If not, then $x_i \in \mathfrak{p}_i$ for all i. Consider

$$y = \sum_{i=1}^{n} x_1 x_2 \dots x_{i-1} x_{i+1} x_{i+2} \dots x_n$$

we have $y \in \mathfrak{a}$ and $y \notin \mathfrak{p}_i$ for each i. This completes the proof. □

Proposition 1.6.3. Let $\mathfrak{a}_1, \dots, \mathfrak{a}_n$ be ideals and $\mathfrak{p}$ be an prime ideal containing $\bigcap_{i=1}^n \mathfrak{a}_i$. Then $\mathfrak{p} \supseteq \mathfrak{a}_i$ for some i. If $\mathfrak{p} = \bigcap_{i=1}^n \mathfrak{a}_i$, then $\mathfrak{p} = \mathfrak{a}_i$ for some i.

Proof. Suppose $\mathfrak{a}_i \neq \mathfrak{p}$ for each i, then there exists $x_i \in \mathfrak{a}_i, x_i \neq \mathfrak{p}$ for each i, and therefore $\prod x_i \in \prod \mathfrak{a}_i \subseteq \bigcap \mathfrak{a}_i$. But $\prod x_i \notin \mathfrak{p}$ since $\mathfrak{p}$ is prime, hence $\bigcap \mathfrak{a}_i \subsetneq \mathfrak{p}$, a contradiction. Finally if $\mathfrak{p} = \bigcap \mathfrak{a}_i$, then $\mathfrak{p} \subseteq \mathfrak{a}_i$, which implies $\mathfrak{p} = \mathfrak{a}_i$. □

Definition 1.6.2 (ideal quotient)**.** If $\mathfrak{a}, \mathfrak{b}$ are ideals in a ring A, their ideal quotient is

$$(\mathfrak{a} : \mathfrak{b}) = \{x \in A : x\mathfrak{b} \subseteq \mathfrak{a}\}$$

which is an ideal.

Exercise 1.6.1.
(1) $\mathfrak{a} \subseteq (\mathfrak{a} : \mathfrak{b})$
(2) $(\mathfrak{a} : \mathfrak{b})\mathfrak{b} \subseteq \mathfrak{a}$

(3) $((\mathfrak{a}:\mathfrak{b}):\mathfrak{c})=(\mathfrak{a}:\mathfrak{b}\mathfrak{c})=((\mathfrak{a}:\mathfrak{c}):\mathfrak{b})$
(4) $(\bigcap_i \mathfrak{a}_i:\mathfrak{b})=\bigcap_i(\mathfrak{a}_i:\mathfrak{b})$
(5) $(\mathfrak{a}:\sum_i \mathfrak{b}_i)=\bigcap_i(\mathfrak{a}:\mathfrak{b}_i)$

Proof. (1) and (2) are almost obvious by definitions. For (3). $x\in((\mathfrak{a}:\mathfrak{b}):\mathfrak{c})$ is equivalent to

$$x\mathfrak{c}\mathfrak{b}\subseteq\mathfrak{a}\Longleftrightarrow x\in((\mathfrak{a}:\mathfrak{c}):\mathfrak{b})$$

Note that our ring is commutative, so that's equivalent to

$$x\mathfrak{b}\mathfrak{c}\subseteq\mathfrak{a}\Longleftrightarrow x\in(\mathfrak{a}:\mathfrak{b}\mathfrak{c})$$

For (4). $x\in(\bigcap_i\mathfrak{a}_i:\mathfrak{b})$ is equivalent to $x\mathfrak{b}\in\bigcap_i\mathfrak{a}_i$, that is equivalent to $x\mathfrak{b}\in\mathfrak{a}_i$ for each i. Thus $x\in\bigcap_i(\mathfrak{a}_i:\mathfrak{b})$.

For (5). $x\in(\mathfrak{a}:\sum_i\mathfrak{b}_i)$ is equivalent to $x(\sum_i\mathfrak{b}_i)\in\mathfrak{a}$, that's also equivalent to $x\mathfrak{b}_i\in\mathfrak{a}$ for each i by definition of $\sum_i\mathfrak{b}_i$. So $x\in\bigcap_i(\mathfrak{a}_i:\mathfrak{b})$. □

Definition 1.6.3 (radical of an ideal)**.** If $\mathfrak{a}$ is any ideal of A, the radical of $\mathfrak{a}$ is

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

Exercise 1.6.2.

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

Proof. (1) and (2) are almost obvious by definition. For (3). Note that

$$(\mathfrak{a}\cap\mathfrak{b})^2\subseteq\mathfrak{a}\mathfrak{b}\subseteq\mathfrak{a}\cap\mathfrak{b}$$

Then by (2) we obtain

$$r(\mathfrak{a}\cap\mathfrak{b})=r((\mathfrak{a}\cap\mathfrak{b})^2)\subseteq r(\mathfrak{a}\mathfrak{b})\subseteq r(\mathfrak{a}\cap\mathfrak{b})$$

which implies $r(\mathfrak{a}\mathfrak{b})=r(\mathfrak{a}\cap\mathfrak{b})$. For the half part. If $x\in\mathfrak{a}\cap\mathfrak{b}$, then there exists m,n such that $x^m\in\mathfrak{a},x^n\in\mathfrak{b}$. Then $x^{\max\{m,n\}}\in\mathfrak{a}\cap\mathfrak{b}$, and converse is clear.

For (4). $r(\mathfrak{a})=(1)$ is equivalent to for all $x\in(1)$, there exists n such that $x^n\in\mathfrak{a}$. Take $x=1$ implies $1\in\mathfrak{a}$, so we have $\mathfrak{a}=(1)$, and converse is clear.

For (5). Consider $m+n$, where $m\in r(\mathfrak{a}),n\in r(\mathfrak{b})$, then there exists a sufficiently large N such that $(m+n)^N\in\mathfrak{a}+\mathfrak{b}$, just by considering binomial expansion. So if there exists n such that $x^n\in r(\mathfrak{a})+r(\mathfrak{b})$, then $x^{nN}\in\mathfrak{a}+\mathfrak{b}$, which implies $x\in r(\mathfrak{a}+\mathfrak{b})$, and converse is clear.

For (6). Just note that $x^n\in\mathfrak{p}$ is equivalent to $x\in\mathfrak{p}$ for a prime ideal $\mathfrak{p}$. □

Proposition 1.6.4. Let $\mathfrak{a},\mathfrak{b}$ be ideals in a ring A such that $r(\mathfrak{a})$ and $r(\mathfrak{b})$ are coprime. Then $\mathfrak{a},\mathfrak{b}$ are coprime.

Proof. By (4) of Exercise 1.6.2, it suffices to show $r(\mathfrak{a}+\mathfrak{b})=(1)$. And by (5) of Exercise 1.6.2, we have

$$r(\mathfrak{a}+\mathfrak{b})=r(r(\mathfrak{a})+r(\mathfrak{b}))=r((1))=(1)$$

This completes the proof. □

1.7. **Extension and contraction.** Let $f\colon A\to B$ be a ring homomorphism. Although for any ideal $\mathfrak{b}\in B$, $f^{-1}(\mathfrak{b})$ is an ideal in A, called the contraction $\mathfrak{b}^c$ of $\mathfrak{b}$, if $\mathfrak{a}$ is an ideal in A, the set of $f(\mathfrak{a})$ may not be an ideal in B.

Example 1.7.1. Let f be the embedding of $\mathbb{Z}$ in $\mathbb{Q}$, and consider any non-zero ideal, since only ideals in $\mathbb{Q}$ is zero or (1).

We define the extension $\mathfrak{a}^e$ of $\mathfrak{a}$ to be the ideal $Bf(\mathfrak{a})$ generated by $f(\mathfrak{a})$ in B. To be explicit. $\mathfrak{a}^e$ is the set of all sums $\sum y_if(x_i)$ where $x_i\in\mathfrak{a}$ and $y_i\in B$. If $\mathfrak{b}$ is a prime ideal of B, so is its contraction. But if $\mathfrak{a}$ is a prime ideal in A, then its extension may not by prime. So as you can see, the property of extension may be quite complicated. The classical example is from algebraic number theory.

Example 1.7.2. Consider $\mathbb{Z}\to\mathbb{Z}[\sqrt{-1}]$, and consider the extension of prime ideal of $\mathbb{Z}$, the situations is as follows.
(1) $(2)^e=((1+\sqrt{-1})^2)$.
(2) If $p\equiv 1 \pmod 4$, then $(p)^e$ is the product of two distinct prime ideals.
(3) If $p\equiv 3 \pmod 4$, then $(p)^e$ is prime in $\mathbb{Z}[\sqrt{-1}]$.

Proposition 1.7.1.
(1) $\mathfrak{a}\subseteq\mathfrak{a}^{ec},\mathfrak{b}\supseteq\mathfrak{b}^{ce}$.
(2) $\mathfrak{b}^c=\mathfrak{b}^{cec},\mathfrak{a}^e=\mathfrak{a}^{ece}$.
(3) If C is the set of contracted ideals in A and if E is the set of extended ideals in B, then $C=\{\mathfrak{a}\mid\mathfrak{a}^{ec}=\mathfrak{a}\},E=\{\mathfrak{b}\mid\mathfrak{b}^{ce}=\mathfrak{b}\}$, and $\mathfrak{a}\mapsto\mathfrak{a}^e$ is a bijective map of C onto E, whose inverse if $\mathfrak{b}\mapsto\mathfrak{b}^c$.

Exercise 1.7.1. Let $f\colon A\to B$ be a homomorphism of rings. If $\mathfrak{a}_1,\mathfrak{a}_2$ are ideals of A and if $\mathfrak{b}_1,\mathfrak{b}_2$ are ideals of B, then

$$\begin{array}{ll}
(\mathfrak{a}_1+\mathfrak{a}_2)^e=\mathfrak{a}_1^e+\mathfrak{a}_2^e & (\mathfrak{b}_1+\mathfrak{b}_2)^c\supseteq\mathfrak{b}_1^c+\mathfrak{b}_2^c\\
(\mathfrak{a}_1\cap\mathfrak{a}_2)^e\subseteq\mathfrak{a}_1^e\cap\mathfrak{a}_2^e & (\mathfrak{b}_1\cap\mathfrak{b}_2)^c=\mathfrak{b}_1^c\cap\mathfrak{b}_2^c\\
(\mathfrak{a}_1\mathfrak{a}_2)^e=\mathfrak{a}_1^e\mathfrak{a}_2^e & (\mathfrak{b}_1\mathfrak{b}_2)^c\supseteq\mathfrak{b}_1^c\mathfrak{b}_2^c\\
(\mathfrak{a}_1:\mathfrak{a}_2)^e\subseteq(\mathfrak{a}_1^e:\mathfrak{a}_2^e) & (\mathfrak{b}_1:\mathfrak{b}_2)^c\subseteq(\mathfrak{b}_1^c:\mathfrak{b}_2^c)\\
r(\mathfrak{a})^e\subseteq r(\mathfrak{a}^e) & r(\mathfrak{b})^c=r(\mathfrak{b}^c)
\end{array}$$

Proof. For extension: For (1). By definition we have

$$(\mathfrak{a}_1+\mathfrak{a}_2)^2=Bf(\mathfrak{a}_1+\mathfrak{a}_2)=Bf(\mathfrak{a}_1)+Bf(\mathfrak{a}_2)=\mathfrak{a}_1^e+\mathfrak{a}_2^e$$

(2) and (3) are similar to (1), since f preserves multiplication and intersection. For (4). By definition we need to check $(\mathfrak{a}_1:\mathfrak{a}_2)^e\mathfrak{a}_2^e\subseteq\mathfrak{a}_1^e$. Directly check as follows:

$$Bf((\mathfrak{a}_1:\mathfrak{a}_2))Bf(\mathfrak{a}_2)=Bf((\mathfrak{a}_1:\mathfrak{a}_2))f(\mathfrak{a}_2)=B(f(\mathfrak{a}_1:\mathfrak{a}_2)\mathfrak{a}_2)\subseteq Bf(\mathfrak{a}_1)$$

As desired. For (5). Note that the extension of a prime ideal may not be prime.

For contraction: (1), (2), (3) and (4) are similar to cases in extension. For (5). Note that $r(\mathfrak{b})$ is the intersection of all prime ideal containing $\mathfrak{b}$ and contraction preserves prime. □

1.8. **Part of solutions of Chapter 1.**

Exercise 1.8.1. Let x be a nilpotent element of a ring A. Show that $1+x$ is a unit of A. Deduce that the sum of a nilpotent element and a unit is a unit.

Proof. If x is a nilpotent element, then $x \in \mathfrak{N} \subseteq \mathfrak{R}$. By Proposition 1.5.2 we have $1-xy$ is unit for any $y \in A$. Take $y=-1$ we obtain $1+x$ is a unit. If y is unit, then we have $x+y=y^{-1}(y^{-1}x+1)$. Since $y^{-1}x$ is also nilpotent, we have $y^{-1}x+1$ is unit, thus $x+y$ is unit. □

Exercise 1.8.2. Let A be a ring and let $A[x]$ be the ring of polynomials in an indeterminate x, with coefficients in A. Let $f=a_0+a_1x+\dots+a_nx^n \in A[x]$. Prove that

(1) f is a unit in $A[x] \Leftrightarrow a_0$ is a unit in A and $a_1,\dots,a_n$ are nilpotent.
(2) f is nilpotent $\Leftrightarrow a_0,a_1,\dots,a_n$ are nilpotent.
(3) f is a zero-divisor $\Leftrightarrow$ there exists $a \neq 0$ in A such that $af=0$.
(4) f is said to be primitive if $(a_0,a_1,\dots,a_n)=(1)$. Prove that if $f,g \in A[x]$, then fg is primitive $\Leftrightarrow f$ and g are primitive.

Proof. For (1). Use $g=\sum_{i=0}^m b_ix^i$ to denote the inverse of f. Since $fg=1$ and if we use c_k to denote $\sum_{m+n=k} a_mb_n$, then we have

$$\begin{cases} c_0=1 \\ c_k=0, \quad k>0 \end{cases}$$

But $c_0=a_0b_0$, thus a_0 is unit. Now let's prove $a_n^{r+1}b_{m-r}=0$ by induction on r: $r=0$ is trivial, since $a_nb_m=c_{n+m}=0$. If we have already proven this for $k<r$. Then consider c_{m+n-r}, we have

$$0=c_{m+n-r}=a_nb_{m-r}+a_{n-1}b_{m-r+1}+\dots$$

and multiply a_n^r we obtain

$$0=a_n^{r+1}b_{m-r}+a_{n-1}\underbrace{a_n^rb_{m-r+1}}_{\text{by induction this term is 0}}+a_{n-2}a_n\underbrace{a_n^{r-1}b_{m-r+2}}_{\text{by induction this term is 0}}+\dots$$

which completes the proof of claim. Take $r=m$, we obtain $a_n^{m+1}b_0=0$. But b_0 is unit, thus a_n is nilpotent and a_nx^n is a nilpotent element in $A[x]$. By Exercise 1.8.1, we know that $f-a_nx^n$ is unit, then we can prove a_{n-1},a_{n-2} is also nilpotent by induction on degree of f. Conversely, if a_0 is unit and $a_1,\dots,a_n$ is nilpotent. We can imagine that if you power f enough times, then we will obtain unit. Or you can see $\sum_{i=1}^n a_ix^i$ is nilpotent, then unit plus nilpotent is also unit.

For (2)[1]. If $a_0, \dots, a_n$ are nilpotent, then clearly f is. Conversely, if f is nilpotent, then clearly a_n is nilpotent, and we have $f - a_n x^n$ is nilpotent, then by induction on degree of f to conclude.

For (3). $af = 0$ for $a \neq 0$ implies f is a zero-divisor is clear. Conversely choose a $g = \sum_{i=0}^m b_i x^i$ of least degree m such that $fg = 0$, then we have $a_n b_m = 0$, hence $a_n g = 0$, since $a_n g f = 0$ and has degree less than m. Then consider

$$0 = fg - a_n x^n g = (f - a_n x^n) g$$

Then $f - a_n x^n$ is a zero-divisor with degree $n-1$, so we can conclude by induction on degree of f.

For (4). Note that $(a_0, \dots, a_n) = 1$ is equivalent to there is no maximal ideal $\mathfrak{m}$ contains $a_0, \dots, a_n$, it's an equivalent description for primitive polynomials. For $f \in A[x]$, f is primitive if and only if for all maximal ideal $\mathfrak{m}$, we have $f \notin \mathfrak{m}[x]$. Note that we have the following isomorphism

$$A[x]/\mathfrak{m}[x] \cong (A/\mathfrak{m})[x]$$

Indeed, consider the following homomorphism

$$\begin{aligned} \varphi \colon A[x] &\to (A/\mathfrak{m})[x] \\ \sum_{i=0}^n a_i x^i &\mapsto \sum_{i=0}^n (a_i + \mathfrak{m}) x^i \end{aligned}$$

Clearly $\ker \varphi = \mathfrak{m}[x]$ and use the first isomorphism theorem. So in other words, $f \in A[x]$ is primitive if and only if $\overline{f} \neq 0 \in (A/\mathfrak{m})[x]$ for any maximal ideal $\mathfrak{m}$. Since $A/\mathfrak{m}$ is a field, then $(A/\mathfrak{m})[x]$ is an integral domain by (3), so $\overline{fg} \neq 0 \in (A/\mathfrak{m})[x]$ if and only if $\overline{f} \neq 0 \in (A/\mathfrak{m})[x], \overline{g} \neq 0 \in (A/\mathfrak{m})[x]$. This completes the proof. □

Exercise 1.8.3. Generalize the results of Exercise 1.8.2 to a polynomial ring $A[x_1, \dots, x_r]$ in several indeterminate.

Proof. It suffices to consider the case of $A[x, y]$, since we can do induction on r to conclude general case. Consider $A[x, y] = A[x][y] = B[y]$, where $B = A[x]$. For $f \in B[y]$, we write it as

$$f = \sum_{ij} a_{ij} x^i y^j = \sum_k b_k y^k, \quad b_k = \sum_i a_{ik} x^i \in B$$

For (1). f is a unit in $B[y]$ if and only if b_0 is a unit in B and b_k is nilpotent for $k > 0$, if and only if a_{00} is a unit, and a_{ij} is nilpotent for otherwise.

For (2). f is a nilpotent in $B[y]$ if and only if b_k is nilpotent for all k, if and only if a_{ij} is nilpotent for all i, j.

[1]An alternative proof of (2). Note that

$$\mathfrak{N}(A[x]) = \bigcap \mathfrak{p}[x] = (\bigcap \mathfrak{p})[x] = \mathfrak{N}(A)[x]$$

For (3). f is a zero divisor in $B[y]$ if and only if there exists $a \in A$ such that $af = 0$. Indeed, if f is a zero divisor in $B[y]$, then there exists $b \in B$ such that $bf = 0$, then $bb_k = 0$ for all k, then for each k there exists a_k such that $a_k b_k = 0$, then consider $a = \prod_k a_k$, then $af = 0$.

For (4). fg is primitive if and only if f and g are primitive. Indeed, proof in Exercise 1.8.2 still holds in this case. □

Exercise 1.8.4. In the ring $A[x]$, the Jacobson radical is equal to the nilradical

Proof. Since we already have $\mathfrak{N} \subseteq \mathfrak{R}$, it suffices to show for any $f \in \mathfrak{R}$, it's nilpotent. Note that by Proposition 1.5.2, we have $1 - fg$ is unit for any $g \in A[x]$. Choose g to be x, then by (1) of Exercise 1.8.1 we know that all coefficients of f is nilpotent in A, and by (2) of Exercise 1.8.1, f is nilpotent. This completes the proof. □

Exercise 1.8.5. Let A be a ring and let $A[[x]]$ be the ring of formal power series $f = \sum_{n=0}^{\infty} a_n x^n$ with coefficients in A. Show that

(1) f is a unit in $A[[x]] \Leftrightarrow a_0$ is a unit in A.
(2) If f is nilpotent, then a_n is nilpotent for all $n \geqslant 0$. Is the converse true?
(3) f belongs to the Jacobson radical of $A[[x]] \Leftrightarrow a_0$ belongs to the Jacobson radical of A.
(4) The contraction of a maximal ideal $\mathfrak{m}$ of $A[[x]]$ is a maximal ideal of A, and $\mathfrak{m}$ is generated by $\mathfrak{m}^c$ and x.
(5) Every prime ideal of A is the contraction of a prime ideal of $A[[x]]$.

Proof. For (1). Let $g = \sum_{j=1}^{\infty} b_j x^j$ be the inverse of f. Since $fg = 1$, then clearly we have $a_0 b_0 = 1$, thus a_0 is a unit. Conversely, if a_0 is a unit, then consider the Taylor expansion of $1/f$ at $x = 0$ to conclude.

For (2). If $f = \sum_{i=0}^{\infty} a_i x^i$ is nilpotent, then a_0 must be nilpotent, so $f - a_0$ is also nilpotent. Consider $(f - a_0)/x$ which is also nilpotent, we will obtain a_1 is nilpotent. Repeat what we have done to conclude $a_0, a_1, a_2, \ldots$ are nilpotent. The converse holds when A is a Noetherian ring.

For (3). $f \in \mathfrak{R}(A[[x]])$ if and only if $1 - fg$ is unit for all $g \in A[[x]]$. Note that the zero term of $1 - fg$ is $1 - a_0 b_0$, so by (1) we obtain $1 - fg$ is unit if and only if $1 - a_0 b_0$ is unit for all $b_0 \in A$, and that's equivalent to $a_0 \in \mathfrak{R}(A)$.

For (4). For maximal ideal $\mathfrak{m} \in A[[x]]$, we have $(x) \subseteq \mathfrak{m}$, since by (3) we have $x \in \mathfrak{R}(A[[x]])$. Then $\mathfrak{m}^c = \mathfrak{m} - (x)$, that is $\mathfrak{m} = \mathfrak{m}^c + (x)$. Furthermore, note that

$$A[[x]]/\mathfrak{m} = A[[x]]/(\mathfrak{m}^c + (x)) \cong A/\mathfrak{m}^c$$

implies $\mathfrak{m}^c$ is maximal. The last isomorphism holds since for a ring A and two ideals $\mathfrak{b} \subseteq \mathfrak{a}$, we have

$$A/\mathfrak{a} \cong (A/\mathfrak{b})/(\mathfrak{a}/\mathfrak{b})$$

just by considering $A/\mathfrak{a} \to A/\mathfrak{b}$ and use first isomorphism theorem.

For (5). Let $\mathfrak{p}$ be a prime ideal in A. Consider the ideal $\mathfrak{q}$ which is generated by $\mathfrak{p}$ and x. Clearly $\mathfrak{q}^c = \mathfrak{p}$ and $\mathfrak{q}$ is prime since

$$A[[x]]/\mathfrak{q} \cong A/\mathfrak{p}$$

□

Exercise 1.8.6. A ring A is such that every ideal not contained in the nilradical contains a nonzero idempotent (that is, an element e such that $e^2 = e \neq 0$). Prove that the nilradical and Jacobson radical of A are equal.

Proof. Take $x \in \mathfrak{R}$ which is not in $\mathfrak{N}$. Then (x) is an ideal not contained in $\mathfrak{N}$. Thus there exists a nonzero idempotent $e = xy \in (x)$. Note that an important property of idempotent is that an idempotent is a zero-divisor, since $e(1-e) = 0$. Thus $1 - e = 1 - xy$ is not a unit. So by Proposition 1.5.2 we have $x \notin \mathfrak{R}$, a contradiction. □

Exercise 1.8.7. Let A be a ring in which every element x satisfies $x^n = x$ for some $n > 1$ (depending on x). Show that every prime ideal in A is maximal.

Proof. The proof is quite similar to above Exercise: Note that every prime ideal is maximal if and only if nilradical and Jacobson radical are equal. If not, take $x \in \mathfrak{R}$ which is not in $\mathfrak{N}$, then from $x^n = x$ we know that $1 - x^{n-1}$ is not a unit, a contradiction to $x \in \mathfrak{R}$. □

Exercise 1.8.8. Let A be a ring $\neq 0$. Show that the set of prime ideals of A has minimal elements with respect to inclusion.

Proof. Let $\operatorname{Spec} A$ denote the set of all prime ideals of A. Clearly it's not empty, since there exists a maximal ideal. We order $\operatorname{Spec} A$ by reverse inclusion, that is $\mathfrak{p}_a \leq \mathfrak{p}_b$ if $\mathfrak{p}_b \subseteq \mathfrak{p}_a$. By Zorn lemma, it suffices to show every chain in $\operatorname{Spec} A$ has a upper bound in $\operatorname{Spec} A$.

For a chain $\{\mathfrak{p}_i\}_{i \in I}$, it's natural to consider the intersection of all $\mathfrak{p}_i$, denote by $\mathfrak{p}$. It's an ideal clearly. Now it suffices to show it's prime. Suppose $xy \in \mathfrak{p}$ and $x, y \notin \mathfrak{p}$. Then there exists $\mathfrak{p}_i, \mathfrak{p}_j$ such that $x \notin \mathfrak{p}_i, y \notin \mathfrak{p}_j$. Without lose of generality we may assume $\mathfrak{p}_i \subset \mathfrak{p}_j$. Then $x, y \notin \mathfrak{p}_i$. But $xy \in \mathfrak{p}$ implies $xy \in \mathfrak{p}_i$, a contradiction to the fact $\mathfrak{p}_i$ is prime. This completes the proof.

Remark 1.8.1. At first I want to check the nilradical is a prime ideal to complete the proof. However, this statement fails in general. And it's easy to explain why: If there exists at least two minimal prime ideals, then nilradical can not be prime. Indeed, the intersections of distinct minimal prime ideal can not be prime, since if $\mathfrak{p}_1, \ldots, \mathfrak{p}_n$ is minimal and if $\mathfrak{p} = \mathfrak{p}_1 \cap \cdots \cap \mathfrak{p}_n$ is prime, then by Proposition 1.6.3 we must have $\mathfrak{p} = \mathfrak{p}_i$ for some i, which implies $\mathfrak{p}_i$ is contained in other $\mathfrak{p}_j, i \neq j$, a contradiction to minimality. Furthermore, as you can see, nilradical of a ring A is prime if and only if A only has one minimal prime ideal.

□

Exercise 1.8.9. Let $\mathfrak{a}$ be an ideal $\neq (1)$ in a ring A. Show that $\mathfrak{a} = r(\mathfrak{a}) \Leftrightarrow \mathfrak{a}$ is an intersection of prime ideals.

Proof. One direction is clear, since $r(\mathfrak{a})$ is the intersection of all prime ideal containing $\mathfrak{a}$. Conversely, if $\mathfrak{a}$ is an intersection of prime ideals, denoted by $\mathfrak{a} = \bigcap_i \mathfrak{p}_i$. If $x^n \in \mathfrak{a}$, then $x^n \in \mathfrak{p}_i$ for each i, then by property of prime ideal we obtain $x \in \mathfrak{p}_i$ for each i, which implies $x \in \mathfrak{a}$. This completes the proof. □

Exercise 1.8.10. Let A be a ring, $\mathfrak{N}$ its nilradical. Show that the following statements are equivalent.

(1) A has exactly one prime ideal.
(2) every element of A is either a unit or nilpotent.
(3) $A/\mathfrak{N}$ is a field.

Proof. (1) to (3): Since A has exactly one prime ideal, it must be a maximal ideal, in this case A is a local ring and clearly $A/\mathfrak{N}$ is a field.

(3) to (2): If $A/\mathfrak{N}$ is a field, thus if an element in A is not a nilpotent, then it must be a unit.

(2) to (1): Consider the set of all nilpotent elements in A, it's clear it's an ideal. Then by (1) of Proposition 1.4.3 to conclude. □

Exercise 1.8.11. A ring A is Boolean if $x^2 = x$ for all $x \in A$. In a Boolean ring A, show that

(1) $2x = 0$ for all $x \in A$.
(2) every prime ideal $\mathfrak{p}$ is maximal, and $A/\mathfrak{p}$ is a field with two elements.
(3) every finitely generated ideal in A is principal.

Proof. For (1). Note that for $x \in A$, we have $-x = (-x)^2 = x^2 = x$, thus $2x = 0$ for all $x \in A$.

For (2). From Exercise 1.8.7 we know that every prime ideal in Boolean ring is maximal. Furthermore $A/\mathfrak{p}$ is field with two elements, since $A/\mathfrak{p}$ is a domain and element in it satisfies $\overline{x}(1-\overline{x}) = 0$.

For (3). It suffices to show that for any $x, y \in A$, then (x, y) is principal. Let $z = x + y - xy$, clearly $(z) \subseteq (x, y)$, but

$$\begin{cases} xz = x^2 + xy - x^2y = x \\ yz = y \end{cases}$$

This completes the proof. □

Exercise 1.8.12. A local ring contains no idempotent $\neq 0, 1$.

Proof. Let $(A, \mathfrak{m})$ be a local ring, and $x \in A$ is an idempotent e which is not equal to $0, 1$. Since e is not unit, then we have $e \in \mathfrak{m} = \mathfrak{R}$. But $1 - e$ is also not a unit, then by Proposition 1.5.2 we must have $e \notin \mathfrak{R} = \mathfrak{m}$, a contradiction. □

Exercise 1.8.13 (Construction of an algebraic closure of a field)**.** Let K be a field and let Σ be the set of all irreducible monic polynomials f in one indeterminate with coefficients in K. Let A be the polynomial ring over K generated by indeterminate x_f, one for each $f \in \Sigma$. Let $\mathfrak{a}$ be the ideal of A generated by the polynomials $f(x_f)$ for all $f \in \Sigma$. Show that $\mathfrak{a} \neq (1)$.

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

Proof. For $\mathfrak{a} \neq (1)$: If we have

$$a_1 f(x_{f_1}) + \cdots + a_n f(x_{f_n}) = 1, \quad a_i \in A, f_i \in \Sigma$$

But we know that there is some field extension K' of K in which the polynomials f_i have root α_i. Working in K', we substitute in α_i for x_{f_i} we obtain $0 = 1$, and this is impossible, since $K \subseteq K'$ implies K' is not a field with only one element. □

Exercise 1.8.14. In a ring A, let Σ be the set of all ideals in which every element is a zero-divisor. Show that the set Σ has maximal elements and that every maximal element of Σ is a prime ideal. Hence the set of zero-divisors in A is a union of prime ideals.

Proof. We still need to use Zorn lemma: Order Σ by inclusion and it suffices to show every chain $\{\mathfrak{a}_i\}_{i \in I}$ has an upper bound in Σ. Consider $\mathfrak{a} = \bigcup_i \mathfrak{a}_i$, clear it consists of zero-divisors and it's an ideal. Now let $\mathfrak{p}$ be a maximal element of Σ, let's show it's prime by definition: if $x, y \notin \mathfrak{p}$, then $(x) + \mathfrak{p}$ contains a non-zero-divisor, the same for $(y) + \mathfrak{p}$, so there exists a non-zero-divisor in $(xy) + \mathfrak{p}$, so $xy \notin \mathfrak{p}$. This shows that $\mathfrak{p}$ is prime.

For a zero-divisor $x \in A$, consider the principal ideal generated by x, then it must lie in some maximal element of Σ, that's a prime ideal. This completes the proof. □

Exercise 1.8.15 (spectrum of a ring)**.** Let A be a ring and let X be the set of all prime ideals of A. For each subset E of A, let $V(E)$ denote the set of all prime ideals of A which contain E. Prove that

(1) if $\mathfrak{a}$ is the ideal generated by E, then $V(E) = V(\mathfrak{a}) = V(r(\mathfrak{a}))$.
(2) $V((0)) = X, V((1)) = \varnothing$.
(3) if $(E_i)_{i \in I}$ is any family of subsets of A, then

$$V(\bigcup_{i \in I} E_i) = \bigcap_{i \in I} V(E_i)$$

(4) $V(\mathfrak{a} \cap \mathfrak{b}) = V(\mathfrak{a}\mathfrak{b}) = V(\mathfrak{a}) \cup V(\mathfrak{b})$ for any ideals $\mathfrak{a}, \mathfrak{b}$ of A.

These results show that the sets $V(E)$ satisfy the axioms for closed sets in a topological space. The resulting topology is called the Zariski topology. The topological space X is called the prime spectrum of A, and is written $\operatorname{Spec} A$.

Proof. For (1). It's clear $V(E) = V(\mathfrak{a})$. For the half part: Clearly $V(r(\mathfrak{a})) \subseteq V(\mathfrak{a})$, since $\mathfrak{a} \subseteq r(\mathfrak{a})$. Conversely, if a prime ideal $\mathfrak{p}$ contains $\mathfrak{a}$, then it must contain $r(\mathfrak{a})$, since it's the intersection of all prime ideal containing $\mathfrak{a}$.

For (2). Since every prime ideal contains (0), so $V((0)) = X$. Note that every ideal contains (1) must be the whole ring, so there is no prime ideal containing (1).

For (3). If a prime ideal contains $\bigcup_{i\in I} E_i$, then clearly it contains E_i for each $i \in I$, thus $V(\bigcup_{i\in I} E_i) \subseteq \bigcap_{i\in I} V(E_i)$, and vice versa.

For (4). Note that by Exercise 1.6.2, we have $r(\mathfrak{ab}) = r(\mathfrak{a}\cap\mathfrak{b}) = r(\mathfrak{a})\cap r(\mathfrak{b})$. Then (1) implies

$$V(\mathfrak{ab}) = V(\mathfrak{a}\cap\mathfrak{b}) = V(r(\mathfrak{a})\cap r(\mathfrak{b}))$$

But $V(r(\mathfrak{a})\cap r(\mathfrak{b})) = V(\mathfrak{a})\cup V(\mathfrak{b})$. Indeed, clearly $V(\mathfrak{a})\cup V(\mathfrak{b}) \subseteq V(r(\mathfrak{a})\cap r(\mathfrak{b}))$. Conversely, note that $r(\mathfrak{a})\cap r(\mathfrak{b})$ is the intersection of all prime ideal either containing $\mathfrak{a}$ or $\mathfrak{b}$, and Proposition 1.6.3 tells the answer. □

Exercise 1.8.16. Draw pictures of $\mathrm{Spec}(\mathbb{Z}), \mathrm{Spec}(\mathbb{R}), \mathrm{Spec}(\mathbb{R}[x]), \mathrm{Spec}(\mathbb{C}[x])$ and $\mathrm{Spec}(\mathbb{Z}[x])$.

Proof. For $\mathrm{Spec}(\mathbb{Z})$: It's known to all only prime ideals in $\mathbb{Z}$ taking the form (0) and (p), where p is a prime number.

For $\mathrm{Spec}(\mathbb{R})$: There is only one prime ideal (0) in $\mathbb{R}$, since $\mathbb{R}$ is a field.

For $\mathrm{Spec}(\mathbb{R}[x])$: The irreducible polynomials in $\mathbb{R}[x]$ are linear polynomials and polynomials with degree 2 which have the following form

$$(x-\alpha)(x+\alpha), \quad \alpha \in \mathbb{H} = \{\alpha \in \mathbb{C} \mid \mathrm{Im}\,\alpha > 0\}$$

So points in $\mathrm{Spec}(\mathbb{R}[x])$ are real numbers together with the upper plane.

For $\mathrm{Spec}(\mathbb{C}[x])$: Things are a little bit easier, since every irreducible polynomials in $\mathbb{C}[x]$ take the form $x-\alpha$. So as a set $\mathrm{Spec}(\mathbb{C}[x])$ consists of complex plane together with a point (0).

For $\mathrm{Spec}(\mathbb{Z}[x])$: All prime ideal of $\mathbb{Z}[x]$ are listed as follows:

(1) (0)
(2) $(f(x))$, where $f(x)$ is an irreducible polynomial.
(3) (p), where p is a prime number.
(4) $(p, f(x))$, where p is a prime number and $f(x)$ is an irreducible polynomial module p.

□

Exercise 1.8.17. For each $f \in A$, let X_f denote the complement of $V(f)$ in $X = \mathrm{Spec}\,A$. The sets X_f are open. Show that they form a basis of open sets for the Zariski topology, and that

(1) $X_f \cap X_g = X_{fg}$.
(2) $X_f = \varnothing \Leftrightarrow f$ is nilpotent.
(3) $X_f = X \Leftrightarrow f$ is a unit.
(4) $X_f = X_g \Leftrightarrow r((f)) = r((g))$.

(5) X is quasi-compact[2].
(6) More generally, each X_f is quasi-compact.
(7) An open subset of X is quasi-compact if and only if it is a finite union of sets X_f The sets X_f are called basic open sets of $X = \operatorname{Spec} A$.

Proof. For any open set U, write it as $U = V(E)^c$ for some $E \subseteq A$. Then we have

$$\bigcup_{f\in E} X_f = \bigcup_{f\in E} (V(f)^c) = (\bigcap_{f\in E} V(f))^c = (V(E))^c$$

as desired.

For (1). By definition and (4) of Exercise 1.8.15 one has

$$X_f \cap X_g = (V(f))^c \cap (V(g))^c = (V(f) \cup V(g))^c = (V(fg))^c = X_{fg}$$

For (2). If f is nilpotent, then $f \in \mathfrak{N}$, thus f lies in every prime ideal, so $V(f) = X$, so $X_f = \varnothing$ and vice versa.

For (3). If f is a unit, then there is no prime ideal containing f, that is $X_f = X$. Conversely, we need to show if there is no prime ideal containing f, then f is unit. Indeed, if f is not unit, then it is contained in some maximal ideal, a contradiction.

For (4). By definition we have$X_f = X_g \iff V(f) = V(g) \iff V((f)) = V((g))$. This is equivalent to say a prime ideal containing (f) if and only if it contains (g), so we have $r((f)) = r((g))$, since $r((f))$ is the intersection of all prime ideal containing (f).

For (5). It suffices to show every open covering taking the form $\{X_{f_i}\}$ has a finite subcovering, since X_f forms a basis of Zariski topology. We can translate $X = \bigcup_{i\in I} X_{f_i}$ as $(f_i)_{i\in I} = (1)$. Indeed,

$$(f_i)_{i\in I} = (1) \iff \bigcap_{i\in I} V(f_i) = V((f_i)_{i\in I}) = \varnothing \iff \bigcup_{i\in I} X_{f_i} = X$$

So if $\{f_i\}_{i\in I}$ generates (1), then there is a finite expression such that

$$\sum_{i=1}^{n} a_i f_i = 1, \quad a_i \in A$$

So we can cover X just using $X_{f_1}, \ldots, X_{f_n}$.

For (6). The proof is same as (5), just replacing (1) by (f).

For (7). Just by definition of quasi-compact. □

Exercise 1.8.18. For psychological reasons it is sometimes convenient to denote a prime ideal of A by a letter such as x or y when thinking of it as a point of $X = \operatorname{Spec} A$. When thinking of x as a prime ideal of A, we denote it by $\mathfrak{p}_x$ (logically, of course, it is the same thing). Show that

(1) the set $\{x\}$ is closed in $\operatorname{Spec} A \Leftrightarrow \mathfrak{p}_x$ is maximal.
(2) $\overline{\{x\}} = V(\mathfrak{p}_x)$
(3) $y \in \overline{\{x\}} \Leftrightarrow \mathfrak{p}_x \subseteq \mathfrak{p}_y$.

[2]Here X is called quasi-compact if every open covering of X has a finite subcovering.

(4) X is a T_0-space[3].

Proof. For (1). If $\{x\}$ is a closed set, then $\{x\} = V(\mathfrak{a})$ for some ideal $\mathfrak{a}$. So there is only one prime ideal $\mathfrak{p}_x$ containing $\mathfrak{a}$, so we must have $\mathfrak{a} = \mathfrak{p}_x$ and $\mathfrak{p}_x$ is maximal. Conversely, if $\mathfrak{p}_x$ is maximal, then $\{x\} = V(\mathfrak{p}_x)$, a closed set.

For (2). By definition the closure of $\{x\}$ is the intersection of all closed set containing $\{x\}$. That's $\bigcap_{i\in I} V(\mathfrak{a}_i)$, where the index runs over all ideals $\mathfrak{a}_i$ such that $\mathfrak{a}_i \subseteq \mathfrak{p}_x$. In particular there exists some i such that $\mathfrak{a}_i = \mathfrak{p}_x$. So

$$\overline{\{x\}} = \bigcap_{i\in I} V(\mathfrak{a}_i) = V(\bigcup_{i\in I} \mathfrak{a}_i) = V(\mathfrak{p}_x)$$

as desired.

For (3). By definition and (2) we have

$$y \in \overline{\{x\}} = V(\mathfrak{p}_x) \iff \mathfrak{p}_x \subseteq \mathfrak{p}_y$$

For (4). If every neighborhood of x contains y and vice versa, then $x \in \overline{\{y\}}$ and $y \in \overline{\{x\}}$. So by (3) we obtain $\mathfrak{p}_x = \mathfrak{p}_y$, a contradiction to the fact $x \neq y$. $\square$

Exercise 1.8.19. A topological space X is said to be 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. Show that $\operatorname{Spec} A$ is irreducible if and only if the nilradical of A is a prime ideal.

Proof. It suffices to check $X_f \cap X_g = \varnothing$ if and only if X_f or X_g is empty. For (1) of Exercise 1.8.17 we know that $X_f \cap X_g = X_{fg}$, and (2) of Exercise 1.8.17 implies $X_{fg} = 0$ if and only if fg is nilpotent. Thus it suffices to show $fg \in \mathfrak{N}$ if and only if f or g is in $\mathfrak{N}$, and that's equivalent to $\mathfrak{N}$ is prime. $\square$

Remark 1.8.2. According to Remark 1.8.1, one can see $\operatorname{Spec} A$ is irreducible if and only if A has only one minimal prime ideal. In fact, the following Exercise shows there is an one to one correspondence between irreducible components and minimal prime ideals, so it's a geometrical explanations of minimal prime ideal.

Exercise 1.8.20. Let X be a topological space.

(1) If Y is an irreducible subspace of X, then the closure P of Y in X is irreducible.
(2) Every irreducible subspace of X is contained in a maximal irreducible subspace.
(3) The maximal irreducible subspaces of X are closed and cover X. They are called the irreducible components of X. What are the irreducible components of a Hausdorff space?
(4) If A is a ring and $X = \operatorname{Spec} A$, then the irreducible components of X are the closed sets $V(\mathfrak{p})$, where $\mathfrak{p}$ is a minimal prime ideal of A

[3]A topological space X is called T_0-space, if for every distinct points $x, y \in X$, either there is a neighborhood of x which does not contain y, or else there is a neighborhood of y which does not contain x.

Proof. For (1). Let U, V be two open subsets in P, by definition of closure, $U \cap Y$ and $V \cap Y$ must be nonempty, so $U \cap Y$ and $V \cap Y$ are two nonempty subsets in Y, then $U \cap V \cap Y \neq \varnothing$, since Y is irreducible. So $U \cap Y \neq \varnothing$, which implies P is also irreducible.

For (2). Use Zorn lemma: Order the set of all irreducible subspace by inclusion. Then it suffices to show any chain $\{Y_i\}$ of irreducible subspace has an upper bound. It suffices to check $Z = \bigcup_i Y_i$ is also an irreducible subspace. Choose U, V are open in Z, and $U \cap Y_i \neq \varnothing, V \cap Y_j \neq \varnothing$. Without lose of generality we may assume $Y_i \subseteq Y_j$, thus $V \cap Y_j, U \cap Y_j$ are not empty, thus $U \cap V \cap Y_j \neq \varnothing$, since Y_j is irreducible. This completes the proof of (2).

For (3). Single points. If a subspace containing more than two distinct points, then by definition of Hausdorff, there exists two neighborhoods separating these two points, thus it's not irreducible.

For (4). In fact we can derive from the proof of Exercise 1.8.19 that every closed set $V(\mathfrak{a})$ is irreducible if and only if $r(\mathfrak{a})$ is a prime ideal. But note that $V(\mathfrak{a}) = V(r(\mathfrak{a}))$, so for any irreducible closed set Y we may write it as $V(\mathfrak{p})$ for some prime ideal $\mathfrak{p}$. It's maximal if and only if $\mathfrak{p}$ is minimal, since V is an operation reversing inclusion relation, i.e. $\mathfrak{p}' \subseteq \mathfrak{p}$ if and only if $V(\mathfrak{p}) \subseteq V(\mathfrak{p}')$. □

Exercise 1.8.21 (morphism of spectrum)**.** Let $\phi \colon A \to B$ be a ring homomorphism. Let $X = \operatorname{Spec} A$ and $Y = \operatorname{Spec} B$. Then ϕ induces a mapping $\phi^* \colon Y \to X$. Show that

(1) If $f \in A$ then $\phi^{*-1}(X_f) = Y_{\phi(f)}$, and hence that ϕ^* is continuous.
(2) If $\mathfrak{a}$ is an ideal of A, then $\overline{\phi^{*-1}(V(\mathfrak{a}))} = V(\mathfrak{a}^e)$.
(3) If $\mathfrak{b}$ is an ideal of B, then $\overline{\phi^*(V(\mathfrak{b}))} = V(\mathfrak{b}^c)$.
(4) If ϕ is surjective, then ϕ^* is a homeomorphism of Y onto the closed subset $V(\ker(\phi))$ of X.
(5) If ϕ is injective, then $\phi^*(Y)$ is dense in X. More precisely, $\phi^*(Y)$ is dense in $X \Leftrightarrow \ker(\phi) \subseteq \mathfrak{N}$.
(6) Let $\psi \colon B \to C$ be another ring homomorphism. Then $(\psi \circ \phi)^* = \phi^* \circ \psi^*$.
(7) Let A be an integral domain with just one non-zero prime ideal $\mathfrak{p}$, and let K be the field of fractions of A. Let $B = (A/\mathfrak{p}) \times K$. Define $\phi \colon A \to B$ by $\phi(x) = (\bar{x}, x)$, where $\bar{x}$ is the image of x in $A/\mathfrak{p}$. Show that ϕ^* is bijective but not a homeomorphism.

Proof. For (1). Directly check by definition: Note that $\mathfrak{q} \in Y_{\phi(f)} = (V(\phi(f)))^c$ is equivalent to $\mathfrak{q}$ doesn't contain $(\phi(f))$, in other words: $\phi(f) \notin \mathfrak{q}$. So

$$\mathfrak{q} \in Y_{\phi(f)} \Leftrightarrow \phi(f) \notin \mathfrak{q} \Leftrightarrow f \notin \phi^*(\mathfrak{q}) \Leftrightarrow \phi^*(\mathfrak{q}) \in X_f \Leftrightarrow \mathfrak{q} \in \phi^{*-1}(X_f)$$

Thus $\phi^{*-1}(X_f) = Y_{\phi(f)}$.

For (2). First we claim that for two ideals $\mathfrak{a} \in A, \mathfrak{b} \in B$, we have

$$\mathfrak{a} \subseteq \mathfrak{b}^c \Longleftrightarrow \mathfrak{a}^e \subseteq \mathfrak{b}$$

Indeed, if $\mathfrak{a} \subseteq \mathfrak{b}^c$, then $\mathfrak{a}^e \subseteq \mathfrak{b}^{ce} \subseteq \mathfrak{b}$. Conversely, if $\mathfrak{a}^e \subseteq \mathfrak{b}$, then $\mathfrak{a} \subseteq \mathfrak{a}^{ec} \subseteq \mathfrak{b}^c$. So

$$\mathfrak{q} \in \phi^{*-1}(V(\mathfrak{a})) \Leftrightarrow \phi^*(\mathfrak{q}) \in V(\mathfrak{a}) \Leftrightarrow \mathfrak{a} \subseteq \mathfrak{q}^c \Leftrightarrow \mathfrak{a}^e \subseteq \mathfrak{q} \Leftrightarrow \mathfrak{q} \in V(\mathfrak{a}^e)$$

For (3). Let's give a general description for closed sets: For $Y \subseteq X$, then

$$\overline{Y} = \bigcap\{V(\mathfrak{a}) \mid Y \subseteq V(\mathfrak{a})\} = \bigcap\{V(\mathfrak{a}) \mid \mathfrak{a} \subseteq \bigcap_{y \in Y} \mathfrak{p}_y\} = V(\bigcup\{\mathfrak{a} : \mathfrak{a} \subseteq \bigcap_{y \in Y} \mathfrak{p}_y\}) = V(\bigcap_{y \in Y} \mathfrak{p}_y)$$

So if we take $Y = \phi^*(V(\mathfrak{b}))$, then

$$\bigcap_{y \in \phi^*(V(\mathfrak{b}))} \mathfrak{p}_y = \bigcap\{\mathfrak{q}^c : \mathfrak{q} \in V(\mathfrak{b})\} = (\bigcap_{\mathfrak{q} \in V(\mathfrak{b})} \mathfrak{q})^c = r(\mathfrak{b})^c = r(\mathfrak{b}^c)$$

But $V(r(\mathfrak{b}^c)) = V(\mathfrak{b}^c)$.

For (4). If ϕ is surjective, and use $\mathfrak{a}$ to denote $\ker\phi$. We can identify B as $A/\mathfrak{a}$ using $\widetilde{\phi} : A/\mathfrak{a} \to B$, the restriction of ϕ to $A/\mathfrak{a}$. Then we have the following commutative diagram

$$\begin{tikzcd}
\operatorname{Spec} B \arrow[r, "\phi^*"] \arrow[d, "\widetilde{\phi}^*"'] & V(\mathfrak{a}) \subset X \\
\operatorname{Spec}(A/\mathfrak{a}) \arrow[ur, "p^*"] &
\end{tikzcd}$$

where p^* is defined by mapping $\mathfrak{p}/\mathfrak{a}$ to $\mathfrak{p}$. $p^*\colon \operatorname{Spec}(A/\mathfrak{a}) \to V(\mathfrak{a})$ is bijective, since there is a one to one correspondence between $V(\mathfrak{a})$ and $\operatorname{Spec}(A/\mathfrak{a})$. So it suffices to check p^* is a closed and continuous: Take a closed set in $\operatorname{Spec}(A/\mathfrak{a})$, denote by $V(\mathfrak{b}/\mathfrak{a})$, then

$$\begin{aligned}
p^*(V(\mathfrak{b}/\mathfrak{a})) &= p^*(\{\mathfrak{p}/\mathfrak{a} : \mathfrak{b} \subseteq \mathfrak{p}, \mathfrak{p} \text{ is prime}\}) \\
&= \{\mathfrak{p} : \mathfrak{b} \subseteq \mathfrak{p}, \mathfrak{p} \text{ is prime}\} \\
&= V(\mathfrak{b})
\end{aligned}$$

And

$$p^{*-1}(V(\mathfrak{b})) = V(\mathfrak{b}/\mathfrak{a})$$

for the same reason. So $p^*\colon \operatorname{Spec}(A/\mathfrak{a}) \to V(\mathfrak{a})$ is a homeomorphism, thus ϕ^* is.

For (5). $\phi^*(Y)$ is dense if and only if $\overline{\phi^*(Y)} = X$. Note that $Y = V((0))$, thus by (3) we have

$$X = \overline{\phi^*(Y)} = \overline{\phi^*(V((0)))} = V((0)^c) = V(\ker\phi)$$

But every prime ideal contains $\ker\phi$ if and only if $\ker\phi \in \mathfrak{N}$.

For (6). It's clear.

For (7). There are only two prime ideals of A: zero ideal and $\mathfrak{p}$. For B, prime ideals are $A/\mathfrak{p} \times \{0\}$ and $\{0\} \times K$, B is not a domain since we have $(1,0)(0,1) = (0,0)$. And it's clear

$$\begin{cases} \phi^*(\{0\} \times K) = \mathfrak{p} \\ \phi^*(A/\mathfrak{p} \times \{0\}) = (0) \end{cases}$$

Thus ϕ^* is bijective. But their topology is different: closed sets in $\operatorname{Spec} A$ are two sets such that one contains another, but closed sets in $\operatorname{Spec} B$ are two disjoint sets. $\square$

Exercise 1.8.22. Let $A = \prod_{i=1}^n A_i$ be the direct product of rings $A_{\rm i}$. Show that $\operatorname{Spec} A$ is the disjoint union of open (and closed) subspaces X_i, where X_i is canonically homeomorphic with $\operatorname{Spec} A_i$. Conversely, let A be any ring. Show that the following statements are equivalent:

(1) $X = \operatorname{Spec} A$ is disconnected.
(2) $A \cong A_1 \times A_2$ where neither of the rings A_1, A_2 is the zero ring.
(3) A contains an idempotent $\neq 0, 1$.

In particular, the spectrum of a local ring is always connected.

Proof. For first part: For each i consider the projection $p_i : \prod A_i \to A_i$. It's a surjective, then by (4) of Exercise 1.8.21, we obtain a homeomorphism $X_i = V(\ker p_i) \cong \operatorname{Spec}(A_i)$. We claim $\{X_i\}$ covers A and $X_i \cap X_j$ for distinct i, j. Note that we can write X_i explicitly as $V(\prod_{i\neq j} A_j)$. Then

$$\bigcup V(\prod_{i\neq j} A_j) = V(\bigcap \prod_{i\neq j} A_j) = V((0)) = X$$

And

$$X_i \cap X_j = V(\prod_{i\neq j} A_j + \prod_{i\neq j} A_i) = V((1)) = \varnothing$$

As desired.

For the half part: (1) to (3). If $X = \operatorname{Spec} A$ is disconnected, then there exists an subset U which is both open and closed, so is its complement. Assume $U = V(\mathfrak{a}), U^c = V(\mathfrak{b})$. $U \cap U^c = \varnothing$ implies $V(\mathfrak{a}) \cap V(\mathfrak{b}) = V(\mathfrak{a}+\mathfrak{b}) = \varnothing$, thus $\mathfrak{a} + \mathfrak{b} = (1)$, so there exists $x \in \mathfrak{a}, y \in \mathfrak{b}$ such that $x + y = 1$. $U \cup U^c = X$ implies $V(\mathfrak{a}) \cup V(\mathfrak{b}) = V(\mathfrak{ab}) = X$, thus $\mathfrak{ab} \subseteq \mathfrak{N}$, that is xy is nilpotent. So consider $x^2 - x = xy$, we obtain a nontrivial idempotent in $A/\mathfrak{N}$. Now let's prove the following lemma to conclude:

Lemma 1.8.1. Let A be a ring, then every idempotent of $A/\mathfrak{N}$ lifts to some idempotent of A.

Proof. Assume $x \in A$ such that $x^2 - x$ is nilpotent, so there exists n such that $0 = (x^2 - x)^n = x^n(x-1)^n$. Since x^n and $(x-1)^n$ are coprime, the Chinese Remainder theorem gives us $A \cong A/x^n \times A/(x-1)^n$. The preimage of $(0, 1)$ is an idempotent $e \in A$ such that $x - e$ is nilpotent, so that e is the desired lift. $\square$

For (3) to (2): Suppose e is a nontrivial idempotent, then $1 - e$ is also a nontrivial idempotent, so (e) and $(1-e)$ are two proper ideals. Furthermore they are coprime since $1 - e + e = 1$ and $(1-e) \cap e = (0)$ since $e(1-e) = 0$. Then consider $A \to A/(e) \times A/(1-e)$, an isomorphism of rings.

For (2) to (1): It's clear. In particular, the spectrum of a local ring is always connected, since Exercise 1.8.12 implies there is no nontrivial idempotent. $\square$

Exercise 1.8.23. Let A be a Boolean ring, and let $X = \operatorname{Spec} A$.

(1) For each $f \in A$, the set X_f is both open and closed in X.
(2) Let $f_1, \ldots, f_n \in A$. Show that $X_{f_1} \cup \ldots \cup X_{f_n} = X_f$ for some $f \in A$.
(3) The sets X_f are the only subsets of X which are both open and closed.
(4) X is a compact Hausdorff space.

Proof. For (1). Clearly X_f is open, it's closed since $V(f) = X_{1-f}$. Indeed, since $(f) + (1-f) = (1)$ and $(f) \cap (1-f) = (0)$, then a prime ideal contains (f) if and only if it doesn't contain $(1-f)$. So X_f is both closed and open.

For (2). Note that

$$\bigcup_i X_{f_i} = \bigcup_i (V(f_i)^c) = (\bigcap V(f_i))^c = (V(\sum (f_i)))^c$$

But we know that every finitely generated ideal of a Boolean ring is principal, so $\sum(f_i) = (f)$ for some $f \in A$.

For (3). Let $Y \subseteq X$ be both open and closed. Since Y is open, it is a union of basic open sets X_f. Since Y is closed and X is quasi-compact, Y is quasi-compact. Hence Y is a finite union of basic open sets. now use (2) above.

For (4). It suffices to show X is Hausdorff. Take $x, y \in X$. We claim that there exists a X_f such that $x \in X_f$ and $y \in X_{1-f}$. If not, then for all X_f we have $x, y \in X_f$, then $y \in \overline{\{x\}}$ and $x \in \overline{\{y\}}$. By (3) of Exercise 1.8.18 we have $x = y$, a contradiction. $\square$

Exercise 1.8.24. Let A be a ring. The subspace of $\operatorname{Spec} A$ consisting of the maximal ideals of A, with the induced topology, is called the maximal spectrum of A and is denoted by $\operatorname{mSpec}(A)$.

Let X be a compact Hausdorff space and let $C(X)$ denote the ring of all real-valued continuous functions on X. For each $x \in X$, let $\mathfrak{m}_x$ be the set of all $f \in C(X)$ such that $f(x) = 0$. The ideal $\mathfrak{m}_x$ is maximal, because it is the kernel of the (surjective) homomorphism $C(X) \to \mathbb{R}$ which takes f to $f(x)$. If $\widetilde{X}$ denotes $\operatorname{mSpec}(C(X))$, we have therefore defined a mapping $\mu\colon X \to \widetilde{X}$, namely $x \mapsto \mathfrak{m}_x$. We shall show that μ is a homeomorphism of X onto $\widetilde{X}$.

(1) Let $\mathfrak{m}$ be any maximal ideal of $C(X)$ and let $V = V(\mathfrak{m})$ be the set of common zeros of the functions in $\mathfrak{m}$: that is,

$$V = \{x \in X : f(x) = 0 \text{ for all } f \in \mathfrak{m}\}$$

Suppose that V is empty. Then for each $x \in X$ there exists $f_x \in \mathfrak{m}$ such that $f_x(x) \neq 0$. Since f_x is continuous, there is an open neighborhood U_x of x in X on which f_x does not vanish. By compactness a finite number of the neighborhoods, say $U'_{x_1}, \ldots, U'_{x_n}$ cover X. Let

$$f = f_{x_1}^2 + \cdots + f_{x_n}^2$$

Then f does not vanish at any point of X, hence is a unit in $C(X)$. But this contracts $f \in \mathfrak{m}$, hence V is not empty.

Let x be a point of V. Then $\mathfrak{m} \subseteq \mathfrak{m}_x$ hence $\mathfrak{m} = \mathfrak{m}_x$ because $\mathfrak{m}$ is maximal. Hence μ is surjective.

(2) By Urysohn's lemma (this is the only non-trivial fact required in the argument) the continuous functions separate the points of X. Hence $x \neq y$ implies $\mathfrak{m}_x \neq \mathfrak{m}_y$, and therefore μ is injective.

(3) Let $f \in C(X)$. let

$$U_f = \{x \in X : f(x) \neq 0\}$$
$$\widetilde{U}_f = \{\mathfrak{m} \in \widetilde{X} : f \notin \mathfrak{m}\}$$

Show that $\mu(U_f) = \widetilde{U}_f$. The open sets U_f (resp. $\widetilde{U}_f$) form a basis of the topology of X (resp. $\widetilde{X}$) and therefore μ is a homeomorphism. Thus X cun be reconstructed from the ring of functions $C(X)$.

Proof. (1) is trivial. For (2). Urysohn's lemma says that a topological space is normal if and only if any two disjoint closed subsets can be separated by a continuous function. And basic point topology tells us a compact Hausdorff space is normal.

For (3). For each $f \in C(X)$, we have

$$f \in U_f \Leftrightarrow f(x) \neq 0 \Leftrightarrow f \notin \mathfrak{m}_x \Leftrightarrow \mathfrak{m}_x \in \widetilde{U}_f$$

So $\mu(U_f) = \widetilde{U}_f$. Now let's prove U_f will form a basis of the topology of X: For $x \in X$, choose a open neighborhood V of x, and consider two disjoint closed sets $\{x\}$ and V^c, by Urysohn's lemma there exists $f \in C(X)$ such that $f(x) = 1$ and $f(V^c) = 0$, thus $x \in U_f$, that is U_f forms a basis of X. $\widetilde{U}_f$ forms a basis of $\widetilde{X}$, since its the restriction of $\mathrm{Spec}(C(X))_f$, which is a basis of $\mathrm{Spec}(C(X))$.

□

Exercise 1.8.25 (affine algebraic varieties)**.** Let k be an algebraically closed field and let

$$f_\alpha\left(t_1, \ldots, t_n\right) = 0$$

be a set of polynomial equations in n variables with coefficients in k. The set X of all points $x = (x_1, \ldots, x_n) \in k^n$ which satisfy these equations is an affine algebraic variety.

Consider the set of all polynomials $g \in k\left[t_1, \ldots, t_n\right]$ with the property that $g(x) = 0$ for all $x \in X$. This set is an ideal $I(X)$ in the polynomial ring, and is called the ideal of the variety X. The quotient ring

$$P(X) = k\left[t_1, \ldots, t_n\right]/I(X)$$

is the ring of polynomial functions on X, because two polynomials g, h define the same polynomial function on X if and only if $g - h$ vanishes at every point of X, that is, if and only if $g - h \in I(X)$.

Let ξ_i be the image of t_i in $P(X)$. The $\xi_i (1 \leq i \leq n)$ are the coordinate functions on X: If $x \in X$, then $\xi_i(x)$ is the ith coordinate of x. $P(X)$

is generated as a k-algebra by the coordinate functions, and is called the coordinate ring (or affine algebra) of X.

For each $x \in X$, let $\mathfrak{m}_x$ be the ideal of all $f \in P(X)$ such that $f(x) = 0$, and it is a maximal ideal of $P(X)$. Hence, if $\widetilde{X} = \mathrm{mSpec}(P(X))$, we have defined a mapping $\mu\colon X \to \widetilde{X}$, namely $x \mapsto \mathfrak{m}_x$.

It is easy to show that μ is injective: If $x \neq y$ we must have $x_i \neq y_i$ for for some $i(1 \leq i \leq n)$, and hence $\xi_i - x_i$ is in $\mathfrak{m}_x$ but not in $\mathfrak{m}_y$, so that $\mathfrak{m}_x \neq \mathfrak{m}_y$. What is less obvious (but still true) is that μ is surjective. This is one form of Hilbert's Nullstellensatz.

Proof. Now let's prove this weak weak form of Nullstellensatz: Here in order to avoid a too long proof, we use a weak version of Nullstellensatz, which will be mentioned in Corollary 7.10 of [AM69].

Corollary 1.8.1. Let k be a field, A a finitely generated k-algebra. Let $\mathfrak{m}$ be a maximal ideal of A. Then the field $A/\mathfrak{m}$ is a finite algebraic extension of k. In particular, if k is algebraically closed, then $A/\mathfrak{m} \cong k$.

Firstly, let's clarify what does $\mathfrak{m}_x$ look like: For $x \in X$, write it as $x = (x_1, \ldots, x_n)$ where $x_i \in k$. Since $\mathfrak{m}_x$ is the kernel of the following morphism

$$\begin{aligned} P(X) &\to k \\ f &\mapsto f(x) \end{aligned}$$

It's clear to see $\mathfrak{m}_x = (\xi_1 - x_1, \ldots, \xi_n - x_n)$ in this point of view, where ξ_i is the coordinates of $P(X)$. So we need to show for any maximal ideal $\mathfrak{m}$ in $P(X)$, it takes this form.

By Corollary 1.8.1 we have $\varphi\colon P(X) \to P(X)/\mathfrak{m} \cong k$, then use x_i to denote the image of ξ_i in $P(x)/\mathfrak{m}$, then clearly $(\xi_1 - x_1, \ldots, \xi_n - x_n) \subseteq \ker \varphi = \mathfrak{m}$, by the maximality of $(\xi_1 - x_1, \ldots, \xi_n - x_n)$ to conclude $\mathfrak{m} = \mathfrak{m}_x$, where $x = (x_1, \ldots, x_n)$. □

Exercise 1.8.26 (regular mapping)**.** Let $f_1, \ldots, f_m$ be elements of $k[t_1, \ldots, t_n]$. They determine a polynomial mapping $\phi\colon k^n \to k^m$: if $x \in k^n$, the coordinates of $\phi(x)$ are $f_1(x), \ldots, f_m(x)$.

Let X, Y be affine algebraic varieties in k^n, k^m respectively, A mapping $\phi\colon X \to Y$ is said to be regular if ϕ is the restriction to X of a polynomial mapping from k^n to k^m.

If η is a polynomial function on Y, then $\eta \circ \phi$ is a polynomial function on X. Hence ϕ induces a k-algebra homomorphism $P(Y) \to P(X)$, namely $\eta \mapsto \eta \circ \phi$. Show that in this way we obtain a one-to-one correspondence between the regular mappings $X \to Y$ and the k-algebra homomorphisms $P(Y) \to P(X)$.

Proof. For a regular mapping $\phi\colon X \to Y$, we use $\phi^{\#}$ to denote the k-algebra homomorphism induced by ϕ.

For injectivity: If $\phi^{\#} = \psi^{\#} : P(Y) \to P(X)$ are two k-algebra homomorphisms, then we need to check ϕ and ψ are the same regular functions. It suffices to check for each coordinate. Use $\{y_i\}_{i=1}^m$ to denote the coordinate functions on Y. Thus

$$\phi_i := y_i \circ \phi = \phi^{\#}(y_i) = \psi^{\#}(y_i) = y_i \circ \psi =: \psi_i$$

So we have $\phi_i = \psi_i$ for each i on X, thus $\phi = \psi$ on X.

For surjectivity: For a k-algebra homomorphism $f\colon P(Y) \to P(X)$, we need to find a regular mapping ϕ such that $\phi^{\#} = f$. We need to construct coordinate by coordinate. Consider $f(y_i) \in P(X)$, it gives an element ϕ_i in $k[t_1, \ldots, t_n]$, since $P(X) = k[t_1, \ldots, t_n]/I(X)$. Claim that regular mapping induced by $\phi_1, \ldots, \phi_m$ is what we desired. Indeed, it suffices to check on each $\{y_i\}$, since $P(Y)$ is generated by these elements.

$$\phi^{\#}(y_i) = y_i \circ \phi = \phi_i = f(y_i)$$

This completes the proof. $\square$

2. Modules

2.1. Modules and homomorphisms.

Definition 2.1.1 (A-module)**.** Let A be a ring. An A-module is an abelian group M on which A acts linearly.

Remark 2.1.1. Equivalently, M is an abelian group with a ring homomorphism $A \to \operatorname{End} M$, where $\operatorname{End} M$ is the ring of endomorphisms of the abelian groups.

Remark 2.1.2. If you' re familiar with representation theory, a representation of a group G is a group homomorphism $\rho\colon G \to \mathrm{GL}(V)$, where V is a finite dimensional vector space over a field k. Consider the group-ring induced from G:

$$k[G] := \{\sum a_i g_i \mid a_i \in k, g_i \in G\}$$

It's a ring, and we can make V into a $k[G]$-module using $\widetilde{\rho}\colon k[G] \to \mathrm{GL}(V)$, where $\widetilde{\rho}$ is obtained from ρ by extending linearly. Conversely, for a $k[G]$-module we can obtain a representation of G. So as you can guess, it's a quite important method to study representation theory using modules.

Definition 2.1.2 (morphism of modules)**.** Let M, N be A-modules. A mapping $f\colon M \to N$ is an A-module homomorphism if it's a group homomorphism which commutes with the action of A.

Notation 2.1.1. We use $\operatorname{Hom}(M, N)$ to denote the set of all A-module homomorphisms between M and N.

Remark 2.1.3. There is a natural A-module structure on $\operatorname{Hom}(M, N)$, given by

$$\begin{aligned}(f+g)(x) &:= f(x) + g(x)\\ (af)(x) &:= af(x)\end{aligned}$$

Definition 2.1.3 (submodule)**.** A submodule M' of M is a subgroup of M which is closed under the action of A.

Definition 2.1.4 (quotient module)**.** For a submodule M' of M, the abelian group M/M' inherits an A-module structure from M, and it's called a quotient module.

2.2. Operations on submodules.

Most operations on ideals considered in Chapter 1 have their counterparts for modules. Let M be an A-module and let $(M_i)_{i\in I}$ be a family of submodules of M. Their sum $\sum M_i$ is the set of all finite sum $\sum x_i$, where $x_i \in M_i$ for all $i \in I$. The intersection $\bigcap M_i$ is again a submodules of M.

Although we can not define the product of two submodules, we can define the product $\mathfrak{a}M$, where $\mathfrak{a}$ is an ideal and M an A-module.

If N, P are submodules of M, we define $(N : P)$ to be the set of $a \in A$ such that $aP \subseteq N$, it's an ideal of A. In particular, $(0 : M)$ is called annihilator of M, and denoted by $\mathrm{Ann}(M)$. If $\mathfrak{a} \subseteq \mathrm{Ann}(M)$, we may regard M as an $A/\mathfrak{a}$-module.

An A-module is faithful if $\mathrm{Ann}(M) = 0$.

Exercise 2.2.1. For annihilator, we have

(1) $\mathrm{Ann}(M + N) = \mathrm{Ann}(M) \cap \mathrm{Ann}(N)$
(2) $(N : P) = \mathrm{Ann}((N + P)/N)$

Proof. Trivial. □

For an element $x \in M$, the set of all multiplies $ax, a \in A$ is a submodule of M, denoted by Ax or (x). If $M = \sum_i Ax_i$, then x_i are said to be a set of generators of M. An A-module M is said to be finitely generated if it has a finite set of generators.

Proposition 2.2.1. *M is a finitely generated A-module if and only if M is isomorphic to a quotient of A^n for some $n > 0$.*

Proposition 2.2.2. *Let M be a finitely generated A-module, let $\mathfrak{a}$ be an ideal of A, and let ϕ be an A-module endomorphism of M such that $\phi(M) \subset \mathfrak{a}M$. Then ϕ satisfies an equation of the form*

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

where $a_i \in \mathfrak{a}$.

Corollary 2.2.1. *Let M be a finitely generated A-module and let $\mathfrak{a}$ be an ideal of A such that $\mathfrak{a}M = M$. Then there exists $x \equiv 1 \pmod{\mathfrak{a}}$ such that $xM = 0$*

Proposition 2.2.3 (Nakayama's lemma)**.** *Let M be a finitely generated A-module and $\mathfrak{a}$ an ideal of A contained in the Jacobson radical $\mathfrak{R}$ of A. Then $\mathfrak{a}M = M$ implies $M = 0$.*

Proof. By Corollary 2.2.1 there exists x such that $xM = 0$ and $x \equiv 1 \pmod{\mathfrak{a}}$. From $1 - x \in \mathfrak{a} \subseteq \mathfrak{R}$, we know that there for any $y \in A$ such that $1 - y(1 - x)$ is unit. Take $y = 1$ we obtain x is a unit. Thus $M = x^{-1}xM = 0$. □

Corollary 2.2.2. *Let M be a finitely generated A-module, N a submodule of M, $\mathfrak{a} \subseteq \mathfrak{R}$. Then $M = \mathfrak{a}M + N$ implies $M = N$.*

Let $(A, \mathfrak{m})$ be a local ring, and $k = A/\mathfrak{m}$ its residue field. Let M be a finitely generated A-module. Note that $A/\mathfrak{m}M$ is annihilated by $\mathfrak{m}$, hence a $A/\mathfrak{m}$-module, that's a finite dimensional k-vector space.

Proposition 2.2.4. *Let x_i be elements in M whose images in $M/\mathfrak{m}M$ form a basis of this vector space. Then x_i generate M.*

2.3. **Tensor product.**

Definition 2.3.1 (Tensor product)**.** Let M, N be A-modules, then the tensor product of M and N is a A-module T together with a A-bilinear map $g\colon M \times N \to T$ such that for any A-module P and any A-bilinear map $f\colon M \times N \to T$, there exists a unique A-module homomorphism $\widetilde{f}$ such that the following diagram commutes:

$$\begin{tikzcd} M \times N \arrow[rr, "f"] \arrow[dr, "g"'] & & P \\ & T \arrow[ur, dashed, "\widetilde{f}"'] & \end{tikzcd}$$

Notation 2.3.1. We always use $M \otimes N$ to denote the tensor product of M and N, and it's generated as A-modules by $x \otimes y$.

Remark 2.3.1. Note that $x \otimes y$ is inherently ambiguous unless we specify the tensor product to which it belongs. Let M', N' be submodules of M, N respectively, and let $x \in M', y \in N'$. Then it can happen that $x \otimes y$ as an element of $M \otimes N$ is zero whilst $x \otimes y$ as an element of $M' \otimes N'$ is not zero. For example, take $A = \mathbb{Z}, M = \mathbb{Z}, N = \mathbb{Z}/2\mathbb{Z}$ and let M' be the submodules $2\mathbb{Z}$ of M and $N' = N$. Consider $2 \otimes x$. As an element in $M \otimes N$ it's zero, since

$$2 \otimes x = 1 \otimes 2x = 1 \otimes 0 = 0$$

But as an element of $M' \otimes N'$ it's not zero. Indeed, consider the following map

$$\begin{aligned} B : 2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} &\to \mathbb{Z}/2\mathbb{Z} \\ (2m, n + 2\mathbb{Z}) &\mapsto mn + 2\mathbb{Z} \end{aligned}$$

Let's check B is well-defined and bilinear:

(1) It's well-defined, since take $n' = n+2k$, then $(2m, n'+2\mathbb{Z}) \mapsto mn'+2\mathbb{Z} = mn + 2km + 2\mathbb{Z} = mn + 2\mathbb{Z}$.
(2) It's clearly B is bilinear.

Then it induces a linear map

$$\begin{aligned} \beta : (2\mathbb{Z}) \otimes \mathbb{Z}/2\mathbb{Z} &\to \mathbb{Z}/2\mathbb{Z} \\ 2m \otimes (n + 2\mathbb{Z}) &\mapsto mn + 2\mathbb{Z} \end{aligned}$$

But $\beta(2 \otimes x) = x \neq 0 \in \mathbb{Z}/2\mathbb{Z}$, thus $2 \otimes x \neq 0 \in 2\mathbb{Z} \otimes \mathbb{Z}/2\mathbb{Z}$.

Corollary 2.3.1. Let $x_i \in M, y_i \in N$ be such that $\sum x_i \otimes y_i = 0 \in M \otimes N$. Then there exists finitely generated submodules M_0 of M and N_0 of N such that $\sum x_i \otimes y_i = 0$ in $M_0 \otimes N_0$.

Exercise 2.3.1. Let A, B be rings, let M be an A-module, P a B-module and N an (A, B)-bimodule (that is, N is simultaneously an A-module and a B-module and the two structures are compatible in the sense that $a(xb) = (ax)b$ for all $a \in A$, $b \in B, x \in N$). Then $M \otimes_A N$ is naturally a B-module, $N \otimes_B P$ an A-module, and we have

$$(M \otimes_A N) \otimes_B P \cong M \otimes_A (N \otimes_B P)$$

Proof. We need to use universal property of tensor product to construct morphism from $(M \otimes_A N) \otimes_B P \to M \otimes_A (N \otimes_B P)$ and its inverse.

Firstly, for each $x \in A$, consider the following map

$$\begin{aligned} f_x : N \times P &\to (M \otimes_A N) \otimes_B P \\ (y, z) &\mapsto (x \otimes y) \otimes z \end{aligned}$$

It's a B-bilinear mapping. Indeed, for $b \in B$, we have

$$\begin{aligned} f_x(yb, z) &= (x \otimes yb) \otimes z = (x \otimes y)b \otimes z = ((x \otimes y) \otimes z))b = f_x(y, z)b \\ f_x(y, zb) &= (x \otimes y) \otimes zb = ((x \otimes y) \otimes z))b = f_x(y, z)b \end{aligned}$$

So each f_x induces a B-linear map $\widetilde{f_x}\colon N \otimes_B P \to (M \otimes_A N) \otimes_B P$, by taking $y \otimes z$ to $(x \otimes y) \otimes z$. Allowing x to vary we obtain a bi-additive map $g\colon A \times (N \otimes_B P) \to (M \otimes_A N) \otimes_B P$. It's A-bilinear. Indeed, for $a \in A$

$$g(ax, y \otimes z) = (ax \otimes y) \otimes z = a(x \otimes y) \otimes z = a((x \otimes y) \otimes z) = ag(x, y \otimes z)$$
$$g(x, a(y \otimes z)) = (x \otimes ay) \otimes z = a(x \otimes y) \otimes z = a((x \otimes y) \otimes z) = ag(x, y \otimes z)$$

Thus g induces a (A, B)-linear map $\widetilde{g}\colon (M \otimes_A N) \otimes_B P \to M \otimes_A (N \otimes_B P)$, by taking $x \otimes (y \otimes z)$ to $(x \otimes y) \otimes z$. A symmetric argument gives the inverse map. □

2.4. **Restriction and Extension of scalars.** Let $f\colon A \to B$ be a homomorphism of rings and let N be a B-module. Then N has an A-module structure defined as follows: If $a \in A$ and $x \in N$, we define ax to be $f(a)x$ using B-module structure on N. This A-module is said to be obtain from N be restriction of scalars. In particular, f defines in this way an A-module structure on B.

Now let M be an A-module. Since B can be regarded as an A-module, we can obtain an A-module $M_B = B \otimes_A M$. The B-module M_B is said to be obtained from M by extension of scalars.

Remark 2.4.1. Now let's back to what we have mentioned in Remark 2.1.2. For a group G and its subgroup H. There is a natural inclusion

$$i : k[H] \to k[G]$$

of group-rings generated by G and H. So using restriction of scalars, we obtain a $k[H]$-module from a $k[G]$-module. That is we can obtain a representation of H from that of G just by restriction. This is called restriction representation.

Conversely, from a $k[H]$-module, we can obtain a $k[G]$-module by tensoring $k[G]$. That is we can obtain a representation of G from that of H. This is called induced representation.

2.5. **Exactness property of tensor product.** For a A-module N, if the functor $- \otimes N$ is an exact functor on the category of A-modules. Then N is called a flat A-module.

Proposition 2.5.1. For an A-module N, the following statements are equivalent.

(1) N is flat.
(2) If $f\colon M' \to M$ is injective and M, M' are finitely generated, then $f \otimes 1 : M' \otimes N \to M \otimes N$ is injective.

Exercise 2.5.1. If $f\colon A \to B$ is a ring homomorphism and M is a flat A-module, then $M_B = B \otimes_A M$ is a flat B-module.

Proof. For any exact sequence $0 \to A_1 \to A_2$ of B-module, it suffices to check

$$0 \to A_1 \otimes_B (B \otimes_A M) \to A_2 \otimes_B (B \otimes_A M)$$

is exact. Using canonical isomorphism we have above sequence is equivalent to the following one

$$0 \to (A_1 \otimes_B B) \otimes_A M \to (A_2 \otimes_B B) \otimes_A M$$

It's exact, since $A_1 \otimes_B B = A_1, A_2 \otimes_B B = A_2$ and M is flat. □

2.6. **Algebras.**

Definition 2.6.1 (algebra)**.** The ring B, equipped with a A-module structure, is said to be an A-algebra. In other words, an A-algebra is a ring B together with a ring homomorphism $f\colon A \to B$.

Remark 2.6.1. In particular, if A is a field k, then f is injective and therefore k can be canonically identified with its image in B. Thus a k-algebra is effectively a ring containing k as a subring.

Example 2.6.1. The group-ring $k[G]$ we mentioned before is a k-algebra in fact, and sometimes is called group-algebra.

Definition 2.6.2 (finite algebra)**.** A ring homomorphism $f\colon A \to B$ is finite, and B is a finite A-algebra, if B is finite generated as A-module.

Definition 2.6.3 (finite generated algebra)**.** A ring homomorphism $f\colon A \to B$ is finite type, and B is a finitely generated A-algebra, if there exists an A-algebra homomorphism from a polynomial ring $A[x_1, \dots, x_n]$ onto B.

Remark 2.6.2. Finite A-algebra is a quite strong requirement: For example, the polynomial $k[x]$ is a finite generated k-algebra, but not a finite k-algebra.

2.7. **Tensor product of Algebras.** Let B, C be two A-algebras, $f\colon A \to B, g\colon A \to C$ the corresponding homomorphisms. Since B, C are A-modules we may form their tensor product $D = B \otimes_A C$, which is an A-module. To make it into an A-algebra, it suffices to define a multiplication on D. Consider the following map $B \times C \times B \times C \to D$, as

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

It induces an A-module homomorphism

$$B \otimes C \otimes B \otimes C \to D$$

that's $D \otimes D \to D$. It corresponds to an A-bilinear mapping $\mu\colon D \times D \to D$ such that

$$\mu(b \otimes c, b' \otimes c') = bb' \otimes cc'$$

Thus we give a multiplication on D, making it into a commutative ring.

2.8. **Part of solutions of Chapter 2.**

Exercise 2.8.1. Show that $(\mathbb{Z}/m\mathbb{Z}) \otimes_{\mathbb{Z}} (\mathbb{Z}/n\mathbb{Z}) = 0$ if m, n are coprime.

Proof. Now we're going to prove the following isomorphism

$$\mathbb{Z}/m\mathbb{Z} \otimes \mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}/\gcd(m,n)\mathbb{Z}$$

Consider the following mapping

$$\begin{aligned} \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z} &\to \mathbb{Z}/\gcd(m,n)\mathbb{Z} \\ (x + m\mathbb{Z}, y + n\mathbb{Z}) &\mapsto xy + \gcd(m,n)\mathbb{Z} \end{aligned}$$

It's well-defined and bilinear, and thus it induces a linear map $f\colon \mathbb{Z}/m\mathbb{Z} \otimes \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/\gcd(m,n)\mathbb{Z}$ such that

$$f(x + m\mathbb{Z} \otimes y + n\mathbb{Z}) = xy + \gcd(m,n)\mathbb{Z}$$

Consider the following map

$$\begin{aligned} g\colon \mathbb{Z}/\gcd(m,n)\mathbb{Z} &\to \mathbb{Z}/m\mathbb{Z} \otimes \mathbb{Z}/n\mathbb{Z} \\ z + \gcd(m,n)\mathbb{Z} &\mapsto (z + m\mathbb{Z}) \otimes (1 + n\mathbb{Z}) \end{aligned}$$

It's well-defined. Indeed, if we let $z' = z + k\gcd(m,n)$, then Bezout theorem implies that there exists $a, b \in \mathbb{Z}$ such that $am + bn = \gcd(m,n)$. Thus

$$\begin{aligned} (z' + m\mathbb{Z}) \otimes (1 + n\mathbb{Z}) &= (z + m\mathbb{Z}) \otimes (1 + n\mathbb{Z}) + (k(am + bn) + m\mathbb{Z}) \otimes (1 + n\mathbb{Z}) \\ &= (z + m\mathbb{Z}) \otimes (1 + n\mathbb{Z}) + (n(kb + m\mathbb{Z})) \otimes (1 + n\mathbb{Z}) \\ &= (z + m\mathbb{Z}) \otimes (1 + n\mathbb{Z}) + (kb + m\mathbb{Z}) \otimes (n + n\mathbb{Z}) \\ &= (z + m\mathbb{Z}) \otimes (1 + n\mathbb{Z}) \end{aligned}$$

It's clear $f \circ g = 1, g \circ f = 1$, so we have desired isomorphism. □

Exercise 2.8.2. Let A be a ring, $\mathfrak{a}$ an ideal, M an A-module. Show that $(A/\mathfrak{a}) \otimes_A M$ is isomorphic to $M/\mathfrak{a}M$.

Proof. Tensor the exact sequence $0 \to \mathfrak{a} \to A \to A/\mathfrak{a} \to 0$ with M, and tensor is a right exact functor we obtain the following exact sequence

$$\mathfrak{a} \otimes_A M \xrightarrow{i} A \otimes_A M \to (A/\mathfrak{a}) \otimes_A M \to 0$$

Then

$$(A/\mathfrak{a}) \otimes_A M \cong A \otimes_A M/\operatorname{im} i$$

But note that there exists an isomorphism $A \otimes_A M \to M$, given by $a \otimes m \mapsto am$. Thus it's clear to see $\operatorname{im} i$ is $\mathfrak{a}M$ under this isomorphism. □

Exercise 2.8.3. Let A be a local ring, M and N finitely generated A-modules. Prove that if $M \otimes N = 0$, then $M = 0$ or $N = 0$.

Proof. Let $\mathfrak{m}$ be the maximal ideal, $k = A/\mathfrak{m}$ the residue field. Let $M_k = k \otimes_A M \cong M/\mathfrak{m}M$ by Exercise 2.8.2. By Nakayama's lemma, $M_k = 0 \Rightarrow M = 0$. Note that by definition we have

$$\begin{aligned}(M \otimes_A N)_k &= k \otimes_A (M \otimes_A N) \\ &= (k \otimes_A M) \otimes_A N \\ &= ((k \otimes_A M) \otimes_k k) \otimes_A N \\ &= (k \otimes_A M) \otimes_k (k \otimes_A N) \\ &= M_k \otimes_k N_k\end{aligned}$$

Thus $M \otimes_A N = 0 \Rightarrow (M \otimes_A N)_k = 0 \Rightarrow M_k \otimes_k N_k = 0 \Rightarrow M_k = 0$ or $N_k = 0$, since M_k, N_k are vector spaces over a field. □

Exercise 2.8.4. Let $M_i, i \in I$ be any family of A-modules and M be their direct sum. Prove that M is flat $\Leftrightarrow$ each M_i is flat.

Proof. It suffices to show tensor commutes with direct sum, that is for any A-module B, we have

$$B \otimes \bigoplus M_i = \bigoplus (B \otimes M_i)$$

And it's clear from Proposition 2.14 of [AM69]. □

Exercise 2.8.5. Let $A[x]$ be the ring of polynomials in one indeterminate over a ring A. Prove that $A[x]$ is a flat A-algebra.

Proof. Note that $A[x] = \bigoplus_i M_i$, where $M_i = Ax^i$. Clearly $M_i \cong A$ as A-modules, and A is flat as an A-module. Thus by Exercise 2.8.4 we obtain $A[x]$ is flat. □

Exercise 2.8.6. For any A-module, let $M[x]$ denote the set of all polynomials in x with coefficients in M, that is to say expressions of the form

$$m_0 + m_1 x + \cdots + m_r x^r \quad m_i \in M$$

Defining the product of an element of $A[x]$ and an element of $M[x]$ in the obvious way, show that $M[x]$ is an $A[x]$-module. Show that $M[x] \cong A[x] \otimes_A M$.

Proof. Firstly, let's define the $A[x]$-module structure on $M[x]$: For $\sum a_i x^i \in A[x], \sum m_j x^j \in M[x]$, define $A[x]$ action as

$$(\sum a_i x^i)(\sum m_j x^j) = \sum c_k x^k, \quad c_k = \sum_{i+j=k} a_i m_j$$

It's a routine to check it do gives an $A[x]$-module structure, we omit here.

Consider the following map

$$\begin{aligned}\phi \colon M[x] &\to A[x] \otimes_A M \\ \sum m_i x^i &\mapsto \sum x^i \otimes m_i\end{aligned}$$

It's an $A[x]$-module homomorphism. Indeed, for $\sum a_i x^i \in A[x]$, we have

$$\begin{aligned}\phi(\sum a_i x^i \sum m_j x^j) &= \phi(\sum_{i+j=k} a_i m_j x^{i+j}) \\ &= \sum_k \sum_{i+j=k} x^{i+j} \otimes a_i m_j \\ &= \sum_{i,j} x^i x^j \otimes a_i m_j \\ &= \sum_j ((\sum_i a_i x^i) x^j \otimes m_j) \\ &= (\sum_i a^i x^i)(\sum_j x^j \otimes m_j) \\ &= (\sum_i a^i x^i)\phi(\sum_j m_j x^j)\end{aligned}$$

As desired. Conversely, consider $\widetilde{\psi}\colon A[x]\times M \to M[x]$ defined by $\widetilde{\psi}(\sum a_i x^i, m) = \sum a_i m x^i$. It induces a linear map $\psi\colon A[x]\otimes_A M \to M[x]$ by sending $(\sum a_i x^i)\otimes m$ to $\sum a_i m x^i$. Clearly ψ and ϕ are inverse. □

Remark 2.8.1. From this Exercise, hope you can get a feeling of a use of tensor product: a kind of changing domain of coefficients.

Exercise 2.8.7. Let $\mathfrak{p}$ be a prime ideal in A. Show that $\mathfrak{p}[x]$ is a prime ideal in $A[x]$. If $\mathfrak{m}$ is a maximal ideal in A, is $\mathfrak{m}[x]$ a maximal ideal in $A[x]$?

Proof. It suffices to check $A[x]/\mathfrak{p}[x]$ is a domain. Note that $A[x]/\mathfrak{p}[x] \cong (A/\mathfrak{p})[x]$. By Exercise 1.8.2, f is a zero-divisor in $(A/\mathfrak{p})[x]$ if and only if there exists $a \in A/\mathfrak{p}$ such that $af = 0$, but it's impossible since $A/\mathfrak{p}$ is a domain. However, $\mathfrak{m}[x]$ may not be a maximal ideal. For example, let $A = \mathbb{Q}$ and $\mathfrak{m} = (0)$, then clearly (0) is not maximal in $\mathbb{Q}[x]$. □

Exercise 2.8.8.

(1) If M and N are flat A-modules, then so is $M \otimes_A N$.
(2) If B is a flat A-algebra and N is a flat B-module, then N is flat as an A-module.

Proof. For (1). It suffices to check for any exact sequence $0 \to A_1 \to A_2$, we have

$$0 \to A_1 \otimes (M \otimes N) \to A_2 \otimes (M \otimes N)$$

is exact. Note that $A_i \otimes (M \otimes N) \cong (A_i \otimes M) \otimes N$, then it's equivalent to check the following sequence is exact

$$0 \to (A_1 \otimes M) \otimes N \to (A_2 \otimes M) \otimes N$$

It's clear to see this by tensoring M and N step by step and use the fact M, N are flat.

For (2). It suffices to check for any exact sequence $0 \to A_1 \to A_2$ of A-modules, we have

$$0 \to A_1 \otimes_A N \to A_2 \otimes_A N$$

is exact. Note that

$$A_i \otimes_A N \cong A_i \otimes_A (B \otimes_B N) \cong (A_i \otimes_A B) \otimes_B N$$

Use the same method of (1) to conclude. □

Exercise 2.8.9. Let $0 \to M' \xrightarrow{f} M \xrightarrow{g} M'' \to 0$ be an exact sequence of A-modules. If M' and M'' are finitely generated, then so is M.

Proof. There exist sets of generators $\{x_i\}_{i\in I}$ of M' and $\{\overline{y_j}\}_{j\in J}$ of M''. Consider the preimage of $\{\overline{y_j}\}_{j\in J}$ in M, denoted by $\{y_j\}_{j\in J}$. It's clear $\{f(x_i)\}_{i\in I}$ together with $\{y_j\}_{j\in J}$ generates M by the exactness of sequence. □

Exercise 2.8.10. Let A be a ring, $\mathfrak{a}$ an ideal contained in the Jacobson radical of A. let M be an A-module and N a finitely generated A-module, and let $u\colon M \to N$ be a homomorphism. If the induced homomorphism $M/\mathfrak{a}M \to N/\mathfrak{a}N$ is surjective, then u is surjective.

Proof. Consider the following composition

$$M \to M/\mathfrak{a}M \xrightarrow{u} N/\mathfrak{a}N$$

It's surjective, since it's a composition of two surjective mappings, which implies $u(M) + \mathfrak{a}N = N$. Note that N is finitely generated and $\mathfrak{a} \subseteq \mathfrak{R}$. Then Nakayama's lemma implies $\mu(M) = N$. □

Exercise 2.8.11. Let A be a ring $\neq 0$. Show that $A^m \cong A^n \Rightarrow m = n$. Furthermore,

(1) If $\phi\colon A^m \to A^n$ is surjective, then $m \geqslant n$.
(2) If $\phi\colon A^m \to A^n$ is injective, is it always the case that $m \leqslant n$?

Proof. Let $\mathfrak{m}$ be a maximal ideal of A and let $\phi\colon A^m \to A^n$ be an isomorphism. Then $1 \otimes \phi\colon (A/\mathfrak{m}) \otimes A^m \to (A/\mathfrak{m}) \otimes A^n$ is an isomorphism between vector spaces of dimensions m and n over the field $k = A/\mathfrak{m}$. Indeed, there is a surjective map $A^m \to A^n$ and surjective map $A^n \to A^m$, so there is a surjective map $(A/\mathfrak{m}) \otimes A^m \to (A/\mathfrak{m}) \otimes A^n$ and verse vice. Hence $m = n$. So it's natural to see (1) is also true.

This method fails for the case ϕ is injective, since tensor is just a right exact functor, but this statement is still true. □

Exercise 2.8.12. Let M be a finitely generated A-module and $\phi\colon M \to A^n$ a surjective homomorphism. Show that $\ker\phi$ is finitely generated.

Proof. Consider the following exact sequence

$$0 \to \ker\phi \to M \xrightarrow{\phi} A^n \to 0$$

Since A^n is a free A-module, so this exact sequence splits, which is equivalent to $\ker \phi$ is a direct summand of M. Then $\ker \phi$ is finitely generated, since M is. □

Exercise 2.8.13. Let $f\colon A \to B$ be a ring homomorphism, and let N be a B-module. Regarding N as an A-module by restriction of scalars, form the B-module $N_B = B \otimes_A N$. Show that the homomorphism $g\colon N \to N_B$ which maps y to $1 \otimes y$ is injective and that $g(N)$ is a direct summand of N_B.

Proof. Consider the following mapping

$$\begin{aligned} p : N_B &\to N \\ b \otimes y &\mapsto by \end{aligned}$$

Directly check $p \circ g$ as follows: Take $y \in N$, then

$$p \circ g(y) = p(1 \otimes y) = y$$

So we have $p \circ g$ is identity on N, which implies g is injective. Furthermore, this implies the following sequence splits

$$0 \to N \xrightarrow{g} N_B \to N_B / \operatorname{im} g \to 0$$

which is equivalent to $g(N)$ is a direct summand of N_B. □

Exercise 2.8.14 (direct limits)**.** A partially ordered set I is said to be a directed set if for each pair i, j in I there exists $k \in I$ such that $i \leqslant k$ and $j \leqslant k$.

Let A be a ring, let I be a directed set and let $(M_i)_{i \in I}$ be a family of A-modules indexed by I. For each pair i, j in I such that $i \leqslant j$, let $\mu_{ij} : M_i \to M_j$ be an A-homomorphism, and suppose that the following axioms are satisfied:

(1) μ_{ii} is the identity mapping of M_i for all $i \in I$.
(2) $\mu_{ik} = \mu_{jk} \circ \mu_{ij}$ whenever $i \leq j \leq k$.

Then the modules M_i and homomorphisms μ_{ij} are said to form a direct system $\mathbf{M} = (M_i, \mu_{ij})$ over the directed set I.

We shall construct an A-module M called the direct limit of the direct system $\mathbf{M}$. Let C be the direct sum of the M_i, and identify each module M_i with its canonical image in C. Let D be the submodule of C generated by all elements of the form $x_i - \mu_{ij}(x_i)$ where $i \leqslant j$ and $x_i \in M_i$. Let $M = C/D$, let $\mu\colon C \to M$ be the projection and let μ_i be the restriction of μ to M_i.

The module M, or more correctly the pair consisting of M and the family of homomorphisms $\mu_i : M_i \to M$, is called the direct limit of the direct system $\mathbf{M}$, and is written $\varinjlim M_i$. From the construction it is clear that $\mu_i = \mu_j \circ \mu_{ij}$ whenever $i \leqslant j$.

Proof. Let's check $\mu_i = \mu_j \circ \mu_{ij}$ on M_i: Note that for $x_i \in M_i$, we have $\mu_i(x_i) = x_i + D \in M = C/D$, since μ_i is just the restriction of natural projection on M_i.

Take $x_i \in M_i$, then $\mu_{ij}(x_i) \in M_j$, and note that $\mu_{ij}(x_i) + D \in M = C/D$ is equivalent to $x_i + D$, since $x_i - \mu_{ij}(x_i) \in D$. So we have

$$\mu_i(x_i) = x_i + D = \mu_{ij}(x_i) + D = \mu_j \circ \mu_{ij}(x_i)$$

As desired. □

Exercise 2.8.15. In the situation of Exercise 2.8.14, show that every element of M can be written in the form $\mu_i(x_i)$ for some $i \in I$ and some $x_i \in M_i$. Show also that if $\mu_i(x_i) = 0$ then there exists $j \geq i$ such that $\mu_{ij}(x_i) = 0$ in M_j.

Proof. For the first part: Take an arbitrary element $x \in M = C/D$, then write it as

$$x = \sum_{j=1}^{n} \mu_j(x_j), \quad x_j \in M_j$$

It suffices to check the case for $n = 2$: There exists $k \in I$ such that $k \geq 1, k \geq 2$ since I is a directed set. Then

$$\mu_1(x_1) + \mu_2(x_2) = \mu_k \circ \mu_{1k}(x_1) + \mu_k \circ \mu_{2k}(x_2)$$

since $\mu_i = \mu_k \circ \mu_{ik}$ for $i \leq k$ in M. Then this element can be written as $\mu_k(\mu_{1k}(x_1) + \mu_{2k}(x_2))$ as desired.

For the half part, by definition we have $\mu_i(x_i) = 0 \in M$ if and only if $\mu_i(x_i) \in D$, that is in C we have

$$x_i = \sum_{k=1}^{n} (x_{i_k} - \mu_{i_k j_k}(x_{i_k}))$$

For this equation, we can make the following assumptions:

(1) $x_{i_k} \neq 0$ for each k.
(2) $i_k \neq j_k$ for each k.
(3) $i_k \neq i_{k'}$ for $k \neq k'$, otherwise we can add them together.
(4) i is the minimal element in $\{i_k\}_{k=1}^n$. Indeed, let i_l to be the minimal element in $\{i_k\}_{k=1}^n$. Note $x_i \in M_i$, thus terms appearing in $M_j, i \neq j$ in $\sum_{k=1}^n (x_{i_k} - \mu_{i_k j_k}(x_{i_k}))$ must be zero, but x_{i_l} is the only term appearing in M_{i_l}, since i_l is minimal. Thus we must have $x_{i_l} = x_i$, that's $i = i_l$.
(5) Furthermore, we can assume all $i_k = i$. Indeed. Consider the minimal element of the set $\{i_k\} \setminus \{i\}$, and denote it by i_l. Note that i_l coordinate vanishes, so either $x_{i_l} = 0$ or $x_{i_l} = \mu_{i i_l}(x_i)$, since $i \leq i_l$ is the only one less than i_l. In later case, we may write the following

$$x_{i_l} - \mu_{i_l j_l}(x_{i_l}) = \mu_{i i_l}(x_i) - \mu_{i j_l}(x_i) = (x_i - \mu_{i j_l}(x_i)) - (x_i - \mu_{i i_l}(x_i))$$

Repeat finite many times to conclude.

Now we have

$$x_i = \sum_{k=1}^{n} \pm (x_i - \mu_{i j_k}(x_i))$$

Since each j_k appear only once and j_k components must vanish, then we must have $\mu_{ij_k}(x_i) = 0$ for each k in the sum. In particular we have the signature of this equation is 1, in other words, the number of "+" minus the number of "−" is 1. Now take j to be any j_k, then

$$\mu_{ij}(x_i) = \mu_{ij_k}(x_i) = 0$$

This completes the proof. □

Exercise 2.8.16 (universal property)**.** Show that the direct limit is characterized (up to isomorphism) by the following property. Let N be an A-module and for each $i \in I$ let $\alpha_i : M_i \to N$ be an A-module homomorphism such that $\alpha_i = \alpha_j \circ \mu_{ij}$ whenever $i \leqslant j$. Then there exists a unique homomorphism $\alpha\colon M \to N$ such that $\alpha_i = \alpha \circ \mu_i$ for all $i \in I$.

Proof. Existence: Note that by universal property of direct sum, there exists a morphism $\phi\colon \bigoplus_i M_i \to N$, such that $\alpha_i = \phi \circ \tau_i$, where $\tau_i : M_i \to \bigoplus_i M_i$ is canonical inclusion. Furthermore, take any element $x_i - \mu_{ij}(x_i) \in D$, then

$$\phi(x_i - \mu_{ij}(x_i)) = \alpha_i(x_i) - \alpha_j \circ \mu_{ij}(x_i) = 0$$

Thus $D \subseteq \ker \phi$, that is we obtain a morphism $\alpha\colon M \to N$ induced by ϕ, and it's clear $\alpha_i = \alpha \circ \mu_i$. What we have done can be shown as follows:

$$\begin{tikzcd}
M_i \arrow[d] \arrow[dr, "\alpha_i"] \arrow[dd, bend right=60, "\mu_i"'] & \\
\bigoplus_i M_i \arrow[r, "\phi"] \arrow[d] & N \\
M \arrow[ur, "\alpha"] &
\end{tikzcd}$$

Uniqueness: If $\beta : M \to N$ is another morphism such that $\alpha_i = \beta \circ \mu_i$ for all $i \in I$. From Exercise 2.8.15 we know each element can be written as $\mu_i(x_i)$ for $x_i \in M_i$. So it suffices to check $\alpha(\mu_i(x_i)) = \beta(\mu_i(x_i))$. Indeed,

$$\alpha(\mu_i(x_i)) = \alpha_i(x_i) = \beta(\mu_i(x_i))$$

□

Exercise 2.8.17. Let $(M_i)_{i \in I}$ be a family of submodules of an A-module, such that for each pair of indices i, j in I there exists $k \in I$ such that $M_i + M_j \subseteq M_k$. Define $i \leqslant j$ to mean $M_i \subseteq M_j$ and let $\mu_{ij} : M_i \to M_j$ be the embedding of M_i in M_j. Show that

$$\varinjlim M_i = \sum M_i = \bigcup M_i.$$

In particular, any A-module is the direct limit of its finitely generated submodules.

Proof. From Exercise 2.8.15, we know that every element of direct limit can be written as $\mu_i(x_i)$ for some $x_i \in M_i$. Then we can write it as

$$x_i + \sum_{k=1}^{n} (x_{i_k} - \mu_{i_k j_k}(x_{i_k})) \in \bigoplus_{i \in I} M_i$$

Note that for each k, we have $x_{i_k} + \mu_{i_k j_k}(x_{i_k}) \in M_{i_k} + M_{j_k} \subseteq M_{l_k}$ for some l_k. After finite times steps, we can show that

$$x_i + \sum_{k=1}^{n} (x_{i_k} - \mu_{i_k j_k}(x_{i_k})) \in M_N$$

for some sufficiently large $N \in I$. Thus $\varinjlim M_i = \bigcup M_i$. In particular, let $\{M_i\}$ be the family of finitely generated submodules of a A-module M, then

$$\varinjlim M_i = \bigcup_i M_i = M$$

since $\bigcup_{x \in M} Ax$ already covers M. □

Exercise 2.8.18. Let $\mathbf{M} = (M_i, \mu_{ij}), \mathbf{N} = (N_i, v_{ij})$ be direct systems of A-modules over the same directed set. Let M, N be the direct limits and $\mu_i : M_i \to M, \nu_i : N_i \to N$ the associated homomorphisms.

A homomorphism $\phi \colon \mathbf{M} \to \mathbf{N}$ is by definition a family of A-module homomorphisms $\phi_i : M_i \to N_i$ such that $\phi_j \circ \mu_{ij} = v_{ij} \circ \phi_i$ whenever $i \leqslant j$. Show that ϕ defines a unique homomorphism $\phi = \varinjlim \phi_i : M \to N$ such that $\phi \circ \mu_i = v_i \circ \phi_i$ for all $i \in I$.

Proof. Consider the following commutative diagram

$$\begin{tikzcd}
& M_i \arrow[dl, "\mu_{ij}"'] \arrow[d, "\phi_i"] \arrow[dr] & \\
M_j \arrow[d, "\phi_j"] & N_i \arrow[dl, "\nu_{ij}"] \arrow[dr, "\nu_i"] & M \arrow[d, dashed, "\phi"] \\
N_j \arrow[rr, "\nu_j"] & & N
\end{tikzcd}$$

Note that $\nu_i \circ \phi_i = \nu_j \circ \phi_j \circ \mu_{ij}$. Thus there is a unique homomorphism ϕ by Exercise 2.8.16, the universal property of direct limit. □

Exercise 2.8.19. A sequence of direct systems and homomorphisms

$$\mathbf{M} \to \mathbf{N} \to \mathbf{P}$$

is exact if the corresponding sequence of modules and module homomorphisms is exact for each $i \in I$. Show that the sequence $M \xrightarrow{f} N \xrightarrow{g} P$ of direct limits is then exact[4].

[4] In other words, direct limit of a direct system of modules over a directed set is an exact functor.

Proof. To be explicit, let $(M_i, \mu_{ij}), (N_i, \nu_{ij}), (P_i, \omega_{ij})$ be direct systems over the same directed set I. A sequence of direct systems is exact

$$\mathbf{M} \xrightarrow{f} \mathbf{N} \xrightarrow{g} \mathbf{P}$$

if and only if for any $i \in I$ we have

$$M_i \xrightarrow{f_i} N_i \xrightarrow{g_i} P_i$$

is exact.

Firstly, $f \circ g$ is clearly zero, since take any element $x \in M$ it must be written as $\mu_i(x_i)$ for $x_i \in M_i$ by Exercise 2.8.15. It suffices to check $g \circ f \circ \mu_i(x_i) = 0$. Indeed,

$$g \circ f \circ \mu_i(x_i) = g \circ \nu_i \circ f_i(x_i) = \omega_i \circ g_i \circ f_i(x_i) = 0$$

That's $\operatorname{im} f \subseteq \ker g$. Conversely, take $x \in \ker g \subset N$, by Exercise 2.8.15 we write it as $\nu_i(x_i)$ for some $x_i \in N_i$. But $g \circ \nu_i(x_i) = \omega_i \circ g_i(x_i) = 0$ implies there exists $j \geq i$ such that $\omega_{ij}(g_i(x_i)) = g_j(\nu_{ij}(x_i)) = 0$, that is $\nu_{ij}(x_i) = f_j(y_j)$ for some $y_j \in M_j$. Consider $\mu_j(y_j)$, we have

$$f \circ \mu_j(y_j) = \nu_j \circ f_j(y_j) = \nu_j \circ \nu_{ij}(x_i) = \nu_i(x_i) = x$$

That's $x \in \operatorname{im} f$. This completes the proof. $\square$

Exercise 2.8.20 (tensor products commute with direct limits)**.** Keeping the same notation as before, let N be any A-module. Then $(M_i \otimes N, \mu_{ij} \otimes 1)$ is a direct system. let $P = \varinjlim(M_i \otimes N)$ be its direct limit.

For each $i \in I$ we have a homomorphism $\mu_i \otimes 1\colon M_i \otimes N \to M \otimes N$, hence by Exercise 2.8.16 a homomorphism $\psi\colon P \to M \otimes N$. Show that ψ is an isomorphism, so that

$$\varinjlim(M_i \otimes N) \cong (\varinjlim M_i) \otimes N$$

Proof. For each $i \in I$, consider two direct system $(M_i \times N, \mu_{ij} \times 1), (M_i \otimes N, \mu_{ij} \otimes 1)$. Claim $\mu_i \times 1\colon M_i \times N \to M \times N$ is the direct limit of the first direct system. Indeed, if $\alpha_i\colon M_i \times N \to L$ is the direct limit of direct system $(M_i \times N, \mu_{ij} \times 1)$, then there exists a mapping $\alpha\colon L \to M \times N$ such that $\mu_i \times 1 = \alpha \circ \alpha_i$. Note that we already have α is surjective, and $\mu_i \times 1$ is injective implies α is injective, thus $\mu_i \times 1\colon M_i \times N \to M \times N$ is direct limit. We use $\nu_i\colon M_i \otimes N \to P$ to denote the second direct limit.

A homomorphism between direct system $g_i\colon M_i \times N \to M_i \otimes N$, that's the canonical bilinear mapping. Passing to the limit we obtain a mapping $g\colon M \times N \to P$. Clearly g is A-bilinear, since each g_i is a A-bilinear one. Hence define a homomorphism $\phi\colon M \otimes N \to P$. Let's that $\phi \circ \psi$ and $\psi \circ \phi$ are identity mappings directly.

Take $m \otimes n \in M \otimes N$, and write $m = \mu_i(m_i), m_i \in M_i$, then

$$\begin{aligned}\psi \circ \phi(\mu_i(m_i) \otimes n) &= \psi \circ g(\mu_i(m_i), n) \\ &= \psi \circ \nu_i \circ g_i(m_i, n) \\ &= \psi \circ \nu_i(m_i \otimes n) \\ &= \mu_i \otimes 1(m_i \otimes n) \\ &= \mu_i(m_i) \otimes n\end{aligned}$$

Take $x \in P$, and write $x = \nu_i(m_i \otimes n)$ for some $m_i \otimes n \in M_i \otimes N$, then

$$\begin{aligned}\phi \circ \psi(\nu_i(m_i \otimes n)) &= \phi \circ \mu_i \otimes 1(m_i \otimes n) \\ &= \phi(\mu_i(m_i) \otimes 1) \\ &= g(\mu_i(m_i), n) \\ &= \nu_i \circ g_i(m_i, n) \\ &= \nu_i(m_i \otimes n)\end{aligned}$$

This completes the check. □

Exercise 2.8.21. Let $(A_i)_{i \in I}$ be a family of rings indexed by a directed set I, and for each pair $i \leqslant j$ in I let $\alpha_{ij} : A_i \to A_j$ be a ring homomorphism, satisfying conditions (1) and (2) of Exercise 2.8.14. Regarding each A_i as a $\mathbf{Z}$-module we can then form the direct limit $A = \varinjlim A_i$. Show that A inherits a ring structure from the A_i so that the mappings $\alpha_i : A_i \to A$ are ring homomorphisms. The ring A is the direct limit of the system (A_i, α_{ij}).

If $A = 0$ prove that $A_i = 0$ for some $i \in I$.

Proof. From Exercise 2.8.15, we know that if $\alpha_i(a_i) = 0$ then there exists $j \geq i$ such that $\alpha_{ij}(a_i) = 0 \in A_j$. But here $A = 0$, thus for any $a_i \in A_i$ we have $\alpha_i(a_i) = 0$. In particular we take $a_i = e_i$, the identity element in A_i, then there exists $j \geq i$ such that $\alpha_{ij}(e_i) = 0$, but α_{ij} is a ring homomorphism, thus $e_i = 0$. This completes the proof. □

Exercise 2.8.22. Let (A_i, α_{ij}) be a direct system of rings and let $\mathfrak{R}_i$ be the nilradical of A_i. Show that $\varinjlim \mathfrak{R}_i$ is the nilradical of $\varinjlim A_i$. If each A_i is an integral domain, then $\varinjlim A_i$ is an integral domain.

Proof. It's clear that $\varinjlim \mathfrak{R}_i \subseteq \mathfrak{R}(\varinjlim A_i)$. Conversely, take $x \in \varinjlim A_i$ and write it as $\alpha_i(a_i)$ for some $a_i \in A_i$. Then x is in nilradical of $\varinjlim A_i$ if and only if it's nilpotent, that is

$$(\alpha_i(a_i))^n = \alpha_i(a_i^n) = 0$$

But this implies there exists $j \geq i$ such that $\alpha_{ij}(a_i^n) = 0$, that is $\alpha_{ij}(a_i)^n = 0$, so we have $\alpha_{ij}(a_i) \in \mathfrak{R}_j$. Thus $\alpha_i(a_i) = \alpha_j(\alpha_{ij}(a_i)) \in \varinjlim \mathfrak{R}_i$. □

Exercise 2.8.23. Let $(B_\lambda)_{\lambda \in \Lambda}$ be a family of A-algebras. For each finite subset J of Λ let B_J denote the tensor product (over A) of the B_λ for $\lambda \in J$. If J' is another finite subset of Λ and $J \subseteq J'$, there is a canonical A-algebra homomorphism $B_J \to B_{J'}$. Let B denote the direct limit of the rings B_J as J runs through all finite subsets of Λ. The ring B has a natural A-algebra structure for which the homomorphisms $i_J : B_J \to B$ are A-algebra homomorphisms. The A-algebra B is the tensor product of the family $(B_\lambda)_{\lambda\in\Lambda}$.

Proof. Let's give an A-algebra structure on B, it suffices to give an A-action on B, since there is already a ring on B. Take any element $x \in B$ and write it as $i_J((\otimes b_\lambda)_{\lambda\in J})$ for some index set J. For $a \in A$, let a act on it as follows

$$a i_J((\otimes b_\lambda)_{\lambda\in J}) = i_J(a(\otimes b_\lambda)_{\lambda\in J})$$

a can act on $(\otimes b_\lambda)_{\lambda\in J}$ since B_J is an A-algebra. Now it suffices to check this is well-defined, since it's clear $i_J : B_J \to B$ is an A-algebra homomorphism by our definition. Take another representation $i_{J'}((\otimes b'_\lambda)_{\lambda\in J'})$, assume $J \subseteq J'$, then we must have

$$x = i_{J'}((\otimes b'_\lambda)_{\lambda\in J'}) = i_{J'} \circ i_{JJ'}((\otimes b_\lambda)_{\lambda\in J}) = i_J((\otimes b_\lambda)_{\lambda\in J})$$

Then

$$\begin{aligned} ax &= i_J(a(\otimes b_\lambda)_{\lambda\in J}) \\ &= i_{J'} \circ i_{JJ'}(a(\otimes b_\lambda)_{\lambda\in J}) \\ &= i_{J'}(a(\otimes b')_{\lambda\in J'}) \end{aligned}$$

□

Exercise 2.8.24 (flatness and Tor functor)**.** If M is an A-module, the following statements are equivalent.

(1) M is flat.
(2) $\mathrm{Tor}_n^A(M,N) = 0$ for all $n > 0$ and all A-modules N.
(3) $\mathrm{Tor}_1^A(M,N) = 0$ for all A-modules N.

Proof. For (1) to (2). Take a free resolution of N as follows

$$\cdots \to F_2 \to F_1 \to F_0 \to N \to 0$$

and tensor it with M to obtain

$$\cdots \to M \otimes F_2 \to M \otimes F_1 \to M \otimes F_0 \to M \otimes N \to 0$$

Since M is flat, the resulting sequence is exact and therefore its homology groups, which are the $\mathrm{Tor}_n^A(M,N)$, are zero for $n > 0$.

(2) to (3) is clear. For (3) to (1). Let $0 \to N' \to N \to N'' \to 0$ be an exact sequence. Then this short exact sequence induces a long exact sequence

$$\cdots \to \mathrm{Tor}_1^A\left(M, N''\right) \to M \otimes N' \to M \otimes N \to M \otimes N'' \to 0$$

Since $\mathrm{Tor}_1^A(M,N'') = 0$ it follows that M is flat. □

Exercise 2.8.25. Let $0 \to N' \to N \to N'' \to 0$ be an exact sequence, with N'' flat. Then N' is flat $\Leftrightarrow$ N is flat.

Proof. Take an arbitrary A-module M and consider the long exact sequence induced by this short exact sequence

$$\cdots \to \operatorname{Tor}_1^A(N', M) \to \operatorname{Tor}_1^A(N, M) \to \operatorname{Tor}_1^A(N'', M) \to \dots$$

From Exercise 2.8.24 we have N' or N is flat if and only if $\operatorname{Tor}_1^A(N', M)$ or $\operatorname{Tor}_1^A(N, M)$ is zero. It's clear since $\operatorname{Tor}_1^A(N'', M) = 0$. □

Exercise 2.8.26. Let N be an A-module. Then N is flat if and only if $\operatorname{Tor}_1^A(A/\mathfrak{a}, N) = 0$ for all finitely generated ideal $\mathfrak{a}$ in A.

Proof. By Proposition 2.5.1, we have N is flat if and only if for any exact sequence $0 \to M' \to M$ where M, M' are finitely generated, we have

$$0 \to M' \otimes N \to M \otimes N$$

is exact. But we always have the following exact sequence

$$\operatorname{Tor}_1^A(M/M', N) \to M' \otimes N \to M \otimes N$$

It's clear M/M' is finitely generated. Thus N is flat if $\operatorname{Tor}_1^A(M, N) = 0$ for all finitely generated A-modules M.

If M is finitely generated, let $x_1, \dots, x_n$ be a set of generators of M, and let M_i be the submodule generated by $x_1, \dots, x_i$. By considering the successive quotients $M_{\mathrm{i}}/M_{\mathrm{i}-1}$ and the following exact sequence

$$0 \to M_{i-1} \to M_i \to M_i/M_{i-1} \to 0$$

If $\operatorname{Tor}_1(M, N) = 0$ for all cyclic A-modules M[5]. So by Exercise 2.8.25 we have M_2 is flat, since M_1 and M_2/M_1 are cyclic. By induction on i we can show $M_n = M$ is also flat, that's $\operatorname{Tor}_1^A(M, N) = 0$. We can show $\operatorname{Tor}_1^A(M, N) = 0$ for all finitely generated A-modules M by this method. Thus N is flat if $\operatorname{Tor}_1(M, N) = 0$ for all cyclic A-modules.

Note that for any cyclic A-module M, there is a natural exact sequence $A \to M \to 0$, defined by $a \mapsto ax$. Thus $M \cong A/\mathfrak{a}$ for some ideal $\mathfrak{a}$. That is, N is flat if $\operatorname{Tor}_1^A(A/\mathfrak{a}, N) = 0$ for all ideals $\mathfrak{a}$, and that's equivalent to

$$0 \to \mathfrak{a} \otimes N \to A \otimes N$$

is exact. Again by Proposition 2.5.1 this will hold if

$$0 \to \mathfrak{a} \otimes N \to A \otimes N$$

is exact for all finitely generated ideal $\mathfrak{a}$, and that's equivalent to $\operatorname{Tor}_1^A(A/\mathfrak{a}, N) = 0$ for all finitely generated ideal $\mathfrak{a}$. □

Exercise 2.8.27. A ring A is absolutely flat if every A-module is flat. Prove that the following statements are equivalent.

(1) A is absolutely flat.
(2) Every principal ideal is idempotent.
(3) Every finitely generated ideal is a direct summand of A.

[5] M is a cyclic A-module if $M = Ax$ for some $x \in M$.

Proof. For (1) to (2). Let $x \in A$, then $A/(x)$ is a flat A-module, hence in the diagram

$$\begin{array}{ccc} (x) \otimes A & \xrightarrow{\beta} & (x) \otimes A/(x) \\ \downarrow & & \downarrow{\scriptstyle \alpha} \\ A & \longrightarrow & A/(x) \end{array}$$

the mapping α is injective. Hence $\operatorname{im}(\beta) = 0$, since from the commutativity of the diagram we have $\alpha \circ \beta = 0$. But $\beta = 1 \otimes \pi$, where $\pi \colon A \to A/(x)$ is surjective, thus β is also surjective. Thus $(x) \otimes A/(x) = 0$. Consider the following exact sequence

$$0 \to (x) \to A \to A/(x) \to 0$$

and tensor it with (x) we have the following exact sequence

$$0 \to (x) \otimes (x) \to A \otimes (x) \to 0$$

But $A \otimes (x) = (x)$ and $(x) \otimes (x) \cong (x^2)$. Hence $(x) = \left(x^2\right)$.

For (2) to (3). Since every principal ideal is idempotent, for $x \in A$, consider principal ideal (x) one has $(x) = (x^2)$, then $x = ax^2$ for some $a \in A$, hence $e = ax$ is idempotent and we have $(e) = (x)$. In other words, any principal ideal is generated by an idempotent element. More generally, for any finitely generated ideal $\mathfrak{a} = (x_1, \ldots, x_n)$, it's generated by $(e_1, \ldots, e_n)$, where e_i is an idempotent. As we can see from the proof of (3) of Exercise 1.8.11, an ideal generated by finite idempotent is principal. In particular, we can assume it's generated by an idempotent element e. Thus $\mathfrak{a} = (e)$, it's clear a summand of A since $A = (e) \oplus (1 - e)$.

For (3) to (1). Take an arbitrary A-module N, from Exercise 2.8.26 it suffices to check $\operatorname{Tor}_1^A(A/\mathfrak{a}, N) = 0$ for all finitely generated ideal $\mathfrak{a}$ in A. Consider the following exact sequence

$$0 \to \mathfrak{a} \to A \to A/\mathfrak{a} \to 0$$

Since $\mathfrak{a}$ is a summand of A, then this exact sequence splits. Moreover a split exact sequence is also exact after tensoring something, which implies $\operatorname{Tor}_1^A(A/\mathfrak{a}, N) = 0$. □

Exercise 2.8.28. We have following statements for absolutely flat rings:

(1) A Boolean ring is absolutely flat.
(2) Let A be a ring in which every element x satisfies $x^n = x$ for some $n > 1$ (depending x), then A is absolutely flat.
(3) Every homomorphism image of an absolutely flat ring is absolutely flat.
(4) If a local ring is absolutely flat, then it is a field.
(5) If A is absolutely flat, every non-unit in A is a zero-divisor.

Proof. For (1) and (2). Consider $x \in A$ and the principal ideal (x) generated by it. Then $x(x^{n-1} - 1) = 0$ implies $A = (x) \oplus (x^{n-1} - 1)$. From Exercise 2.8.27 we have A is absolutely flat.

For (3). Consider the surjective mappings $f\colon A \to B$ such that A is absolutely flat. Take $x \in B$, and consider one of its preimage y, i.e. $f(y) = x$. Since A is absolutely flat, then there exists $a \in A$ such that $y = ay^2$, that is $x = ax^2$. So $(x) = (x^2)$ implies B is absolutely flat.

For (4). Let $(A, \mathfrak{m})$ be a local ring such that it's absolutely flat. To show A is a field, it suffices to show $\mathfrak{m} = 0$ Take $x \neq 0 \in \mathfrak{m}$, then $(x) = (x^2)$ implies there exists $a \in A$ such that $x = ax^2$, that is $x(1 - ax) = 0$. But $x \in \mathfrak{m} = \mathfrak{R}$, that $1 - ax$ is a unit, thus $x = 0$.

For (5). If A is absolutely flat and take $x \in A$ to be a non-unit. Since $(x) = (x^2)$ we have $x = ax^2$ such that $ax \neq 1$, that is $x(1 - ax) = 0$, x is a zero-divisor. $\square$

3. Localization

3.1. **Basic definitions.** The procedure by which one construct rational number $\mathbb{Q}$ from $\mathbb{Z}$ extends easily to any integral domain A and we obtain its field of fractions. The construction consists in taking all ordered pairs (a, s) where $a, s \in A$ and $s \neq 0$, and setting up an equivalence relations between such pairs:

$$(a, s) \sim (b, t) \iff at - bs = 0$$

In fact, fraction is a method to make all elements in $A \setminus \{0\}$ to be unit, that is you can find a inverse of it, and it's the most economic way to do this. More generally, we can do the same thing for any multiplicative closed subset.

Definition 3.1.1 (multiplicative closed subset)**.** Let A be a ring. A multiplicative closed subset of A is a subset S of A such that

(1) $1 \in S$.
(2) $xy \in S$ for any $x, y \in S$.

Definition 3.1.2 (localization)**.** Let $f\colon A \to B$ be a ring homomorphism, and $S \subset A$ a multiplicative closed subset. B is called the localization of A with respect to S, if

(1) $f(x)$ is unit for all $x \in S$.
(2) If $g\colon A \to C$ is a ring homomorphism such that $g(x)$ is a unit for all $x \in S$, then there exists a unique homomorphism $h : B \to C$ such that $g = h \circ f$.

Remark 3.1.1. The universal property explains what does "the most economic" mean: If there is another homomorphism such that all elements in S is unit, then this homomorphism must factor through this localization.

Now let's give an explicit construction of localization, which is quite similar to what we have done in fraction. Define a relation $\sim$ on $A \times S$ as follows

$$(a, s) \sim (b, t) \iff (at - bs)u = 0, \quad \text{for some } u \in S$$

It's an equivalence relation. Indeed, it's clear reflexive and symmetric. To see it's transitive. Suppose $(a, s) \sim (b, t), (b, t) \sim (c, u)$, then there exists $v, w \in S$ such that

$$(at - bs)v = 0$$
$$(bu - ct)w = 0$$

Now let's eliminate b from these two equations as follows: multiply uw on sides of first equation and sv on sides of second equation, we obtain

$$atvuw = ctwsv \implies (au - cs)tvw = 0$$

Note that $t, v, w \in S$ and S is multiplicative closed, thus $(a, s) \sim (c, u)$. Use a/s to denote the equivalence class of (a, s), and let $S^{-1}A$ denote the set of equivalence classes.

Now let's give a ring structure as follows

$$(a/s) + (b/t) = (at + bs)/st$$
$$(a/s)(b/t) = ab/st$$

Remark 3.1.2. It's a routine to verify that these definitions are independent of the choices of representatives (a, s) and (b, t), and $S^{-1}A$ is a commutative ring with identity. Here we omit it, since it's tooooo boring and meaningless.

There is a natural homomorphism $f\colon A \to S^{-1}A$, defined by $a \mapsto a/1$. Then let's show $S^{-1}A$ satisfies (1) and (2) in Definition 3.1.2.

(1) For any $s \in S$, we have $f(s) = s/1$ with inverse $1/s$, since $(s/1)(1/s) = s/s \sim 1/1$.
(2) For any $g\colon A \to C$ such that $g(x)$ is unit for all $x \in S$, we define $h(a/s) = g(a)g(s)^{-1}$.
   (a) It's well-defined. Indeed, if $a/s = b/t$, then there exists $u \in S$ such that $(at-bs)u = 0$, then $g((at-bs)u) = g(at-bs)g(u) = 0$, but $g(u)$ is a unit, thus $g(a)g(t) = g(b)g(s)$, that is $g(a)g(s)^{-1} = g(b)g^{-1}(t)$.
   (b) It's unique, since $h \circ f = g$, then $h(a/1) = h \circ f(a) = g(a)$ for all $a \in A$. hence if $s \in S$ we have $h(1/s) = h(s/1)^{-1} = g(s)^{-1}$, therefore $h(a/s) = h(a/1)h(1/s) = g(a)g(s)^{-1}$, which implies h is uniquely determined by g.

Remark 3.1.3. It's natural to ask $f\colon A \to S^{-1}A$, is it injective? Since it's clear we have $\mathbb{Z} \hookrightarrow \mathbb{Q}$. Unfortunately, this fails in general, since

$$\ker f = \{a \in A \mid sa = 0 \text{ for some } s \in S\}$$

So if there exists a zero-divisor in S, f fails to be injective.

3.2. **Localization and local ring.** A local ring $(A, \mathfrak{m})$ is a ring with only one maximal ideal $\mathfrak{m}$, so it's natural to ask the relation between local ring and localization. In order to answer this question, we need to study what will happen to ideals after localization.

Recall extension of an ideal: Given an ideal $\mathfrak{a}$ of a ring A, and a homomorphism $f\colon A \to B$, the extension of $\mathfrak{a}$ is $A\mathfrak{a}$, that is the set of all summations $\sum y_i f(x_i)$ where $x_i \in \mathfrak{a}$ and $y_i \in B$. In particular, we use $S^{-1}\mathfrak{a}$ to denote the extended ideal obtained from $\mathfrak{a}$ by localization with respect to S, that is, for any $y \in S^{-1}\mathfrak{a}$, y is of form $\sum a_i/s_i$, where $a_i \in \mathfrak{a}, s_i \in S$.

Theorem 3.2.1. Let A be a ring and $S^{-1}A$ is its localization with respect to some multiplicative closed subset S, then

(1) Every ideal in $S^{-1}A$ is an extended ideal.
(2) If $\mathfrak{a}$ is an ideal in A, then $\mathfrak{a}^{ec} = \bigcup_{s\in S}(\mathfrak{a} : s)$. Hence $\mathfrak{a}^e = (1)$ if and only if $\mathfrak{a}$ meets S.
(3) An ideal $\mathfrak{a}$ of A is a contracted ideal if and only if no element of S is a zero-divisor in $A/\mathfrak{a}$.
(4) The prime ideals of $S^{-1}A$ are in one to one correspondence ($\mathfrak{p} \leftrightarrow S^{-1}\mathfrak{p}$) with prime ideals of A which don't meet S.

Proof. For (1). Let $\mathfrak{b}$ be an ideal in $S^{-1}A$, and let $x/s \in \mathfrak{b}$. Then one has $x/1 \in \mathfrak{b}$ and thus $x \in \mathfrak{b}^c$. As a consequence one has $x/s \in \mathfrak{b}^{ce}$, that is, $\mathfrak{b} \subseteq \mathfrak{b}^{ce}$. Thus we have $\mathfrak{b} = \mathfrak{b}^{ce}$, since $\mathfrak{b}^{ce} \subseteq \mathfrak{b}$ automatically holds.

For (2). $x \in \mathfrak{a}^{ec}$ if and only if $x = f^{-1}(a/s)$ for some $a \in \mathfrak{a}, s \in S$, and that's equivalent to $x/1 = a/s$. By definition we have this is equivalent to $(xs - a)t = 0$ for some $t \in S$, and that's equivalent to $xst \in \mathfrak{a}$, i.e. $x \in \bigcup_{s\in S}(\mathfrak{a} : s)$. It's clear to see if $\mathfrak{a}$ meets S then $\mathfrak{a}^e = (1)$. Conversely, if $\mathfrak{a}^e = (1)$, then

$$\mathfrak{a}^{ec} = (1) = \bigcup_{s\in S}(\mathfrak{a} : s)$$

which implies there exists $s \in S$ such that $s \cdot 1 = s \in \mathfrak{a}$, that is $\mathfrak{a}$ meets S.

For (3). $\mathfrak{a}$ is a contracted ideal if and only if $\mathfrak{a}^{ec} = \mathfrak{a}$. Indeed, if $\mathfrak{a} = \mathfrak{b}^c$, then

$$\mathfrak{a}^{ec} = \mathfrak{b}^{cec} = \mathfrak{b}^c = \mathfrak{a}$$

But (2) gives us a description for $\mathfrak{a}^{ec}$, so this is equivalent to $sx \in \mathfrak{a}$ for some $s \in S$ implies $x \in \mathfrak{a}$, and that's equivalent to there is no $s \in S$ such that it's a zero-divisor in $A/\mathfrak{a}$.

For (4). If $\mathfrak{q}$ is a prime ideal in $S^{-1}A$, then $\mathfrak{p} = \mathfrak{q}^c$ is a prime ideal in A. Furthermore $\mathfrak{p} \cap S = \varnothing$, since $\mathfrak{q}$ doesn't contain unit of $S^{-1}A$. Conversely, if $\mathfrak{p}$ is a prime ideal in A such that $\mathfrak{p} \cap S = \varnothing$. Then

$$\frac{a}{s}\frac{b}{t} \in S^{-1}\mathfrak{p} \implies \text{there exists } r \in S \text{ such that } rab \in \mathfrak{p}$$

But $r \notin \mathfrak{p}$, so either a or b in $\mathfrak{p}$, implies either a/t or b/s is in $S^{-1}\mathfrak{p}$. Thus $S^{-1}\mathfrak{p}$ is prime. □

Now let's see an important example in algebraic geometry and explain the relation between localization and local ring.

Example 3.2.1. Let $\mathfrak{p}$ be a prime ideal of A. Then $S = A - \mathfrak{p}$ is multiplicative closed. We write $A_{\mathfrak{p}}$ for $S^{-1}A$ in this case.

For ring $A_{\mathfrak{p}}$, we claim it's a local ring, with maximal ideal $S^{-1}\mathfrak{p} = \mathfrak{p}A_{\mathfrak{p}}$, and denote it by $\mathfrak{p}A_{\mathfrak{p}}$. Indeed, take any arbitrary element $a/s \in A_{\mathfrak{p}} - \mathfrak{p}A_{\mathfrak{p}}$, then we have $a, s \in A - \mathfrak{p}$, so it must be invertible, since its inverse is $s/a \in A_{\mathfrak{p}}$. So any element not in $\mathfrak{p}A_{\mathfrak{p}}$ is a unit, and by (1) of Proposition 1.4.3, then $\mathfrak{p}A_{\mathfrak{p}}$ is the only maximal ideal of A_{p}. So localization with respect to the complement of a prime ideal, we will obtain a local ring.

From (4) of Theorem 3.2.1, we can have a better understanding of ideals in this local ring $A_{\mathfrak{p}}$: Any prime ideal $\mathfrak{q} \in A_{\mathfrak{p}}$ has a one to one correspondence to prime ideals in A which do not intersect with $A - \mathfrak{p}$, or in other words, prime ideals which is contained in $\mathfrak{p}$.

Remark 3.2.1. In algebraic geometry, we regard a prime ideal as a point. You can imagine localization at this prime ideal $\mathfrak{p}$ geometrically is to consider the local property of this point, that is only to consider prime ideals contained in $\mathfrak{p}$.

Another important example is localization at an element.

Example 3.2.2. Let $f \in A$ be an element which is not nilpotent. Consider multiplicative closed subset $S = \{1, f, f^2, \dots\}$. In this case we always write $S^{-1}A$ as A_f. Again from (4) of Theorem 3.2.1, we know prime ideals in A_f has a one to one correspondence to prime ideals in A which do not contain f, and that's exactly X_f we met in the exercises of Chapter 1. You can show that $\operatorname{Spec} A_f$ is homeomorphic to X_f. In fact, $\operatorname{Spec} A_f$ is isomorphic to $(X_f, \mathcal{O}_{\operatorname{Spec} A}|_{X_f})$ as schemes.

In the last of this section we give a statement for when a prime ideal is a contraction of a prime ideal. As we already know, for an ideal $\mathfrak{a}$, it's a contraction ideal if and only if $\mathfrak{a}^{ec} = \mathfrak{a}$. For a prime ideal, it can be stronger:

Proposition 3.2.1. Let $A \to B$ be a ring homomorphism and let $\mathfrak{p}$ be a prime ideal of A. Then $\mathfrak{p}$ is the contraction of a prime ideal if and only if $\mathfrak{p}^{ec} = \mathfrak{p}$.

Proof. If $\mathfrak{p}$ is a contradiction of a prime ideal $\mathfrak{q}$, that is $\mathfrak{p} = \mathfrak{q}^c$, it's clear $\mathfrak{p}^{ec} = \mathfrak{p}$. Conversely, if $\mathfrak{p}^{ec} = \mathfrak{p}$, let S be the image of $A - \mathfrak{p}$ in B. Then $\mathfrak{p}^e$ does not meet S, therefore its extension in $S^{-1}B$ is a proper ideal hence is contained in a maximal ideal $\mathfrak{m}$ of $S^{-1}B$. If $\mathfrak{q}$ is the contraction of $\mathfrak{m}$ in B, then $\mathfrak{p}^e \subseteq \mathfrak{q}$ and $\mathfrak{q} \cap S = \varnothing$, which implies $\mathfrak{q}^c = \mathfrak{p}$. $\square$

3.3. **Localization of a module.** The construction of $S^{-1}A$ can be carried through with an A-module M in place of the ring A. Define a relation $\sim$ on $M \times S$ as follows

$$(m, s) \sim (m', s') \iff (sm' - s'm)t = 0, \quad \text{for some } t \in S$$

As before it's also an equivalence relation. We use m/s to denote the equivalence class of (m, s) and use $S^{-1}M$ to denote the set of equivalence classes.

There is a natural way to make $S^{-1}M$ into a $S^{-1}A$-module: take $a/s \in S^{-1}A$, it acts on $S^{-1}M$ as follows: Take $m/s' \in S^{-1}M$, then

$$a/s \cdot (m/s') := a \cdot m/ss'$$

Let $u\colon M \to N$ be an A-module homomorphism, then it give rise to a $S^{-1}A$-module homomorphism $S^{-1}u\colon S^{-1}M \to S^{-1}N$, namely $S^{-1}u$ map m/s to $u(m)/s$. It's a routine to check it's well-defined.

Proposition 3.3.1. The operation S^{-1} is exact.

Proof. For an exact sequence $M' \xrightarrow{f} M \xrightarrow{g} M''$, we need to show $S^{-1}M' \xrightarrow{S^{-1}f} S^{-1}M \xrightarrow{S^{-1}g} S^{-1}M''$ is also exact. It's clear $S^{-1}g \circ S^{-1}f = 0$, since $S^{-1}g \circ S^{-1}f = S^{-1}(g \circ f) = S^{-1}(0) = 0$. Conversely, for $m/s \in \ker S^{-1}g$, then $g(m)/s = 0 \in S^{-1}M''$, so there exists $t \in S$ such that $tg(m) = 0$ in M'', that is $tm \in \ker g = \operatorname{im} f$. So there exists $m' \in M'$ such that $f(m') = tm$. So we have

$$\frac{m}{s} = \frac{tm}{st} = \frac{f(m')}{st} = S^{-1}f(\frac{m'}{st})$$

This completes the proof. □

Corollary 3.3.1. Formation of localization commutes with formation of finite sums, finite intersections and quotients. To be explicit, if N, P are submodules of an A-module M, 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 isomorphic.

Proof. For (1) it's clear. For (2). If $y/s = z/t$ where $y \in N, z \in P, s, t \in S$, then there exists $u \in S$ such that $u(ty - sz) = 0$, hence $w = uty = usz \in N \cap P$ and therefore $y/s = w/stu \in S^{-1}(N \cap P)$. Thus $S^{-1}N \cap S^{-1}P \subseteq S^{-1}(N \cap P)$, and the reverse inclusion is obvious.

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

Proposition 3.3.2. Let M be an A-module. Then $S^{-1}A$-modules $S^{-1}M$ and $S^{-1}A \otimes_A M$ are isomorphic.

Proof. Consider the $S^{-1}A$-bilinear mapping
$$S^{-1}A \times M \to S^{-1}M$$
$$(a/s, m) \mapsto am/s$$
then it induces an $S^{-1}A$-module homomorphism $f\colon S^{-1}A \otimes_A M \to S^{-1}M$. It's clear f is surjective. Let $\sum_i (a_i/s_i) \otimes m_i$ be any element of $S^{-1}A \otimes M$. If $s = \prod_i s_i \in S, t_i = \prod_{i \neq j} s_j$, then
$$\sum_i \frac{a_i}{s_i} \otimes m_i = \sum_i \frac{a_i t_i}{s} \otimes m_i = \sum_i \frac{1}{s} \otimes a_i t_i m = \frac{1}{s} \otimes \sum_i a_i t_i m_i$$
So every element of $S^{-1}A \otimes M$ is of form $(1/s) \otimes m$. Suppose $f((1/s) \otimes m) = 0$. Then $m/s = 0$, hence $tm = 0$ for some $t \in S$. Therefore,
$$\frac{1}{s} \otimes m = \frac{t}{st} \otimes m = \frac{1}{st} \otimes tm = \frac{1}{st} \otimes 0 = 0$$
□

Corollary 3.3.2. $S^{-1}A$ is a flat A-module.

Proof. For any exact sequence of A-module $0 \to M' \to M$, we need to show
$$0 \to S^{-1}A \otimes_A M' \to S^{-1}A \otimes_A M$$
is exact. But this is isomorphic to
$$0 \to S^{-1}M' \to S^{-1}M$$
use the fact operation S^{-1} is exact to conclude. □

Proposition 3.3.3. If M, N are A-modules, there is a unique isomorphism of $S^{-1}A$-modules $f\colon S^{-1}M \otimes_{S^{-1}A} S^{-1}N \to S^{-1}(M \otimes_A N)$ such that
$$f((m/s) \otimes (n/t)) = (m \otimes n)/st$$

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

Proof. Note that
$$\begin{aligned}
S^{-1}M \otimes_{S^{-1}A} S^{-1}N &\cong (S^{-1}A \otimes_A M) \otimes_{S^{-1}A} (S^{-1}A \otimes_A N)\\
&= (M \otimes_A S^{-1}A) \otimes_{S^{-1}A} (S^{-1}A \otimes_A N)\\
&= M \otimes_A (S^{-1}A \otimes_{S^{-1}A} (S^{-1}A \otimes_A N))\\
&= M \otimes_A (S^{-1}A \otimes_A N)\\
&= S^{-1}A \otimes_A (M \otimes_A N)\\
&= S^{-1}(M \otimes_A N)
\end{aligned}$$
□

3.4. **Local properties.** A property P of a ring A or of an A-module M is said to be a local property if the following is true: A or M has P if and only if $A_{\mathfrak{p}}$ or $M_{\mathfrak{p}}$ has P for each prime ideal $\mathfrak{p}$ of A.

Proposition 3.4.1. Let M be an A-module. Then the following statements are equivalent.

(1) $M = 0$.
(2) $M_{\mathfrak{p}} = 0$ for all prime ideals $\mathfrak{p}$ of A.
(3) $M_{\mathfrak{m}} = 0$ for all maximal ideals $\mathfrak{m}$ of A.

Proof. It's clear (1) to (2) to (3). For (3) to (1). If $M \neq 0$, take $x \in M$ as a non-zero element of M, and let $\mathfrak{a} = \mathrm{Ann}(x)$. $\mathfrak{a}$ is an ideal which is contained in a maximal ideal $\mathfrak{m}$. Consider $x/1 \in M_{\mathfrak{m}}$. Since $M_{\mathfrak{m}} = 0$ thus $x/1 = 0$, that is x is killed by some element of $A \setminus \mathfrak{m}$, but this is impossible. □

Proposition 3.4.2. Let $\phi\colon M \to N$ be an A-module homomorphism. Then the following statements are equivalent.

(1) ϕ is injective.
(2) $\phi_{\mathfrak{p}}\colon M_{\mathfrak{p}} \to N_{\mathfrak{p}}$ is injective for each prime ideal $\mathfrak{p}$.
(3) $\phi_{\mathfrak{m}}\colon M_{\mathfrak{m}} \to N_{\mathfrak{m}}$ is injective for each maximal ideal $\mathfrak{m}$.

Proof. (1) to (2) is clear, since localization is an exact functor. (2) to (3) is also clear.

For (3) to (1). Let $M' = \ker\phi$, then $0 \to M' \to M \to N$ is exact, hence $0 \to M'_{\mathfrak{m}} \to M_{\mathfrak{m}} \to N_{\mathfrak{m}}$ is exact and $M'_{\mathfrak{m}} \cong \ker\phi_{\mathfrak{m}} = 0$ since $\phi_{\mathfrak{m}}$ is injective. Thus $M' = 0$ by Proposition 3.4.1. □

Proposition 3.4.3. For any A-module M, the following statements are equivalent:

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

Proof. For (1) to (2). Note that $M_{\mathfrak{p}} \cong A_{\mathfrak{p}} \otimes_A M$ and M is a flat A-module, thus $M_{\mathfrak{p}}$ is a flat $A_{\mathfrak{p}}$-module.

(2) to (3) is clear. For (3) to (1). For any exact sequence of A-module $0 \to N \to P$, we need to show $0 \to N \otimes M \to P \otimes M$ is exact. It suffices to show

$$0 \to (N \otimes M)_{\mathfrak{m}} \to (P \otimes M)_{\mathfrak{m}}$$

is exact for all maximal ideal $\mathfrak{m}$. Note that localization commutes with tensor product, that is above sequence is isomorphic to

$$0 \to N_{\mathfrak{m}} \otimes_{A_{\mathfrak{m}}} M_{\mathfrak{m}} \to P_{\mathfrak{m}} \otimes_{A_{\mathfrak{m}}} M_{\mathfrak{m}}$$

It's exact since $M_{\mathfrak{m}}$ is a flat $A_{\mathfrak{m}}$-module. □

3.5. **Operations which commute with localization.** Here we give a summary for operations which commute with localization:

(1) Finite sum.
(2) Product.
(3) Intersection.
(4) Quotient.
(5) Radical.
(6) Tensor.
(7) Annihilator.

3.6. **Part of solutions of Chapter 3.**

Exercise 3.6.1. Let S be a multiplicative closed subset of a ring A, and let M be a finitely generated A-module. Prove that $S^{-1}M = 0$ if and only if there exists $s \in S$ such that $sM = 0$.

Proof. If $S^{-1}M = 0$, then $x/1 = 0$ for all $x \in M$. Let $\{x_1, \dots, x_n\}$ denote the set of generators of M. So for each x_i we have a s_i such that $s_i x_i = 0$, then $s = \prod_{i=1}^n s_i$ is such that $sM = 0$. Converse is clear. □

Exercise 3.6.2. Let $\mathfrak{a}$ be an ideal of a ring A, and let $S = 1 + \mathfrak{a}$. Show that $S^{-1}\mathfrak{a}$ is contained in the Jacobson radical of $S^{-1}A$.

Proof. It suffices to show for every maximal ideal $\mathfrak{m}$ of $S^{-1}A$, we have $S^{-1}\mathfrak{a} \subseteq \mathfrak{m}$. Note that every ideal of $S^{-1}A$ is an extended ideal, thus there exists an ideal $\mathfrak{b}$ of A such that $S^{-1}\mathfrak{b} = \mathfrak{m}$. Furthermore, $\mathfrak{b} \cap (1 + \mathfrak{a}) = \varnothing$, which implies $(\mathfrak{a} + \mathfrak{b}) \cap (1 + \mathfrak{a}) = 0$. Thus $S^{-1}\mathfrak{a} + S^{-1}\mathfrak{b} \neq (1)$ and it contains $S^{-1}\mathfrak{b}$. By maximality of $S^{-1}\mathfrak{b}$ we have $S^{-1}\mathfrak{a} \subseteq \mathfrak{m}$. This completes the proof. □

Remark 3.6.1. Now let's show we can derive Corollary 2.2.1 from Nakayama's lemma: If M is a finitely generated A-module and $\mathfrak{a}$ is an ideal of A such that $\mathfrak{a}M = M$. Let $S = 1 + \mathfrak{a}$ and note that

$$S^{-1}M = S^{-1}(\mathfrak{a}M) = (S^{-1}\mathfrak{a})(S^{-1}M)$$

Since $S^{-1}\mathfrak{a}$ is contained in Jacobson radical, so Nakayama's lemma implies $S^{-1}M = 0$. By Exercise 3.5.1, there exists $x = 1 + a \in S$ such that $xM = 0$. In this case, $x = 1 + a \equiv 1 \pmod{\mathfrak{a}}$ as desired.

Exercise 3.6.3. Let A be a ring, let S and T be two multiplicative closed subsets of A, and let U be the image of T in $S^{-1}A$. Show that the rings $(ST)^{-1}A$ and $U^{-1}\left(S^{-1}A\right)$ are isomorphic.

Proof. It suffices to show $U^{-1}(S^{-1}A)$ is also the localization of A with respect to ST, and use the fact localization is unique. Take $g\colon A \to B$ such that $g(st)$ is a unit for all $s \in S, t \in T$. Consider the following commutative diagram

$$\begin{tikzcd}
A \arrow[r, "f_S"] \arrow[d, "g"'] & S^{-1}A \arrow[r, "f_U"] \arrow[dl, dashed, "h_1"'] & U^{-1}(S^{-1}A) \arrow[dll, dashed, "h_2"] \\
B & &
\end{tikzcd}$$

h_1 is induced by the fact $g(s)$ is unit for all $s \in S$. Furthermore, $h_1(\bar{t})$ is unit in B for all $\bar{t} \in U$, since $\bar{t} = f_S(t)$ for some $t \in T$ and $h_1 \circ f_S = g$, so it induces h_2. Note that $h_2 \circ f_U \circ f_S = g$, which implies that $U^{-1}(S^{-1}A)$ is the localization of A with respect to ST. $\square$

Exercise 3.6.4. Let $f\colon A \to B$ be a homomorphism of rings and let S be a multiplicative closed subset of A. Let $T = f(S)$. Show that $S^{-1}B$ and $T^{-1}B$ are isomorphic as $S^{-1}A$-modules.

Proof. It's clearly $S^{-1}B$ is a $S^{-1}A$-module, and the $S^{-1}A$-module structure on $T^{-1}B$ is given by $a/s \cdot b := f(a) \cdot b/f(s)$. Consider the following $S^{-1}A$-module morphism:

$$\begin{aligned}\phi\colon S^{-1}B &\to T^{-1}B \\ b/s &\mapsto b/f(s)\end{aligned}$$

It's well-defined, since for $b/s = b'/s'$, there exists $u \in S$ such that $(bs' - b's)u = 0$, thus $f((bs' - b's)u) = (bf(s') - b'f(s))f(u) = 0$, that is $b/f(s) = b'/f(s')$ in $T^{-1}B$.

It's clearly surjective. For injectivity: If $\phi(b/s) = 0$, then there exists $f(s') \in T$ such that $f(s')b = 0$. But if we want to show $b/s = 0$, we need to find $s' \in S$ such that $s' \cdot b = 0$, and that's exactly $f(s')b = 0$. So ϕ is an isomorphism. $\square$

Exercise 3.6.5. Let A be a ring. Suppose that, for each prime ideal $\mathfrak{p}$, the local ring $A_{\mathfrak{p}}$ has no nilpotent element $\neq 0$. Show that A has no nilpotent element $\neq 0$. If each $A_{\mathfrak{p}}$ is an integral domain, is A necessarily an integral domain?

Proof. That's to show nilpotence is a local property: It suffices to show nilradical $\mathfrak{N}$ of A is zero, note that $(\mathfrak{N})_{\mathfrak{p}}$ is the nilradical of $A_{\mathfrak{p}}$. If for all prime ideal $\mathfrak{p}$ we have $A_{\mathfrak{p}}$ contains no nilpotent element, thus $(\mathfrak{N})_{\mathfrak{p}} = 0$ for all prime ideals $\mathfrak{p}$, which implies $\mathfrak{N} = 0$.

However, integral is not a local property. Consider $\mathbb{Z}_6$, it's clearly not a domain. The prime ideals of it are

$$\begin{aligned}\mathfrak{p} &= \mathbb{Z}_3 \\ \mathfrak{q} &= \mathbb{Z}_2\end{aligned}$$

Now let's see its localization at $\mathfrak{p}$: Since it's a local ring, it suffices to consider it's maximal ideal, that's the extension of $\mathfrak{p}$

$$\begin{aligned}\mathfrak{p}(\mathbb{Z}_6)_\mathfrak{p} &= \{r/s \mid r \in \mathfrak{p}, s \notin \mathfrak{p}\} \\ &= \{\frac{0}{1}, \frac{2}{1}, \frac{4}{1}, \frac{0}{3}, \frac{2}{3}, \frac{4}{3}, \frac{0}{5}, \frac{2}{5}, \frac{4}{5}\}\end{aligned}$$

However, $r_1/s_1 = r_2/s_2$ if and only if there is $u \notin \mathfrak{p}$ such that $u(r_1s_2 - r_2s_1) = 0$. Thus $2/1 = 0/1$ since $3(2 \times 1 - 0) = 0$. In fact, after simple computations we can see $\mathfrak{p}(\mathbb{Z}_6)_\mathfrak{p} = 0$. That's it's a field, definitely a domain. □

Exercise 3.6.6. Let A be a ring $\neq 0$ and let Σ be the set of all multiplicative closed subsets S of A such that $0 \notin S$. Show that Σ has maximal elements, and that $S \in \Sigma$ is maximal if and only if $A - S$ is a minimal prime ideal of A.

Proof. By Zorn's lemma it's easy to see it has a maximal element. Now let's see S is maximal if and only if $A - S$ is a minimal prime ideal: Note that for a general multiplicative closed subset, the complement of it may not be a prime ideal. However, for a maximal multiplicative closed subset, the complement of it must be a prime ideal: For a multiplicative closed subset S, and $\mathfrak{p} = A - S$.

(1) To see $a + b \in \mathfrak{p}$ for any $a, b \in \mathfrak{p}$: It suffices to show $a + b \in S$ implies either $a \in S$ or $b \in S$. If $a + b \in S$, consider the multiplicative sets $A = S(a^n)_{n\geq 0}$ and $B = S(b^n)_{n\geq 0}$. If $0 \in A \cap B$, then there exists $s_1, s_2 \in S$ and $n, m \geq 0$ such that
$$s_1a^n = s_2b^m = 0$$
Then we have
$$0 = s_1s_2(a + b)^{n+m} \in S$$
A contradiction. Therefore, Without lose of generality we may assume $0 \notin S(a^n)_{n\geq 0}$. By maximality of S, this implies $S(a^n)_{n\geq 0} = S$ and so that $a \in S$.

(2) To see $ra \in \mathfrak{p}$ for any $r \in A, a \in \mathfrak{p}$: Its contrapositive is $ra \in S$ for some $r \in A$ implies $a \in S$. Similarly if $0 \in S(a^n)_{n\geq 0}$ then there exists $s_1 \in S$ and $n \geq 0$ such that $s_1a^n = 0$. Then
$$0 = s_1r^na^n \in S$$
A contradiction. Therefore again by maximality of S we have $a \in S$.

(3) $\mathfrak{p}$ is prime is clear.

Thus for a maximal multiplicative closed subset S, $\mathfrak{p} = A - S$ must be a prime ideal, and it must be minimal, otherwise for $\mathfrak{p}' \subseteq \mathfrak{p}$, $A - \mathfrak{p}'$ will contain S.

On the other hand: assume $\mathfrak{p} = A - S$ is a minimal prime ideal, and it's not maximal. Then S must be contained in some maximal multiplicative closed subset S', note that $S' = A - \mathfrak{p}'$ for some minimal prime ideal, but $S \subseteq S'$ implies $\mathfrak{p}' \subseteq \mathfrak{p}$, a contradiction to the minimality of $\mathfrak{p}$. □

Exercise 3.6.7. A multiplicative closed subset S of a ring A is said to be saturated if $xy \in S$ if and only if $x \in S$ and $y \in S$. Prove that

(1) S is saturated if and only if $A - S$ is a union of prime ideals.
(2) If S is any multiplicative closed subset of A, there is a unique smallest saturated multiplicative closed subset $\overline{S}$ containing S, and that $\overline{S}$ is the complement in A of the union of the prime ideals which do not meet S. ($\overline{S}$ is called the saturation of S.)
(3) If $S = 1 + \mathfrak{a}$, where $\mathfrak{a}$ is an ideal of A, find $\overline{S}$.

Proof. For (1). If $\mathfrak{p}$ is a union of prime ideals, then it's clear S is saturated. Conversely, if S is saturated, then if $x \notin S$, then $rx \notin S$ for all $r \in A$, which implies $(x) \cap S = \varnothing$. So $S^{-1}(x) \neq (1)$, and it is contained in some prime ideal $\mathfrak{q}$. Then

$$(x) \subseteq (S^{-1}(x))^c \subseteq \mathfrak{q}^c$$

Furthermore, $\mathfrak{q}^c \cap S = \varnothing$, thus (x) is contained in a prime $\mathfrak{q}^c \subseteq A - S$. That is every element of $A - S$ lies in some prime ideal, thus $A - S$ is a union of prime ideals.

For (2). If $\mathfrak{p}$ is the union of all prime ideals which do not meet S, then $\overline{S} = A - \mathfrak{p}$ is a saturated multiplicative closed subset containing S. If $\overline{S}$ is not minimal, then the minimal one $\overline{S}'$ must be contained in $\overline{S}$, then consider $\mathfrak{p}' = A - \overline{S}'$, clear $\mathfrak{p} \subseteq \mathfrak{p}'$. Furthermore, $\mathfrak{p}'$ is the union of prime ideals which do not meet S, thus $\mathfrak{p}$ do not contain all, a contradiction.

For (3). If $S = 1 + \mathfrak{a}$. □

Exercise 3.6.8. Let S, T be multiplicative closed subsets of A, such that $S \subseteq T$. Let $\phi\colon S^{-1}A \to T^{-1}A$ be the homomorphism which maps each $a/x \in S^{-1}A$ to a/x considered as an element of $T^{-1}A$. Show that the following statements are equivalent:

(1) ϕ is bijective.
(2) For each $t \in T, t/1$ is a unit in $S^{-1}A$.
(3) For each $t \in T$ there exists $x \in A$ such that $xt \in S$.
(4) T is contained in the saturation of S.
(5) Every prime ideal which meets T also meets S.

Proof. For (1) to (2). Since ϕ is surjective, then there exists $a/s \in S^{-1}A$ such that $\phi(a/s) = 1/t$ in $T^{-1}A$. Consider $\phi(a/s \cdot t/1) = 1/1 \in T^{-1}A$, by injectivity of ϕ we have a/s is the inverse of $t/1$.

For (2) to (3). If $t/1$ is a unit in $S^{-1}A$, use a/s to denote its inverse. Then $at/s = 1/1$ in $S^{-1}A$ implies there exists $u \in S$ such that $u(at-s) = 0$. Let $x = au$, we have $xt \in S$.

For (3) to (1). For injectivity: if $a/s = 0$ in T^{-1}A, then there exists $t \in T$ such that $at = 0$. But there exists $x \in A$ such that $xt \in S$, thus $axt = 0$ implies $a/s = 0$ in $S^{-1}A$. For surjectivity, for $a/t \in T^{-1}A$, since there exists $x \in A$ such that $xt \in S$. Note that $a/t = ax/xt \in T^{-1}A$, thus $\phi(ax/xt) = a/t$ as desired.

For (3) to (4). For $t \in T$ there exists $x \in A$ such that $xt \in S \subset \overline{S}$, then $t \in \overline{S}$ since $\overline{S}$ is saturated.

For (4) to (5). If there exists a prime ideal which meets T but not meets S, then T can not be contained in $\overline{S}$, since $\overline{S}$ is the complement of the union of all prime ideals which do not meet S.

For (5) to (3). If there exists a $t \in T$ such that there is no $x \in A$ satisfying $xt \in S$, then $(t) \cap S = \varnothing$. Then consider $S^{-1}(t) \in S^{-1}A$, it must be contained in some prime ideal $\mathfrak{p}$. Then $(t) \subseteq \mathfrak{p}^c$, that is (t) is contained in a prime ideal which does not meet S, a contradiction. $\square$

Exercise 3.6.9. The set S_0 of all non-zero-divisors in A is a saturated multiplicative closed subset of A. Hence the set D of zero-divisors in A is a union of prime ideals. Show that every minimal prime ideal of A is contained in D.

The ring $S_0^{-1}A$ is called the total ring of fractions of A. Prove that

(1) S_0 is the largest multiplicative closed subset of A for which the homomorphism $A \to S_0^{-1}A$ is injective.
(2) Every element in $S_0^{-1}A$ is either a zero-divisor or a unit.
(3) Every ring in which every non-unit is a zero-divisor is equal to its total ring of fractions (i.e., $A \to S_0^{-1}A$ is bijective).

Proof. For any minimal prime ideal $\mathfrak{p}$, $S = A - \mathfrak{p}$ is a maximal multiplicative closed subset. If we want to show every minimal prime ideal of A is contained in D, it suffices to show S_0 is contained in every maximal multiplicative closed subset. Indeed, if $S_0 \not\subseteq S$ for some maximal multiplicative closed subset S which does not contain 0, then SS_0 must contain 0, since it strictly contains S. But this implies there exist $s_0 \in S_0, s \in S$ such that $s_0 s = 0$, a contradiction to the definition of S_0.

For (1). It's clear $f\colon A \to S_0^{-1}A$ is injective, since by Remark 3.1.5 we know the kernel of f is zero divisor of A. Furthermore, $S_0^{-1}A$ is maximal. Indeed, assume $S_0 \subset S$ for some S, then there exists a zero-divisor a of A in S, then $f\colon A \to S^{-1}A$ maps u into zero, not injective.

For (2). Note that if $a/s = 0 \in S_0^{-1}A$ is a zero-divisor, then there exists $u \in S_0$ such that $au = 0$, but u is a non-zero-divisor, then $a = 0$. So $a/s = 0 \in S_0^{-1}A$ if and only if $a = 0$, thus $a/s \in S_0^{-1}A$ is a zero-divisor if and only if a is. So if a/s is not a zero-divisor, thus a is not a zero-divisor, that is $a \in S_0$, thus a/s is a unit.

For (3). Note that if in ring A every non-unit is a zero-divisor, then S_0, the set of all non-zero-divisors is exactly the set of all units. Thus $A \to S_0^{-1}A$ clearly a bijective, since localization is the most economic operation to make all elements in S_0 to be unit. □

Exercise 3.6.10. Let A be a ring.

(1) If A is absolutely flat and S is any multiplicative closed subset of A, then $S^{-1}A$ is absolutely flat.
(2) A is absolutely flat $\Leftrightarrow A_{\mathfrak{m}}$ is a field for each maximal ideal $\mathfrak{m}$.

Proof. For (1). Note that a ring A is absolutely flat if and only if every principal ideal is idempotent. For $x/s \in S^{-1}A$, then $x \in A$ implies there exists $a \in A$ such that $x = ax^2$, since A is absolutely flat. Thus

$$\frac{x}{s} = \frac{ax^2}{s} = \frac{as}{1}(\frac{x}{s})^2$$

thus $S^{-1}A$ is absolutely flat.

For (2). If A is absolutely flat, then by (1) we know $A_{\mathfrak{m}}$ is absolutely flat for all maximal ideal $\mathfrak{m}$, thus by (4) of Exercise 2.8.28, $A_{\mathfrak{m}}$ is a field since it's a local ring. Conversely, we need to show every A-module M, it's flat: That is to show for any exact sequence $0 \to B' \to B$ of A-modules, we have the following exact sequence

$$0 \to B' \otimes_A M \to B \otimes_A M$$

Since exactness is a local property, it suffices to show for any maximal ideal $\mathfrak{m}$ we have the following exact sequence

$$0 \to B'_{\mathfrak{m}} \otimes_{A_{\mathfrak{m}}} M_{\mathfrak{m}} \to B_{\mathfrak{m}} \otimes_{A_{\mathfrak{m}}} M_{\mathfrak{m}}$$

But this is clearly exact, since tensor product of vector space is always exact. □

Exercise 3.6.11. Let A be a ring. Prove that the following statements are equivalent.

(1) $A/\mathfrak{N}$ is absolutely flat.
(2) Every prime ideal of A is maximal.
(3) $\operatorname{Spec} A$ is a T_1-space.
(4) $\operatorname{Spec} A$ is Hausdorff.

If these conditions are satisfied, show that $\operatorname{Spec} A$ is compact and totally disconnected.

Proof. For (1) to (4). Note that $\operatorname{Spec} A = \operatorname{Spec}(A/\mathfrak{N})$, thus it suffices to show $\operatorname{Spec}(A/\mathfrak{N})$ is Hausdorff. In general, for an absolutely flat ring A', $\operatorname{Spec} A'$ is Hausdorff. Indeed, for any $f \in A'$, we have $f(1 - af) = 0$ for some $a \in A'$, which implies $X_f \coprod X_{1-af} = \operatorname{Spec} A'$. For any distinct points $\mathfrak{p}_x, \mathfrak{p}_y \in \operatorname{Spec} A'$, there must exist some X_f such that X_f, X_{1-af} must separate $\mathfrak{p}_x$ and $\mathfrak{p}_y$, otherwise $\mathfrak{p}_x \in \overline{\{\mathfrak{p}_y\}}$ and $\mathfrak{p}_y \in \overline{\{\mathfrak{p}_x\}}$, which implies $\mathfrak{p}_x = \mathfrak{p}_y$, a contradiction.

For (4) to (3) is clear.

For (3) to (2). By (1) of Exercise 1.8.19, we have the subset consisting of a Single point $\{\mathfrak{p}_x\}$ is closed if and only if $\mathfrak{p}_x$ is maximal.

For (2) to (1). If every prime ideal of A is maximal, $A' = A/\mathfrak{N}$ is a ring without nilpotent element such that every prime ideal is maximal. Fix $x \in A'$ and consider $S = \{x^n(1+ax) \mid n \geq 0, a \in A'\}$. If $0 \notin S$, $S^{-1}A$ is not a zero ring thus we can find some prime ideal of it. Then there exists a prime ideal $\mathfrak{p}$ such that $\mathfrak{p} \cap S = \varnothing$. But either x or $1 - ax$ in $\mathfrak{p}$ since $\mathfrak{p}$ is maximal, a contradiction. Thus $0 \in S$, so there exists $n \geq 0, a \in A'$ such that

$$x^n(1 - ax) = 0$$

which implies $x(1 - ax)$ is nilpotent, thus it's zero. So we have $(x) = (x^2)$, that is A' is absolutely flat. □

Exercise 3.6.12. Let A be an integral domain and M an A-module. An element $x \in M$ is a torsion element of M if Ann $(x) \neq 0$, that is if x is killed by some non-zero element of A. Show that the torsion elements of M form a submodule of M. This submodule is called the torsion submodule of M and is denoted by $T(M)$. If $T(M) = 0$, the module M is said to be torsion-free. Show that

(1) If M is any A-module, then $M/T(M)$ is torsion-free.
(2) If $f : M \to N$ is a module homomorphism, then $f(T(M)) \subseteq T(N)$.
(3) If $0 \to M' \xrightarrow{f} M \xrightarrow{g} M''$ is an exact sequence, then the sequence $0 \to T(M') \xrightarrow{f} T(M) \xrightarrow{g} T(M'')$ is exact.
(4) If M is any A-module, then $T(M)$ is the kernel of the mapping $x \mapsto 1 \otimes x$ of M into $K \otimes_A M$, where K is the field of fractions of A.

Proof. It's clear that all torsion elements form a submodule module of M. For (1). We need to show $T(M/T(M)) = 0$: If $x + T(M) \in M/T(M)$ is a torsion element, so there exists $a_1 \in A$ such that $a_1 x \in T(M)$, so there exists a_2 such that $a_2 a_1 x = 0$, that is $x \in T(M)$.

For (2). Take $x \in T(M)$, then there exists $a \in A$ such that $ax = 0$, it's clear to see $f(a)f(x) = 0$, so $f(x) \in T(N)$, which implies $f(T(M)) \subseteq T(N)$.

For (3). It's clear $f : T(M') \to T(M)$ is still injective, since for $x \in T(M')$ we can regard it as an element in M' and $f(x) = 0$ implies $x = 0$. By the same method, we can see $\operatorname{im} f \subseteq \ker g$. Now it suffices to show $\ker g \subseteq \operatorname{im} f$. Take $x \in T(M)$ such that $g(x) = 0$, then there exists $y \in M'$ such that $f(y) = x$, then it suffices to show $y \in T(M')$. Indeed, note that there exists $a \in A$ such that $ax = 0$, so $f(ay) = 0$, then $ay = 0$ since f is injective.

For (4). It's clear $T(M)$ lies in the kernel of this mapping. Conversely, note that $K \otimes_A M \cong (A \setminus \{0\})^{-1}M$, this isomorphism is defined by $a/s \otimes m \mapsto am/s$. So the kernel of $M \to K \otimes_A M$ is the same as the kernel of $M \to K \otimes_A M \to (A \setminus \{0\})^{-1}M$. The latter mapping is given by $m \mapsto m/1$. So $m/1 = 0$ implies there exists $a \in A \setminus \{0\}$ such that $am = 0$, that is $m \in T(M)$. □

Exercise 3.6.13. Let S be a multiplicative closed subset of an integral domain A. In the notation of Exercise 3.5.12, show that $T(S^{-1}M) = S^{-1}(T(M))$. Deduce that the following statements are equivalent.

(1) M is torsion-free.
(2) $M_{\mathfrak{p}}$ is torsion-free for all prime ideal $\mathfrak{p}$.
(3) $M_{\mathfrak{m}}$ is torsion-free for all maximal ideals $\mathfrak{m}$.

Proof. For $x \in T(M)$, there exists $a \in A$ such that $ax = 0$, so $x/s \in T(S^{-1}M$ since $a/1 \cdot x/s = 0$, that is $S^{-1}(T(M)) \subseteq T(S^{-1}M)$. Conversely, if $x/s \in T(S^{-1}M)$, there exists a/s' such that $a/s' \cdot x/s = 0$, that is there exists $u \in S$ such that $uax = 0$, that is $x \in T(M)$. Thus $T(S^{-1}M) = S^{-1}(T(M))$.

For (1) to (2). It's clear since $T(M_{\mathfrak{p}}) = T(M)_{\mathfrak{p}} = 0$. For (2) to (3). Trivial.

For (3) to (1). It suffices to show $T(M)_{\mathfrak{m}}$ for all maximal ideal $\mathfrak{m}$, and that's clear. □

Exercise 3.6.14. Let M be an A-module and $\mathfrak{a}$ an ideal of A. Suppose that $M_{\mathfrak{m}} = 0$ for all maximal ideals $\mathfrak{m} \supseteq \mathfrak{a}$. Prove that $M = \mathfrak{a}M$.

Proof. It suffices to show $A/\mathfrak{a}$-module $M/\mathfrak{a}M = 0$. But

$$(M/\mathfrak{a})_{\mathfrak{m}} \cong M_{\mathfrak{m}}/(\mathfrak{a}M)_{\mathfrak{m}} = 0$$

This completes the proof. □

Exercise 3.6.15. Let A be a ring, and let F be the A-module A^n. Show that every set of n generators of F is a basis of F. Deduce that every set of generators of F has at least n elements.

Proof. Let $x_1, \dots, x_n$ be a set of generators and $e_1, \dots, e_n$ the canonical basis of F. Define $\phi\colon F \to F$ by $\phi(e_i) = x_i$. Then ϕ is surjective and we have to prove that it is an isomorphism. Since injectivity is a local property we may assume that A is a local ring. Let N be the kernel of ϕ and let $k = A/\mathfrak{m}$ be the residue field of A. Since field is always flat, the exact sequence $0 \to N \to F \xrightarrow{\phi} F \to 0$ gives an exact sequence

$$0 \to k \otimes N \to k \otimes F \xrightarrow{1\otimes\phi} k \otimes F \to 0$$

Now $k \otimes F = k^n$ is an n-dimensional vector space over k. $1 \otimes \phi$ is surjective, hence bijective, hence $k \otimes N = N/\mathfrak{m}N = 0$. Also N is finitely generated, by Chapter 2, Exercise 2.8.12, hence $N = 0$ by Nakayama's lemma, since $N = \mathfrak{m}N$ and for a local ring $\mathfrak{m} = \mathfrak{R}$. Hence ϕ is an isomorphism.

Assume $\{x_1, \dots, x_k\}, k < n$ is a set of generators of F, then add $\{e_{k+1}, \dots, e_n\}$ into them we still obtain a set of generators, with n elements. Then we know that

$$\begin{cases} \phi(e_i) = x_i, & 1 \leq i \leq k \\ \phi(e_i) = e_i, & k < i \leq n \end{cases}$$

is an isomorphism. Claim $\{x_1, \ldots, x_k\}$ can not generate e_{k+1}. Indeed, if $\sum_{i=1}^k a_i x_i = e_{k+1}$, then

$$\phi(\sum_{i=1}^k a_i e_i) = \sum_{i=1}^k a_i x_i = e_{k+1} = \phi(e_{k+1})$$

But ϕ is injective, thus $\sum_{i=1}^k a_i e_i = e_{k+1}$, a contradiction. □

Exercise 3.6.16. Let B be a flat A-algebra. Then the following conditions are equivalent:

(1) $\mathfrak{a}^{ec} = \mathfrak{a}$ for all ideals $\mathfrak{a}$ of A.
(2) $\operatorname{Spec} B \to \operatorname{Spec} A$ is surjective.
(3) For every maximal ideal $\mathfrak{m}$ of A we have $\mathfrak{m}^e \neq (1)$.
(4) If M is any non-zero A-module, then $M_B \neq 0$.
(5) For every A-module M, the mapping $x \mapsto 1 \otimes x$ of M into M_B is injective.

In this case, B is called faithfully flat over A.

Proof. For (1) to (2). It's clear since for any ideal $\mathfrak{a}$ of A, we have $\mathfrak{a}$ is the contraction of $\mathfrak{a}^e$, thus $\operatorname{Spec} B \to \operatorname{Spec} A$ is surjective.

For (2) to (3). If there exists a maximal ideal $\mathfrak{m}$ of A such that $\mathfrak{m}^e = (1)$, consider $\mathfrak{b}^c = \mathfrak{m}$ since surjectivity. Then

$$(1) = \mathfrak{b}^{ce} \subseteq \mathfrak{b}$$

a contradiction.

For (3) to (4). Let $x \in M$ be a non-zero element, and consider $M' = Ax$. Note that we have an inclusion $M' \hookrightarrow M$ and B is flat over A, then $M' \otimes_A B \to M \otimes_A B$ is also injective, that is $M'_B \hookrightarrow M_B$. So it suffices to show $M'_B \neq 0$. If we write $M' \cong A/\mathfrak{a}$ for some ideal $\mathfrak{a}$, then $M'_B \cong A/\mathfrak{a} \otimes_A B \cong B/\mathfrak{a}B = B/\mathfrak{a}^e$. Since $\mathfrak{a}$ is contained in some maximal ideal $\mathfrak{m}$, thus $\mathfrak{a}^c \subseteq \mathfrak{m}^c \neq (1)$, which implies $M'_B \neq 0$.

For (4) to (5). Let M' be the kernel of $M \to M_B$. Since B is flat over A, then following sequence is exact

$$0 \to M'_B \to M_B \to (M_B)_B$$

But Exercise 2.8.13 implies $M_B \to (M_B)_B$ is injective, thus $M'_B = 0$, so we have $M' = 0$, as desired.

For (5) to (1). Consider $M = A/\mathfrak{a}$, then we the following mapping is injective $A/\mathfrak{a} \to B/\mathfrak{a}^e$, which implies $\mathfrak{a}^{ec} = \mathfrak{a}$. □

Exercise 3.6.17. Let $A \xrightarrow{f} B \xrightarrow{g} C$ be ring homomorphisms. If $g \circ f$ is flat and g is faithfully flat, then f is flat.

Proof. It suffices to check for any exact sequence of A-modules $0 \to M' \to M$, we have the following sequence is exact

$$0 \to M'_B \to M_B$$

Note that we have $(M'_B)_C = M'_C$ and $(M_B)_C = M_C$. Indeed, $(M \otimes_A B) \otimes_B C = M \otimes_A (B \otimes_B C) = M \otimes_A C$. So we have the two columns of following commutative diagram is exact since C is faithfully flat over C:

$$\begin{tikzcd}
 & 0 \arrow[d] & 0 \arrow[d] \\
0 \arrow[r] & M'_B \arrow[r] \arrow[d] & M_B \arrow[d] \\
0 \arrow[r] & M'_C \arrow[r] & M_C
\end{tikzcd}$$

Furthermore the second row is also exact since C is flat over A, it's easy to check the first row is exact using commutativity of diagram. □

Exercise 3.6.18. Let $f\colon A \to B$ be a flat homomorphism of rings, let $\mathfrak{q}$ be a prime ideal of B and let $\mathfrak{p} = \mathfrak{q}^c$. Then $f^* : \operatorname{Spec} B_{\mathfrak{q}} \to \operatorname{Spec} A_{\mathfrak{p}}$ is surjective.

Proof. Note that flat is a local property thus $B_{\mathfrak{p}}$ is flat over $A_{\mathfrak{p}}$. If we use S to denote $A - \mathfrak{p}$ and T to denote $B - \mathfrak{q}$, we have

$$B_{\mathfrak{q}} = T^{-1}B = U^{-1}(f(S))^{-1}B = U^{-1}B_{\mathfrak{p}}$$

where U is the image of T in $f(S)^{-1}B$. Thus $B_{\mathfrak{q}}$ is flat over $B_{\mathfrak{p}}$ since it's a localization of $B_{\mathfrak{p}}$. So we have $B_{\mathfrak{q}}$ is flat over $A_{\mathfrak{p}}$. Now it suffices to show it's faithfully flat. Consider the extension of only maximal ideal $\mathfrak{p}A_p$, it must lie in the only maximal ideal of $B_{\mathfrak{p}}$ and thus $\neq (1)$. By (3) of Exercise 3.5.16 we know $B_{\mathfrak{q}}$ is faithfully flat over $A_{\mathfrak{p}}$. □

Exercise 3.6.19. Let A be a ring, M an A-module. The support of M is defined to be the set $\operatorname{supp}(M)$ of prime ideals $\mathfrak{p}$ of A such that $M_{\mathfrak{p}} \neq 0$. Prove the following results:

(1) $M \neq 0$ if and only if $\operatorname{supp}(M) \neq \varnothing$.
(2) $V(\mathfrak{a}) = \operatorname{supp}(A/\mathfrak{a})$.
(3) If $0 \to M' \to M \to M'' \to 0$ is an exact sequence, then $\operatorname{supp}(M) = \operatorname{Supp}(M') \cup \operatorname{supp}(M'')$.
(4) If $M = \sum M_i$, then $\operatorname{supp}(M) = \bigcup \operatorname{supp}(M_i)$.
(5) If M is finitely generated, then $\operatorname{supp}(M) = V(\operatorname{Ann}(M))$ (and is therefore a closed subset of $\operatorname{Spec} A$).
(6) If M, N are finitely generated, then $\operatorname{supp}(M \otimes_A N) = \operatorname{supp}(M) \cap \operatorname{Supp}(N)$.
(7) If M is finitely generated and $\mathfrak{a}$ is an ideal of A, then $\operatorname{supp}(M/\mathfrak{a}M) = V(\mathfrak{a} + \operatorname{Ann}(M))$.
(8) If $f\colon A \to B$ is a ring homomorphism and M is a finitely generated A module, then $\operatorname{supp}(B \otimes_A M) = f^{*-1}(\operatorname{supp}(M))$.

Proof. For (1). It's clear since $M = 0$ if and only if $M_{\mathfrak{p}} = 0$ for all prime ideals $\mathfrak{p}$.

For (2). For any prime ideal $\mathfrak{p} \in V(\mathfrak{a})$, we have

$$(A/\mathfrak{a})_{\mathfrak{p}} = A_{\mathfrak{p}}/\mathfrak{a}A_{\mathfrak{p}} = A_{\mathfrak{p}}/\mathfrak{a}^e$$

Note that $\mathfrak{a}^e \subseteq \mathfrak{p}^e \subset (1)$, thus $A/\mathfrak{a}^e \neq 0$, that is $V(\mathfrak{a}) \subseteq \operatorname{supp}(A/\mathfrak{a})$. Conversely, if a prime ideal $\mathfrak{p}$ of A such that $A_{\mathfrak{p}}/\mathfrak{a}^e \neq 0$, so $\mathfrak{a}^e$ is contained in some (also the unique one) prime ideal $\mathfrak{a}^e \subseteq \mathfrak{p}^e$. So $\mathfrak{a} \subseteq \mathfrak{a}^{ec} \subseteq \mathfrak{p}^{ec} = \mathfrak{p}$.

For (3). Since localization is an exact functor, thus for a prime ideal $\mathfrak{p}$, we have the following exact sequence

$$0 \to M'_{\mathfrak{p}} \to M_{\mathfrak{p}} \to M''_{\mathfrak{p}} \to 0$$

It's clear to see desired result from this exact sequence.

For (4). Note that localization commutes with summation, that is for any prime ideal $\mathfrak{p}$,

$$M_{\mathfrak{p}} = (\sum M_i)_{\mathfrak{p}} = \sum (M_i)_{\mathfrak{p}}$$

Thus $M_{\mathfrak{p}} \neq 0$ if and only if there exists some i such that $(M_i)_{\mathfrak{p}}$.

For (5). Note that for a prime ideal $\mathfrak{p}$, we have $M_{\mathfrak{p}} = 0$ if and only if there exists $s \in A - \mathfrak{p}$ such that $sM = 0$, i.e. $\operatorname{Ann}(M) \cap A - \mathfrak{p} \neq \varnothing$. So $M_{\mathfrak{p}} \neq 0$ if and only if $\operatorname{Ann}(M) \cap A - \mathfrak{p} = \varnothing$, which is equivalent to $\operatorname{Ann}(M) \subseteq \mathfrak{p}$.

For (6). Note that for any prime ideal $\mathfrak{p}$

$$(M \otimes_A N)_{\mathfrak{p}} = M_{\mathfrak{p}} \otimes_{A_{\mathfrak{p}}} N_{\mathfrak{p}}$$

Thus $(M \otimes_A N)_{\mathfrak{p}} \neq 0$ if and only if both $M_{\mathfrak{p}}$ and $N_{\mathfrak{p}}$ are not zero.

For (7). Note that

$$\operatorname{Ann}(M/\mathfrak{a}M) = \mathfrak{a} + \operatorname{Ann}(M)$$

and use (5).

For (8). □

Exercise 3.6.20. Let $f\colon A \to B$ be a ring homomorphism, $f^* : \operatorname{Spec} B \to \operatorname{Spec} A$ the associated mapping. Show that

(1) Every prime ideal of A is a contracted ideal $\Leftrightarrow f^*$ is surjective.
(2) Every prime ideal of B is an extended ideal $\Rightarrow f^*$ is injective.

Is the converse of (2) true?

Proof. For (1). It's just (1) and (2) of Exercise 3.5.16.

For (2). For every prime ideal $\mathfrak{q}$ of B, write it as $\mathfrak{q} = \mathfrak{p}^e$. Then if $\mathfrak{q}^c = 0$, then

$$\mathfrak{p} \subseteq \mathfrak{p}^{ec} = \mathfrak{q}^c = 0$$

then $\mathfrak{q}$ is the extension of zero divisor, thus a zero divisor. The converse of (2) may fail. For example: For a field k and consider $k[\varepsilon] := k[x]/(x^2)$, there is a natural inclusion $k \to k[\varepsilon]$. Claim that $k[\varepsilon]$ is a local ring with only one prime (also maximal) ideal (x). Indeed, for $a + bx \in k[\varepsilon]$, if $a = 0$, it's not a unit clearly. if $a \neq 0$, thus

$$(a + bx)(a^{-1} - a^{-2}bx) = 1$$

which implies $a+bx$ is a unit. Thus any element not in (x) is a unit thus (x) is a maximal ideal and $k[\varepsilon]$ is a local ring. Furthermore, since (0) is the only ideal contained in (x) and it's not prime. So $k[\varepsilon]$ is a local ring with only one prime ideal. So $\operatorname{Spec}(k[\varepsilon]) \to \operatorname{Spec} k$ is injective. In fact, it's bijective. But (x) is not an extended ideal, since there are only two ideals of k, that is (1) and (0). Neither of them extend to (x). □

Exercise 3.6.21. This Exercise illustrate the fiber of a morphism between affine schemes.

(1) Let A be a ring, S a multiplicative closed subset of A, and $\phi\colon A \to S^{-1}A$ the canonical homomorphism. Show that $\phi^*\colon \operatorname{Spec}\left(S^{-1}A\right) \to \operatorname{Spec} A$ is a homeomorphism of $\operatorname{Spec}\left(S^{-1}A\right)$ onto its image in $X = \operatorname{Spec} A$. Let this image be denoted by $S^{-1}X$. In particular, if $f \in A$, the image of $\operatorname{Spec}(A_f)$ in X is the basic open set X_f.
(2) Let $f\colon A \to B$ be a ring homomorphism. Let $X = \operatorname{Spec} A$ and $Y = \operatorname{Spec} B$, and let $f^* : Y \to X$ be the mapping associated with f. Identifying $\operatorname{Spec}\left(S^{-1}A\right)$ with its canonical image $S^{-1}X$ in X, and $\operatorname{Spec}(S^{-1}B) := \operatorname{Spec}(f(S)^{-1}B)$ with its canonical image $S^{-1}Y$ in Y, show that $S^{-1}f^* : \operatorname{Spec}\left(S^{-1}B\right) \to \operatorname{Spec}\left(S^{-1}A\right)$ is the restriction of f^* to $S^{-1}Y$, and that $S^{-1}Y = f^{*-1}\left(S^{-1}X\right)$
(3) Let $\mathfrak{a}$ be an ideal of A and let $\mathfrak{b} = \mathfrak{a}^e$ be its extension in B. Let $f\colon A/\mathfrak{a} \to B/\mathfrak{b}$ be the homomorphism induced by f. If $\operatorname{Spec}(A/\mathfrak{a})$ is identified with its canonical image $V(\mathfrak{a})$ in X, and $\operatorname{Spec}(B/\mathfrak{b})$ with its image $V(\mathfrak{b})$ in Y, show that f^* is the restriction of f^* to $V(\mathfrak{b})$.
(4) Let $\mathfrak{p}$ be a prime ideal of A. Take $S = A - \mathfrak{p}$ in (2) and then reduce $\operatorname{mod} S^{-1}\mathfrak{p}$ as in (3). Deduce that the subspace $f^{*-1}(\mathfrak{p})$ of Y is naturally homeomorphic to $\operatorname{Spec}(B_\mathfrak{p}/\mathfrak{p}B_\mathfrak{p}) = \operatorname{Spec}(k(\mathfrak{p}) \otimes_A B)$, where $k(\mathfrak{p})$ is the residue field of the local ring $A_\mathfrak{p}$. $\operatorname{Spec}(k(\mathfrak{p}) \otimes_A B)$ is called the fiber of f^* over $\mathfrak{p}$.

Proof. For (1). Note that every prime ideal of $S^{-1}A$ is an extended ideal, thus by (2) of Exercise 3.5.20, we have $\phi^* : \operatorname{Spec}(S^{-1}A) \to \operatorname{Spec} A$ is injective, thus it's a bijective and continuous map from $\operatorname{Spec}(S^{-1}A)$ to its image. To see it's closed, just note that

$$\phi^*(V(\mathfrak{a}^e)) = V(\mathfrak{a}) \cap \operatorname{im} \phi^*$$

Indeed, take a prime ideal $\mathfrak{q}$ of $S^{-1}A$ such that it contains $\mathfrak{a}^e$, we have $\mathfrak{q}^c \supseteq \mathfrak{a}^{ec} \supseteq \mathfrak{a}$, thus $\phi^*(V(\mathfrak{a}^e)) \subseteq V(\mathfrak{a}) \cap \operatorname{im} \phi^*$. Conversely, take some element of $V(\mathfrak{a}) \cap \operatorname{im} \phi^*$, that is $\mathfrak{q}^c \supseteq \mathfrak{a}$ where $\mathfrak{q}$ is a prime ideal of $S^{-1}A$. Recall that $\mathfrak{q}^c \supseteq \mathfrak{a}$ is equivalent to $\mathfrak{q} \supseteq \mathfrak{a}^e$, so $\mathfrak{q}^c \in \phi^*(V(\mathfrak{a}^e))$. In particular, $\operatorname{Spec} A_f$ consists of prime ideals of A which do not contain f, and that's exactly X_f.

For (2). We have the following commutative diagram

$$\begin{array}{ccc} A & \xrightarrow{f} & B \\ \downarrow{\scriptstyle \phi_A} & & \downarrow{\scriptstyle \phi_B} \\ S^{-1}A & \xrightarrow{S^{-1}f} & S^{-1}B \end{array}$$

Then by applying Spec we obtain the following commutative diagram

$$\begin{array}{ccc} \operatorname{Spec} A & \xleftarrow{f^*} & \operatorname{Spec} B \\ \uparrow{\scriptstyle \phi_A^*} & & \uparrow{\scriptstyle \phi_B^*} \\ \operatorname{Spec}(S^{-1}A) & \xleftarrow{S^{-1}f^*} & \operatorname{Spec}(S^{-1}B) \end{array}$$

The commutativity of the diagram implies that $S^{-1}f^*$ is the restriction of f^* on the image of ϕ_B^*, that is $S^{-1}Y$. Furthermore, $f(S) \cap \mathfrak{q} \neq \varnothing$ if and only if $S \cap f^*(\mathfrak{q}) = \varnothing$. So

$$\mathfrak{q} \in S^{-1}Y \iff f^*(\mathfrak{q}) \in S^{-1}X \iff \mathfrak{q} \in f^{*-1}(S^{-1}X)$$

That is $S^{-1}Y = f^{*-1}(S^{-1}X)$. The proof of (3) is the same as (2).

For (4). It's clear from the following diagram:

$$\begin{array}{ccc} \operatorname{Spec} A & \xleftarrow{f^*} & \operatorname{Spec} B \\ \uparrow & & \uparrow \\ \operatorname{Spec}(A_{\mathfrak{p}}) & \longleftarrow & \operatorname{Spec}(B_{\mathfrak{p}}) \\ \uparrow & & \uparrow \\ \operatorname{Spec}(k(\mathfrak{p})) & \longleftarrow & \operatorname{Spec}(B_{\mathfrak{p}}/\mathfrak{p}B_{\mathfrak{p}}) \end{array}$$

□

Exercise 3.6.22. Let A be a ring and $\mathfrak{p}$ a prime ideal of A. Then the canonical image of $\operatorname{Spec}(A_{\mathfrak{p}})$ in $\operatorname{Spec} A$ is equal to the intersection of all the open neighborhoods of $\mathfrak{p}$ in $\operatorname{Spec} A$.

Proof. The canonical image of $\operatorname{Spec}(A_{\mathfrak{p}})$ in $\operatorname{Spec} A$ is the set of all prime ideals $\mathfrak{q}$ which are contained in $\mathfrak{p}$.

For any open basis X_f such that $\mathfrak{p} \in X_f$, then $f \notin \mathfrak{p}$, so $f \notin \mathfrak{q}$ for those $\mathfrak{q} \subseteq \mathfrak{p}$, which implies $\operatorname{Spec}(A_f) \subseteq X_f$ for all X_f such that $\mathfrak{p} \in X_f$. Thus $\operatorname{Spec}(A_{\mathfrak{p}})$ lies in the intersection of all open neighborhoods of $\mathfrak{p}$. Conversely, if $\mathfrak{q}$ lies in the intersection of all open neighborhoods of $\mathfrak{p}$, then $\mathfrak{p} \in \overline{\{\mathfrak{q}\}} = V(\mathfrak{q})$, thus $\mathfrak{q} \subseteq \mathfrak{p}$. □

Exercise 3.6.23 (structure sheaf of affine schemes)**.** Let A be a ring, $X = \operatorname{Spec} A$ and U be a basic open set in X.

(1) If $U = X_f$, show that the ring $A(U) = A_f$ depends only on U and not on f.

(2) Let $U' = X_g$ be another basic open set such that $U' \subseteq U$. Show that there is an equation of the form $g^n = uf$ for some integer $n > 0$ and some $u \in A$, and use this to define a homomorphism $\rho\colon A(U) \to A(U')$ by mapping a/f^m to au^m/g^{mn}, which is called restriction homomorphisms. Show that ρ depends only on U and U'.
(3) If $U = U'$, then ρ is the identity map.
(4) If $U \supseteq U' \supseteq U''$ are basic open sets in X, show that the diagram

$$\begin{tikzcd} A(U) \arrow[rr] \arrow[dr] & & A(U'') \\ & A(U') \arrow[ur] & \end{tikzcd}$$

is commutative.
(5) Let $x = \mathfrak{p}$ be a point of X. Show that

$$\varinjlim_{x\in U} A(U) \cong A_{\mathfrak{p}}$$

The assignment of the ring $A(U)$ to each basic open set U of X, and the restriction homomorphisms ρ, satisfying the conditions (3) and (4) above, constitutes a presheaf of rings on the basis of open sets $(X_f)_{f\in A}$. (5) says that the stalk of this presheaf at $x \in X$ is the corresponding local ring $A_{\mathfrak{p}}$.

Proof. For (1). If $U = X_f = X_g$, it suffices to show $A_f = A_g$. Note that $X_f = X_g$ if and only if $r(f) = r(g)$, so there exists $a, b \in A$ and $m, n \geq 0$ such that

$$f = ag^n, g = bf^m$$

So $f/1$ is a unit in A_g, since

$$\frac{f}{1}\frac{1}{ag^n} = 1 \in A_g$$

Thus for any $k \geq 0$, we have f^k is a unit in A_g, so by universal property of A_f, there exists a homeomorphism $\phi\colon A_f \to A_g$. Similarly there exists $\psi\colon A_g \to A_f$. Note that localization is unique with respect to a unique morphism, thus $\psi \circ \phi$ is identity so is $\phi \circ \phi$. So $A_f \cong A_g$, if $X_f = X_g$.

For (2). If $X_g \subseteq X_f$, thus $V(r(f)) \subseteq V(r(g))$, which implies $f \in r(g)$. So there exists $n > 0$ and $u \in A$ such that $g^n = uf$.

For (3). Take $f = g$ and $n = 1, u = 1$, it's clear ρ is identity.

For (4). If $U = X_f, U' = X_g, U'' = X_h$, and $g^n = uf, h^k = vg$, thus $h^{kn} = v^n g^n = v^n uf$. So

$$\frac{a}{f^m} \mapsto \frac{au^m}{g^{mn}} \mapsto \frac{au^m v^{mn}}{h^{kmn}}$$

This shows the diagram commutes.

For (5). For $\mathfrak{p} \in X_f$, that is $f \notin \mathfrak{p}$, so $\{f^k\}_{k\geq 0} \subseteq A - \mathfrak{p}$, thus there is a natural inclusion $\phi_u\colon A(U) = A_f \to A_{\mathfrak{p}}$. So by universal property of direct limit we have there is a mapping $\phi\colon \varinjlim A(U) \to A_{\mathfrak{p}}$, and it's injective since μ_U is injective for any U. To see ϕ is surjective: For any $a/f \in A_{\mathfrak{p}}$, we have

$\mathfrak{p} \in X_f = U$, thus consider $\mu_U(a/f) \in \varinjlim A(U)$, it's clear $\phi \circ \mu_U(a/f) = a/f$ since $\phi \circ \mu_U = \phi_U$, and ϕ_U is natural inclusion. $\square$

Exercise 3.6.24. Show that the presheaf of Exercise 3.5.23 has the following property. Let $(U_i)_{i \in I}$ be a covering of X by basic open sets. For each $i \in I$ let $s_i \in A(U_i)$ be such that, for each pair of indices i, j, the images of s_i and s_j in $A(U_i \cap U_j)$ are equal. Then there exists a unique $s \in A(= A(X))$ whose image in $A(U_i)$ is s_i, for all $i \in I$. (This essentially implies that the presheaf is a sheaf.)

Proof. Existence: Suppose there are $U_i = X_{f_i}$ that cover X, then there is a finite linear combination

$$1 = \sum_{i=1}^{m} c_i f_i$$

So $(f_1, \ldots, f_m) = (1)$. Note that $X_f = X_{f^n}$ for any $n > 0$, thus we have the similar equation with f_i^n replacing f_i, with c_i depending on n. Suppose we have $s_i \in A_{f_i}$ such that for each i, j the image of s_i, s_j in $A_{f_i f_j}$ coincide. Represent s_i as $a_i/f_i^{n_i}$. For finite $s_1, \ldots, s_m$, we may assume all n_i are equal to n. Then for each pair i, j we have

$$s_i|_{A_{f_i f_j}} - s_j|_{A_{f_i f_j}} = \frac{a_i f_i^n}{(f_i f_j)^n} - \frac{a_j f_j^n}{(f_i f_j)^n} = 0$$

In other words, there exists some power of $f_i f_j$, denoted by $(f_i f_j)^l$ such that

$$a_i f_i^l f_j^{l+n} = a_j f_j^l f_i^{n+l}$$

Since $s_i = a_i f_i^l / f_i^{l+n}$ in A_{f_i} and $s_j = a_j f_j^l / f_j^{l+n}$ in A_{f_j}, this shows by replacing $a_i f_i^l$ with a_i and $l + n$ with n, that for each of the finite number of pairs $1 \leq i, j \leq m$, we can choose the form $s_i = a_i / f_i^n$ with big enough n such that $f_j^n a_i = f_i^n a_j$. Then choose c_i such that $1 = \sum c_i f_i^n$ and consider

$$s = \sum_{i=1}^{m} c_i a_i$$

Claim $s/1 = a_i/f_i^n$ in A_{f_i}. Indeed, note that

$$f_i^n s = \sum_{j=1}^{m} c_j f_i^n a_j = \sum_{j=1}^{m} c_j f_j^n a_i = (\sum_{j=1}^{m} c_j f_j^n) a_i = a_i$$

This shows existence.

Uniqueness. It suffices to show for if $\{X_{f_i}\}_{i=1}^m$ covers X and $s \in A$ such that $s/1 = 0 \in A_{f_i}$ for all $i = 1, \ldots, m$, then $s = 0$. Note that $s/1 = 0 \in A_{f_i}$ implies there exists n_i such that $f_i^{n_i} s = 0$, Without lose of generality we may assume all n_i are equal to n since there are only finitely many. Thus $f_i^n s = 0$ for all $i = 1, \ldots, m$. But there exists c_i such that $\sum_{i=1}^m c_i f_i^n = 1$, which implies

$$s = \sum_{i=1}^{n} c_i f_i^n s = 0$$

$\square$

Exercise 3.6.25. Let $f\colon A \to B, g\colon A \to C$ be ring homomorphisms and let $h : A \to B \otimes_A C$ be defined by $h(x) = f(x) \otimes g(x)$. Let X, Y, Z, T be the prime spectra of A, B, C, $B \otimes_A C$ respectively. Then $h^*(T) = f^*(Y) \cap g^*(Z)$

Proof. Let $\mathfrak{p} \in X$, and $k = k(\mathfrak{p})$ be the residue field at $\mathfrak{p}$. By Exercise 3.5.21, the fiber of $h^{*-1}(\mathfrak{p})$ is the spectrum of $(B \otimes_A C) \otimes_A k \cong (B \otimes_A k) \otimes_k (C \otimes_A k)$. Hence $\mathfrak{p} \in h^*(T)$ if and only if $(B \otimes_A k) \otimes_k (C \otimes_A k) \neq 0$ if and only $(B \otimes_A k) \neq 0$ and $(C \otimes_A k) \neq 0$ if and only if $p \in f^*(Y) \cap g^*(Z)$. $\square$

Exercise 3.6.26. Let $(B_\alpha, g_{\alpha\beta})$ be a direct system of rings and B the direct limit. For each α, let $f_\alpha : A \to B_\alpha$ be a ring homomorphism such that $g_{\alpha\beta} \circ f_\alpha = f_\beta$ whenever $\alpha \leqslant \beta$ (the B_α form a direct system of A-algebras). The f_α induce $f\colon A \to B$. Show that

$$f^*(\operatorname{Spec} B) = \bigcap_\alpha f_\alpha^*(\operatorname{Spec}(B_\alpha)),$$

Proof. Let $\mathfrak{p} \in \operatorname{Spec}(A)$. Then $f^{*-1}(\mathfrak{p})$ is the spectrum of

$$B \otimes_A k(\mathfrak{p}) \cong \varinjlim (B_\alpha \otimes_A k(\mathfrak{p}))$$

since tensor products commute with direct limits. By Exercise 2.8.21 of Chapter 2 it follows that $f^{*-1}(\mathfrak{p}) = \varnothing$ if and only if $B_\alpha \otimes_A k(\mathfrak{p}) = 0$ for some α, i.e., if and only if $f_\alpha^{*-1}(\mathfrak{p}) = \varnothing$. This completes the proof. $\square$

Exercise 3.6.27. Constructible topology

(1) Let $f_\alpha : A \to B_\alpha$ be any family of A-algebras and let $f\colon A \to B$ be their tensor product over A. Then

$$f^*(\operatorname{Spec} B) = \bigcap_\alpha f_{\alpha^*}^* (\operatorname{Spec}(B_\alpha)).$$

(2) Let $f_\alpha : A \to B_\alpha$ be any finite family of A-algebras and let $B = \prod_\alpha B_\alpha$. Define $f\colon A \to B$ by $f(x) = (f_\alpha(x))$. Then $f^*(\operatorname{Spec} B) = \bigcup_\alpha f_\alpha^* (\operatorname{Spec}(B_\alpha))$.
(3) Hence the subsets of $X = \operatorname{Spec} A$ of the form $f^*(\operatorname{Spec} B)$, where $f\colon A \to B$ is a ring homomorphism, satisfy the axioms for closed sets in a topological space. The associated topology is the constructible topology on X. It is finer than the Zariski topology.
(4) Let X_C denote the set X endowed with the constructible topology. Show that X_C is quasi-compact.

Proof. For (1). Recall the definition of tensor product of any family of A-algebras B_α indexed by I in Exercise 2.8.23. It's a direct limit of direct system $\{B_J, i_{JJ'}\}$ where J is a finite subset of I, $i_{JJ'}$ is natural inclusion if $J \subseteq J'$. Use this direct system together with Exercise 3.5.25, 3.5.26 to conclude.

For (2). Let $\mathfrak{p} \in \operatorname{Spec} A$ and $k(\mathfrak{p})$ is the residue field of $\mathfrak{p}$. Then $f^{*-1}(\mathfrak{p})$ is the spectrum of

$$B \otimes_A k(\mathfrak{p}) \cong \prod_{\alpha} B_\alpha \otimes_A k(\mathfrak{p})$$

isomorphism here holds since tensor product commutes with direct limit, and product is a special direct limit. Thus $B \otimes_A k(\mathfrak{p}) \neq 0$ if and only if there exists some α such that $B_\alpha \otimes_A k(\mathfrak{p})$.

For (3). It suffices to show every closed subset in sense of Zariski is closed in sense of constructible, and it's clear, since any Zariski closed subset takes the form $V(\mathfrak{a})$ for some ideal $\mathfrak{a}$ of A, and that's homeomorphic to $f^*(\operatorname{Spec}(A/\mathfrak{a}))$, where $f\colon A \to A/\mathfrak{a}$ is natural projection.

For (4). Let $\{U_\alpha\}_{\alpha \in I}$ be an open cover of X, that's equivalent to $\bigcap_{\alpha \in I} C_\alpha = \varnothing$, where $C_\alpha = X - U_\alpha$. Since C_α are closed, we may write $C_\alpha = f_\alpha^*(\operatorname{Spec} B_\alpha)$, where $f_\alpha : A \to B_\alpha$ is some ring homomorphism. Note that $\bigcap C_\alpha$ is equal to the spectrum of tensor product of B_α, this spectrum is empty implies this tensor product is a zero ring. So by property of direct limit there exists some finite subset $J \subseteq I$ such that $B_J = 0$. If we write $f_J : A \to B_J$, then

$$\bigcap_{\alpha \in J} C_\alpha = \bigcap_{\alpha \in J} f_\alpha^*(\operatorname{Spec} B_\alpha) = f_J^*(\operatorname{Spec} B_J) = 0$$

This implies X with constructible topology is quasi-compact equipped. □

Exercise 3.6.28. Continuation of Exercise 3.5.27.

(1) For each $g \in A$, the set X_g is both open and closed in the constructible topology.
(2) Let C' denote the smallest topology on X for which the sets X_g are both open and closed, and let $X_{C'}$ denote the set X endowed with this topology. Show that $X_{C'}$ is Hausdorff.
(3) Deduce that the identity mapping $X_C \to X_{C'}$ is a homeomorphism. Hence a subset E of X is of the form $f^*(\operatorname{Spec} B)$ for some $f\colon A \to B$ if and only if it is closed in the topology C'.
(4) The topological space X_C is compact, Hausdorff and totally disconnected.

Proof. For (1). It's clear X_f is a open set of constructible topology, since it's a Zariski open set, and constructible topology is finer. It's also a closed subset of constructible topology, since $X_f = f*(\operatorname{Spec} A_f)$ where $f\colon A \to A_f$ is canonical mapping.

For (2). Let $\mathfrak{p}, \mathfrak{q}$ be two distinct points of X. Without lose of generality we may assume $\mathfrak{p} \not\subseteq \mathfrak{q}$, so there exists $f \in \mathfrak{p}$ such that $f \notin \mathfrak{q}$, then $\mathfrak{q} \in X_f$ and $\mathfrak{p} \in X - X_f$. But X_f is both closed and open, this completes the proof.

For (3). It's clear identity mapping is bijective and continuous, since there are more open sets in X_C. To see it's closed, just a trick of point topology: For closed subset Z of X_C, it's compact since X_C is quasi-compact, then

$f(Z)$ is compact in $X_{C'}$. However, compact subset of a Hausdorff space is closed, this completes the proof.

For (4). We already know X_C is quasi-compact, and $X_{C'}$ is Hausdorff and totally disconnected is clear. □

Exercise 3.6.29. Let $f\colon A \to B$ be a ring homomorphism. Show that $f^* : \operatorname{Spec} B \to \operatorname{Spec} A$ is a continuous closed mapping for the constructible topology.

Proof. It's clear to see f^* is closed: For any closed subset $g^*(\operatorname{Spec} B_\alpha)$ of $\operatorname{Spec} B$, where $g\colon B \to B_\alpha$ is ring homomorphism, we have $f^*(g^*(\operatorname{Spec} B_\alpha)) = (g \circ f)^*(\operatorname{Spec} B_\alpha)$, where $g \circ f\colon A \to B_\alpha$ is a ring homomorphism, so it's closed in $\operatorname{Spec} A$.

To see f^* is continuous, since we know constructible topology is the smallest topology such that X_g is both open and closed, thus X_g is a topology basis of $\operatorname{Spec} A$. Furthermore, $f^{*-1}(X_g) = X_{f(g)}$, which is open in $\operatorname{Spec} B$. □

Exercise 3.6.30. Show that the Zariski topology and the constructible topology on $\operatorname{Spec} A$ are the same if and only if $A/\mathfrak{N}$ is absolutely flat.

Proof. From Exercise 3.5.11, we know that $A/\mathfrak{N}$ is absolutely flat if and only if $\operatorname{Spec} A$ is Hausdorff. So it suffices to show $\operatorname{Spec} A$ is Hausdorff if and only if Zariski topology coincides with constructible topology.

One direction is clear since constructible topology is Hausdorff. Conversely, if Zariski topology is Hausdorff, consider the identity mapping $i : X_C \to X$, here we use X_C to denote $X = \operatorname{Spec} A$ equipped with constructible topology. It's clear identity mapping is bijective and continuous, since X_C has more open sets. Furthermore, it's closed since X is Hausdorff, a trick we have mentioned before. □

4. Primary decomposition

4.1. Basic definitions.

Definition 4.1.1 (primary ideal)**.** An ideal $\mathfrak{q}$ in a ring A is primary if and only if $xy \in \mathfrak{q}$ implies either $x \in \mathfrak{q}$ or $y^n \in \mathfrak{q}$ for some $n > 0$.

Remark 4.1.1. It's easy to see $\mathfrak{q}$ is a primary ideal if and only if $A/\mathfrak{q} \neq 0$ and every zero divisor in $A/\mathfrak{q}$ is nilpotent. Indeed, if $xy \in \mathfrak{q}$ and $x \notin \mathfrak{q}$, so y is a zero divisor in $A/\mathfrak{q}$ and thus $y^n \in \mathfrak{q}$ since y is nilpotent in $A/\mathfrak{q}$, that is $\mathfrak{q}$ is primary prime. Conversely, for a zero divisor y of $A/\mathfrak{q}$, there exists $x \neq 0 \in A/\mathfrak{q}$ such that $xy \in \mathfrak{q}$. So we have $y^n \in \mathfrak{q}$ for some $n > 0$, which implies y is nilpotent in $A/\mathfrak{q}$.

Proposition 4.1.1. Let $\mathfrak{q}$ be a primary ideal in a ring A. Then $r(\mathfrak{q})$ is the smallest prime ideal containing $\mathfrak{q}$.

Proof. It suffices to show $\mathfrak{p} = r(\mathfrak{q})$ is prime by definition. □

Remark 4.1.2. If $\mathfrak{p} = r(\mathfrak{q})$ for some primary ideal $\mathfrak{q}$, then $\mathfrak{q}$ is said to be $\mathfrak{p}$-primary.

The prototype of primary ideal is the prime-power in $\mathbb{Z}$: Since $\mathbb{Z}$ is a unique factorization domain, any integer can be decomposed as a product of prime-powers. But this fails for general rings, and primary ideal is a generalization of prime-power in $\mathbb{Z}$ in some sense.

However, prime-power and primary ideal are not related so closely in general rings, which can be seen in the following examples.

Example 4.1.1. Let $A = k[x, y]$ and $\mathfrak{q} = (x, y^2)$. Then $A/\mathfrak{q} \cong k[y]/(y^2)$. Every zero divisor must be a multiplies of y thus nilpotent, so $\mathfrak{q}$ is primary, and its radical is (x, y). Note that

$$\mathfrak{p}^2 \subset \mathfrak{q} \subseteq \mathfrak{p}$$

so as we can see, a primary ideal may not be a prime-power.

Example 4.1.2. Let $A = k[x, y, z]/(xy - z^2)$ and let $\overline{x}, \overline{y}, \overline{z}$ denote the image of x, y, z in A. Then $\mathfrak{p} = (\overline{x}, \overline{z})$ is a prime ideal since $A/\mathfrak{p} = k[y]$, but $\mathfrak{p}^2$ is not primary. Indeed, consider $\overline{xy} = \overline{z}^2 \in \mathfrak{p}^2$, but $x \notin \mathfrak{p}^2$ and $\overline{y} \notin r(\mathfrak{p}^2) = \mathfrak{p}$. This implies a prime power may not be primary.

Proposition 4.1.2. If $r(\mathfrak{a})$ is maximal, then $\mathfrak{a}$ is primary. In particular, the powers of a maximal ideal $\mathfrak{m}$ is $\mathfrak{m}$-primary.

Proof. Let $r(\mathfrak{a}) = \mathfrak{m}$. The image of $\mathfrak{m}$ in $A/\mathfrak{a}$ is the nilradical of $A/\mathfrak{a}$. Note that $\mathfrak{m}$ is still a maximal ideal (thus prime) in $A/\mathfrak{a}$ and nilradical is the intersection of all prime ideals, we know that $A/\mathfrak{a}$ only has one prime ideal $\mathfrak{m}$. Hence every element of $A/\mathfrak{a}$ is either a unit or nilpotent, and so every zero-divisor of $A/\mathfrak{a}$ is nilpotent. □

Lemma 4.1.1. If $\mathfrak{q}_i, 1 \leq i \leq n$ are $\mathfrak{p}$-primary, then $\mathfrak{q} = \bigcap_{i=1}^n \mathfrak{q}_i$ is $\mathfrak{p}$-primary.

Lemma 4.1.2. Let $\mathfrak{q}$ be a $\mathfrak{p}$-primary ideal, x an element of A. Then

(1) If $x \in \mathfrak{q}$ then $(\mathfrak{q} : x) = (1)$.
(2) If $x \notin \mathfrak{q}$ then $(\mathfrak{q} : x)$ is $\mathfrak{p}$-primary.
(3) If $x \notin \mathfrak{p}$, then $(\mathfrak{q} : x) = \mathfrak{q}$.

Definition 4.1.2 (primary decomposition)**.** A primary decomposition of an ideal $\mathfrak{a}$ in A in an expression of $\mathfrak{a}$ as a finite intersection of primary ideals:

$$\mathfrak{a} = \bigcap_{i=1}^{n} \mathfrak{q}_i$$

Remark 4.1.3. Here are some remarks:

(1) In general such primary decomposition may not exhibits. An ideal $\mathfrak{a}$ is decomposable if it has a primary decomposition.
(2) By Lemma 4.1.1, we may assume the $r(\mathfrak{q}_i)$ are all distinct. We can also assume $\mathfrak{q}_i \not\supseteq \bigcap_{j\neq i} \mathfrak{q}_j$, since we can omit such superfluous terms. Such primary decomposition is said to be minimal.

Theorem 4.1.1 (first uniqueness theorem)**.** Let $\mathfrak{a}$ be a decomposable ideal and let $\mathfrak{a} = \bigcap_{i=1}^{n} \mathfrak{q}_i$ be a minimal primary decomposition of $\mathfrak{a}$. Let $\mathfrak{p}_i = r(\mathfrak{q}_i)$. Then $\mathfrak{p}_i$ are precisely the prime ideals which occur in the set of ideals $r(\mathfrak{a} : x)$, and hence are independent of the particular decomposition of $\mathfrak{a}$.

Remark 4.1.4. Consider $A/\mathfrak{a}$ as an A-module, then $\mathfrak{p}_i$ are precisely the prime ideals which occur as radical of annihilators of elements of $A/\mathfrak{a}$.

Example 4.1.3. 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 since $\mathfrak{p}_2$ is maximal. So prime ideals occurring in the decompositions are $\mathfrak{p}_1$ and $\mathfrak{p}_2$. Note that here $\mathfrak{p}_1 \cap \mathfrak{p}_2$, thus $r(\mathfrak{a}) = \mathfrak{p}_1 \cap \mathfrak{p}_2 = \mathfrak{p}_2$.

Remark 4.1.5. Note that primary decomposition may not be unique, which can be seen from Example 4.1.1, we have

$$(x^2, xy) = (x) \cap (x, y)^2 = (x) \cap (x^2, xy)$$

Definition 4.1.3 (minimal/isolated prime ideal)**.** For an decomposable ideal $\mathfrak{a}$ with associated prime ideals $\{\mathfrak{p}_1, \dots, \mathfrak{p}_n\}$, minimal elements of associated primes are called minimal prime ideals or isolated prime ideals belonging to $\mathfrak{a}$. The others are called embedded prime ideals.

Example 4.1.4. In the case of Example 4.1.3, $\mathfrak{p}_1$ is isolated prime ideal and $\mathfrak{p}_2$ is embedded.

Remark 4.1.6. As you can see, $V(\mathfrak{p}_2) \subseteq V(\mathfrak{p}_1)$, and that's why $\mathfrak{p}_2$ is called embedded.

Proposition 4.1.3. Let $\mathfrak{a}$ be a decomposable ideal. Then any prime ideal $\mathfrak{p} \supseteq \mathfrak{a}$ contains a minimal prime ideal belonging to $\mathfrak{a}$, and thus the minimal prime ideals of $\mathfrak{a}$ are precisely the minimal elements in the set all prime ideals containing $\mathfrak{a}$.

Proposition 4.1.4. Let $\mathfrak{a}$ be a decomposable ideal, let $\mathfrak{a} = \bigcap_{i=1}^n \mathfrak{q}_i$ be a minimal primary decomposition, and let $r(\mathfrak{q}_i) = \mathfrak{p}_i$. Then

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

Remark 4.1.7. In general, primary decomposition of zero ideal is quite important, since primary decomposition of any ideal $\mathfrak{a}$ of A can be reduced to the primary decomposition of zero ideal in $A/\mathfrak{a}$.

We have the following observations of primary decomposition of zero ideal:

(1) The set of zero divisor of A is the union of prime ideals belonging to 0. It's clear from above proposition.
(2) The set of nilpotent of A is the intersection of all minimal prime ideals belonging to 0. This can be seen directly from the primary decomposition of zero ideal, since nilradical is radical of zero ideal.

Recall that we have already defined minimal prime ideal, which is closely related to the irreducible components of the spectrum of a ring. In fact, minimal prime ideal we defined before is exactly the minimal prime ideal associated to zero ideal. Indeed, nilradical is the intersection of prime ideals, thus it's the intersection of minimal prime ideals. That maybe why we use the same name.

In particular, if zero ideal do admits a primary decomposition, then there are only finitely many minimal prime ideals, thus there are only finitely many irreducible components of its spectrum, that's Exercise 4.3.1.

4.2. **Second uniqueness theorem.**

Proposition 4.2.1. Let S be a multiplicative closed subset of A, and let $\mathfrak{q}$ be a $\mathfrak{p}$-primary ideal.

(1) If $S \cap \mathfrak{p} \neq \varnothing$, then $S^{-1}\mathfrak{q} = S^{-1}A$.
(2) If $S \cap \mathfrak{p} = \varnothing$, then $S^{-1}\mathfrak{q}$ is $S^{-1}\mathfrak{p}$-primary and its contraction in A is $\mathfrak{q}$.

Proof. For (1). If $s \in S \cap \mathfrak{p}$, then $s^n \in S \cap \mathfrak{q}$ for some $n > 0$, hence $S^{-1}\mathfrak{q}$ contains $s^n/1$, which is a unit in $S^{-1}A$, thus $S^{-1}\mathfrak{q} = S^{-1}A$.

For (2). If $S \cap \mathfrak{p} = \varnothing$, then $s \in S$ such that $as \in \mathfrak{q}$ implies $a \in \mathfrak{q}$. So

$$\mathfrak{q}^{ec} = \bigcup_{s \in S} (\mathfrak{q} : s) \subseteq \mathfrak{q}$$

thus $\mathfrak{q}^{ec} = \mathfrak{q}$. We also know radical commutes with localization, thus $r(\mathfrak{q}^e) = r(S^{-1}\mathfrak{q}) = S^{-1}r(\mathfrak{q}) = S^{-1}\mathfrak{p}$, and $S^{-1}\mathfrak{q}$ is primary since $\mathfrak{q}$ is.

So primary ideals corresponds to primary ideals in the correspondence between ideals in $S^{-1}A$ and contracted ideals in A. □

Notation 4.2.1. For any ideal $\mathfrak{a}$ and any multiplicative closed subset S in A, the contraction in A of the ideal $S^{-1}\mathfrak{a}$ is denoted by $S(\mathfrak{a})$.

Proposition 4.2.2. Let S be a multiplicative closed subset of A and let $\mathfrak{a}$ be a decomposable ideal. Let $\mathfrak{a} = \bigcap_{i=1}^n \mathfrak{q}_i$ be a minimal primary decomposition of $\mathfrak{a}$. Let $\mathfrak{p}_i = r(\mathfrak{q}_i)$ and suppose $\mathfrak{q}_i$ numbered so that S meets $\mathfrak{p}_{m+1}, \dots, \mathfrak{p}_n$ but not $\mathfrak{p}_1, \dots, \mathfrak{p}_m$. Then

$$S^{-1}\mathfrak{a} = \bigcap_{i=1}^{m} S^{-1}\mathfrak{q}_i, \quad S(\mathfrak{a}) = \bigcap_{i=1}^{m} \mathfrak{q}_i$$

Definition 4.2.1 (isolated set)**.** A set Σ of prime ideals belonging to $\mathfrak{a}$ is said to be isolated, if it satisfies the following condition: If $\mathfrak{p}'$ is a prime ideal belonging to $\mathfrak{a}$ and $\mathfrak{p}' \subseteq \mathfrak{p}$ for some $\mathfrak{p} \in \Sigma$, then $\mathfrak{p}' \in \Sigma$.

Let Σ be an isolated set of prime ideals belonging to $\mathfrak{a}$, and let $S = A - \bigcup_{\mathfrak{p}\in\Sigma} \mathfrak{p}$. Then S is a multiplicative closed subset and for each prime ideal $\mathfrak{p}'$ belonging to $\mathfrak{a}$ we have

(1) $\mathfrak{p}' \in \Sigma$ implies $\mathfrak{p}' \cap S = \varnothing$.

(2) $\mathfrak{p}' \notin \Sigma$ implies $\mathfrak{p}' \notin \bigcup_{\mathfrak{p}\in\Sigma} \mathfrak{p}$ and this implies $\mathfrak{p}' \cap S \neq \varnothing$.

Then Proposition 4.2.2 implies

Theorem 4.2.1 (second uniqueness theorem)**.** Let $\mathfrak{a}$ be a decomposable ideal, let $\mathfrak{a} = \bigcap_{i=1}^{n} \mathfrak{q}_i$ be a minimal primary decomposition of $\mathfrak{a}$, and let $\{\mathfrak{p}_{i_1}, \dots, \mathfrak{p}_{i_m}\}$ be an isolated set of prime ideals of $\mathfrak{a}$. Then $\mathfrak{q}_{i_1} \cap \dots \mathfrak{q}_{i_m}$ is independent of decomposition.

Corollary 4.2.1. The isolated primary components are uniquely determined by $\mathfrak{a}$.

4.3. Part of solutions of Chapter 4.

Exercise 4.3.1. If an ideal $\mathfrak{a}$ has a primary decomposition, then $\mathrm{Spec}(A/\mathfrak{a})$ has only finitely many irreducible components.

Proof. See Remark 4.1.7. □

Exercise 4.3.2. If $\mathfrak{a} = r(\mathfrak{a})$, then $\mathfrak{a}$ has no embedded prime ideals.

Proof. Consider any primary decomposition of $\mathfrak{a}$ as $\mathfrak{a} = \bigcap_{i=1}^{n} \mathfrak{q}_i$, where $\mathfrak{q}_i$ is $\mathfrak{p}_i$-primary. Taking radical we have $\mathfrak{a} = \bigcap_{i=1}^{n} \mathfrak{p}_i$. Without lose of generality we can assume $\mathfrak{p}_i \not\subseteq \mathfrak{p}_j$ for any i, j, since such term doesn't make sense when taking intersection. So $\mathfrak{a} = \bigcap_{i=1}^{n} \mathfrak{p}_i$ gives a primary decomposition, and clearly there is no embedded prime ideal. □

Exercise 4.3.3. If A is absolutely flat, every primary ideal is maximal.

Proof. For a primary ideal $\mathfrak{p}$, it suffices to show $A/\mathfrak{p}$ is a field. For any element $x \in A$, there exists $a \in A$ such that $x(1 - ax) = 0$ since A is absolutely flat. Note that $0 \in \mathfrak{p}$, so if $1 - ax \notin \mathfrak{p}$, there exists $n > 0$ such that $x^n \in \mathfrak{p}$ since $\mathfrak{p}$ is primary. But

$$x = ax^2 = a^2x^3 = \cdots = a^{n-1}x^n \in \mathfrak{p}$$

which implies if $\overline{x}$ is not a unit in $A/\mathfrak{p}$, then it must be zero. □

Exercise 4.3.4. In the polynomial ring $\mathbb{Z}[t]$, the ideal $\mathfrak{m} = (2, t)$ is maximal and the ideal $\mathfrak{q} = (4, t)$ is $\mathfrak{m}$-primary, but is not a power of $\mathfrak{m}$.

Proof. It' clear $\mathfrak{m}^2 \subseteq \mathfrak{q} \subseteq \mathfrak{m}$, $\mathfrak{m}$ is maximal and $r(\mathfrak{q}) = \mathfrak{m}$, it suffices to show $\mathfrak{q}$ is primary. Note that

$$\mathbb{Z}[t] = \mathbb{Z}/4\mathbb{Z}$$

Clearly any zero-divisor is a multiplies of 2, so it's nilpotent. □

Exercise 4.3.5. In the polynomial ring $k[x, y, z]$ where k is a field and x, y, z are independent indeterminate, let $\mathfrak{p}_1 = (x, y), \mathfrak{p}_2 = (x, z), \mathfrak{m} = (x, y, z)$.$\mathfrak{p}_1$ and $\mathfrak{p}_2$ are prime, and $\mathfrak{m}$ is maximal. Let $\mathfrak{a} = \mathfrak{p}_1\mathfrak{p}_2$. Show that $\mathfrak{a} = \mathfrak{p}_1 \cap \mathfrak{p}_2 \cap \mathfrak{m}^2$ is a reduced primary decomposition of $\mathfrak{a}$. Which components are isolated and which are embedded?

Proof. It's clear to see $\mathfrak{p}_1, \mathfrak{p}_2$ and $\mathfrak{m}^2$ are primary, and if $\mathfrak{a} = \mathfrak{p}_1 \cap \mathfrak{p}_2 \cap \mathfrak{m}^2$, then embedded prime ideal is $\mathfrak{m}$ and isolated prime ideals are $\mathfrak{p}_1, \mathfrak{p}_2$. So it suffices to check this identity. To see this, we need to write every generator explicitly:

$$\begin{aligned}
\mathfrak{a} = \mathfrak{p}_1\mathfrak{p}_2 &= (x, y)(x, z) = (x^2, xy, xz, yz) \\
\mathfrak{m}^2 &= (x, y, z)(x, y, z) = (x^2, y^2, z^2, xy, xz, yz) \\
\mathfrak{p}_1 \cap \mathfrak{m}^2 &= (x, y) \cap (x^2, y^2, z^2, xy, xz, yz) = (x^2, y^2, xy, xz, yz) \\
\mathfrak{p}_2 \cap \mathfrak{p}_1 \cap \mathfrak{m} &= (x, z) \cap (x^2, y^2, xy, xz, yz) = (x^2, xy, xz, yz)
\end{aligned}$$

This completes the proof. □

Exercise 4.3.6. Let X be an infinite compact Hausdorff space, $C(X)$ the ring of real-valued continuous functions on X. Is the zero ideal decomposable in this ring?

Proof. The answer is no. If zero ideal is decomposable, then there exists only finite minimal prime ideals. Since X is an infinite space, there are infinite many maximal ideals $\mathfrak{m}_x$ in $C(X)$. Clearly every maximal ideal contains some minimal prime ideal. It suffices to show if $x \neq y$, then minimal prime ideals contained in $\mathfrak{m}_x$ and $\mathfrak{m}_y$, denoted by $\mathfrak{p}_x, \mathfrak{p}_y$ are not same.

Since X is compact Hausdorff, thus X is normal. So there exists an open neighborhood U of x such that $x \in U$ and $y \notin \overline{U}$. By Urysohn's lemma, there exist $f \in C(X)$ such that $f(y) = 1, f(\overline{U}) = 0$ and $g \in C(X)$ such that $g(X - U) = 0$ and $g(x) = 1$. Thus $fg = 0 \in \mathfrak{p}_1$ but $g \notin \mathfrak{p}_1$ since $g(x) \neq 0$, so $f \in \mathfrak{p}_1$ since $\mathfrak{p}_1$ is prime. But $f \notin \mathfrak{p}_2$ since $f(y) \neq 0$. Thus $\mathfrak{p}_x \neq \mathfrak{p}_2$. This completes the proof. □

Exercise 4.3.7. Let A be a ring and let $A[x]$ denote the ring of polynomials in one indeterminate over A. For each ideal $\mathfrak{a}$ of A, let $a[x]$ denote the set of all polynomials in $A[x]$ with coefficients in $\mathfrak{a}$.

(1) $\mathfrak{a}[x]$ is the extension of $\mathfrak{a}$ to $A[x]$.
(2) If $\mathfrak{p}$ is a prime ideal in A, then $\mathfrak{p}[x]$ is a prime ideal in $A[x]$.
(3) If $\mathfrak{q}$ is a $\mathfrak{p}$-primary ideal in A, then $\mathfrak{q}[x]$ is a $\mathfrak{p}[x]$-primary ideal in $A[x]$.
(4) If $\mathfrak{a} = \bigcap_{i=1}^n \mathfrak{q}_\mathfrak{i}$ is a minimal primary decomposition in A, then $\mathfrak{a}[x] = \bigcap_{i=1}^n \mathfrak{q}_i[x]$ is a minimal primary decomposition in $A[x]$.

(5) If $\mathfrak{p}$ is a minimal prime ideal of $\mathfrak{a}$, then $\mathfrak{p}[x]$ is a minimal prime ideal of $\mathfrak{a}[x]$.

Proof. We have already seen (1) and (2) before.

For (3). Let's see $r(\mathfrak{q}[x]) = \mathfrak{p}[x]$ firstly: Note that $r(\mathfrak{q}[x])$ is the nilradical of $A[x]/\mathfrak{q}[x] \cong A/\mathfrak{q}[x]$. By Exercise (2) of Exercise 1.8.2, we know that f is nilpotent of $A/\mathfrak{q}[x]$ if and only if all coefficients of f are nilpotent, which is equivalent to $f \in \mathfrak{p}[x]$. To see $\mathfrak{q}[x]$ is primary, consider $A[x]/\mathfrak{q}[x] \cong A/\mathfrak{q}[x]$, still by Exercise 1.8.2, f is a zero-divisor in $A/\mathfrak{q}[x]$ if and only if there exists $a \neq 0 \in A/\mathfrak{q}$ such that $af = 0$, since $\mathfrak{q}$ is primary, this implies every coefficients of f is nilpotent, which is equivalent to f is nilpotent. This completes the proof.

For (4). It's clear $\mathfrak{a}[x] = \bigcap_{i=1}^n \mathfrak{q}_i[x]$ is still a primary decomposition, it suffices to show its minimality.

(1) For $i \neq j$, we have $r(\mathfrak{q}_i[x]) = \mathfrak{p}_i[x] \neq \mathfrak{p}_j[x] = r(\mathfrak{q}_j[x])$.
(2) It's clearly $\mathfrak{q}_i[x] \not\supseteq \bigcap_{j\neq i} \mathfrak{q}_j[x] = (\bigcap_{j\neq i} \mathfrak{q}_i)[x]$.

For (5). If $\mathfrak{p}[x]$ is not a minimal prime ideal of $\mathfrak{a}[x]$, thus there exists $\mathfrak{q}$ such that

$$\mathfrak{a}[x] \subset \mathfrak{q} \subset \mathfrak{p}[x]$$

Then consider its contraction $\mathfrak{a} \subset \mathfrak{q}^c \subset \mathfrak{p}$, we obtain $\mathfrak{q}^c = \mathfrak{p}$ since $\mathfrak{p}$ is a minimal prime ideal of $\mathfrak{a}$. Then

$$\mathfrak{p}[x] = \mathfrak{q}^{ce} \subseteq \mathfrak{q} \subset \mathfrak{p}[x]$$

Thus we have $\mathfrak{q} = \mathfrak{p}[x]$, which implies $\mathfrak{p}[x]$ is minimal. □

Exercise 4.3.8. Let k be a field. Show that in the polynomial ring $k[x_1, \dots, x_n]$ the ideals $\mathfrak{p}_i = (x_1, \dots, x_i)$ where $1 \leq i \leq n$ are prime and all their powers are primary.

Proof. It's clear $\mathfrak{p}_i$ is prime, since we have

$$k[x_1, \dots, x_n]/\mathfrak{p}_i = k[x_{i+1}, \dots, x_n]$$

is a domain. Now let's show for any $l > 0$ we have $\mathfrak{p}_i^l$ is primary. Consider

$$k[x_1, \dots, x_n]/\mathfrak{p}_i^l \cong (k[x_1, \dots, x_i]/\mathfrak{p}_i^l)[x_{i+1}, \dots, x_n]$$

It suffices to show every zero-divisor is a nilpotent one. Recall Exercise 1.8.3, we know that $f \in (k[x_1, \dots, x_i]/\mathfrak{p}_i^l)[x_{i+1}, \dots, x_n]$ is a zero-divisor if and only if there exists $g \neq 0 \in k[x_1, \dots, x_i]/\mathfrak{p}_i^l$ such that $gf = 0$. Then every coefficients of f is a zero divisor of $k[x_1, \dots, x_i]/\mathfrak{p}_i^l$. But $\mathfrak{p}_i$ is maximal in $k[x_1, \dots, x_i]$ thus $\mathfrak{p}_i^l$ is primary in $k[x_1, \dots, x_i]$, we conclude that every coefficients of f is nilpotent thus f is. □

Exercise 4.3.9. In a ring A, let $D(A)$ denote the set of prime ideals $\mathfrak{p}$ which satisfy the following condition: there exists $a \in A$ such that $\mathfrak{p}$ is minimal in the set of prime ideals containing $(0 : a)$. Show that $x \in A$ is a zero divisor $\Leftrightarrow x \in \mathfrak{p}$ for some $\mathfrak{p} \in D(A)$.

Let S be a multiplicative closed subset of A, and identify Spec $\left(S^{-1}A\right)$ with its image in Spec A. Show that

$$D\left(S^{-1}A\right)=D(A)\cap \operatorname{Spec}\left(S^{-1}A\right).$$

If the zero ideal has a primary decomposition, show that $D(A)$ is the set of associated prime ideals of 0 .

Proof. (1) For the first part: If x is a zero-divisor, then there exists $a\in A$ such that $ax=0$, thus $x\in(0:a)\subseteq\mathfrak{p}$ for some $\mathfrak{p}\in D(A)$. Conversely, if $x\in\mathfrak{p}$ for some $\mathfrak{p}\in D(A)$, that is $\mathfrak{p}$ is the minimal prime ideal containing $(0:a)$ for some $a\in A$. Thus $\mathfrak{p}/(0:a)$ is the minimal prime ideal in $A/(0:a)$. Consider $S=A/(0:a)-\mathfrak{p}/(0:a)$, it's a maximal multiplicative closed subset which doesn't contain $0+(0:a)\in A/(0:a)$, thus $S(x^n+(0:a))_{n\geq 0}$ must contain 0, that is there exists $b+(0:a)\in S$ such that

$$0+(0:a)=(b+(0:a))(x^n+(0:a))=bx^n+(0:a)$$

which implies $bx^n\in(0:a)$, that is $abx^n=0$, so x is a zero-divisor. It's a trick we have seen in Exercise 3.5.6.

(2) For $\operatorname{Spec}(S^{-1}A)\cap D(A)\subseteq D(S^{-1}A)$: If we identify $\operatorname{Spec}(S^{-1}A)$ with its image in Spec A, that is for any prime ideal $\mathfrak{q}$, we consider its contraction $\mathfrak{p}=\mathfrak{q}^c$. So any element in $D(A)\cap\operatorname{Spec}(S^{-1}A)$ is prime ideal $\mathfrak{p}$ of A taking form $\mathfrak{p}=\mathfrak{q}^c$ and $\mathfrak{p}\in D(A)$. Since $\mathfrak{p}\in D(A)$, so there exists $a\in A$ such that $\mathfrak{p}$ is minimal prime ideal containing $(0:a)$. Claim $\mathfrak{q}$ is minimal prime ideal containing $(0:a/1)$. Indeed,

(1) $(0:a/1)\subseteq\mathfrak{q}$, since $(0:a)\subseteq\mathfrak{p}$, then we have $S^{-1}(0:a)\subseteq S^{-1}\mathfrak{p}=\mathfrak{q}$. Note that $(0:a)$ is the annihilator of a and localization commutes with annihilator, which implies $S^{-1}(0:a)=S^{-1}\operatorname{ann}(a)=\operatorname{ann}(S^{-1}a)=\operatorname{ann}(a/1)=(0:a/1)$.

(2) $\mathfrak{q}$ is minimal over $(0:a/1)$. If not, there is a $\mathfrak{q}'$ such that $(0:a/1)\subseteq\mathfrak{q}'\subseteq\mathfrak{q}$. By contracting we obtain

$$(0:a)\subseteq(0:a/1)^c\subseteq(\mathfrak{q}')^c\subseteq\mathfrak{q}^c=\mathfrak{p}$$

Thus we have $(\mathfrak{q}')^c=\mathfrak{p}$ since $\mathfrak{p}$ is minimal, that is $\mathfrak{q}'=\mathfrak{q}$, since $\mathfrak{q}=\mathfrak{p}^{ce}$ and the same for $\mathfrak{q}'$.

(3) For $D(S^{-1}A)\subseteq\operatorname{Spec}(S^{-1}A)\cap D(A)$. If $\mathfrak{q}\in D(S^{-1}A)$, that is there exists $a/s\in S^{-1}A$ such that $\mathfrak{q}$ is minimal over $(0:a/s)$, Without lose of generality, we may assume $s=1$ since $(0:a/s)=(0:a/1)$. It suffices to show $\mathfrak{q}^c\in D(A)$. Claim $\mathfrak{q}^c$ is minimal over $(0:a)$. Indeed,

(1) It's clear $(0:a)\subseteq\mathfrak{q}^c$, since $(0:a)\subseteq(0:a/1)^c$.

(2) If $\mathfrak{q}^c$ is not minimal over $(0:a)$, there exists $\mathfrak{p}$ such that $(0:a)\subseteq\mathfrak{p}\subseteq\mathfrak{q}^c$. By extension we have

$$(0:a)^e=(0:a/1)\subseteq\mathfrak{p}^e\subseteq\mathfrak{q}$$

then $\mathfrak{p}^e=\mathfrak{q}$ since $\mathfrak{q}$ is minimal, thus $\mathfrak{p}=\mathfrak{q}^c$.

(4) If zero ideal has a primary decomposition, write $(0)=\bigcap_{i=1}^n\mathfrak{q}_i$ with $\mathfrak{p}_i=\mathfrak{q}_i$. Note that first uniqueness theorem implies that $\mathfrak{p}_i$ are

exactly prime ideals which occur in the set of $r(0:x)$, but if $r(0:x)$ is prime, it's clear minimal over $(0:x)$. So clear $\{\mathfrak{p}_1,\dots,\mathfrak{p}_n\}\subseteq D(A)$. Conversely, if $\mathfrak{p}$ is the minimal prime ideal containing $(0:x)$ for some $x\in A$, thus $\mathfrak{p}=r(0:x)$, so it must be some $\mathfrak{p}_i$. So if zero ideal has a primary decomposition, $D(A)=\{\mathfrak{p}_1,\dots,\mathfrak{p}_n\}$, a finite set.

□

Exercise 4.3.10. For any prime ideal $\mathfrak{p}$ in a ring A, let $S_{\mathfrak{p}}(0)$ denote the kernel of the homomorphism $A\to A_{\mathfrak{p}}$. Prove that

(1) $S_{\mathfrak{p}}(0)\subseteq\mathfrak{p}$.
(2) $r\left(S_{\mathfrak{p}}(0)\right)=\mathfrak{p}\Leftrightarrow\mathfrak{p}$ is a minimal prime ideal of A.
(3) If $\mathfrak{p}\supseteq\mathfrak{p}'$, then $S_{\mathfrak{p}}(0)\subseteq S_{\mathfrak{p}'}(0)$.
(4) $\bigcap_{\mathfrak{p}\in D(A)}S_{\mathfrak{p}}(0)=0$, where $D(A)$ is defined in Exercise 4.3.9.

Proof. For (1). Take $x\in S_{\mathfrak{p}}(0)$, so $x/1=0\in A_{\mathfrak{p}}$, which implies there exists $s\in A-\mathfrak{p}$ such that $sx=0\in\mathfrak{p}$, but $\mathfrak{p}$ is a prime ideal, then $x\in\mathfrak{p}$.

For (2). If $\mathfrak{p}$ is a minimal prime ideal of A, then $S=A-\mathfrak{p}$ is a maximal multiplicative closed subset which do not contain 0, thus for any $x\in\mathfrak{p}$, $0\in S(x^n)_{n>0}$, that is there exists $n>0$ and $s\in S$ such that $sx^n=0$, in other words, $x^n\in S_{\mathfrak{p}}(0)$ or $x\in r(S_{\mathfrak{p}}(0))$. So we obtain $\mathfrak{p}\subseteq r(S_{\mathfrak{p}}(0))$. It's clear we have reverse inclusion from (1). Conversely, if $r(S_{\mathfrak{p}}(0))=\mathfrak{p}$, we need to show $S=A-\mathfrak{p}$ is maximal multiplicative closed subset which doesn't contain 0. If not, then $S\subseteq S'$ for some multiplicative closed subset S' which doesn't contain 0, then take $x\in S'-S$, it's clear $x\in\mathfrak{p}$, thus there exists $n>0$ such that $x^n/1$ is zero in $A_{\mathfrak{p}}$, a contradiction to the fact S' doesn't meet 0.

For (3). If $\mathfrak{p}'\subseteq\mathfrak{p}$, we have $A-\mathfrak{p}\subseteq A-\mathfrak{p}'$. Thus if $x/1$ is zero in $A_{\mathfrak{p}}$, then there exists $s\in A-\mathfrak{p}$ such that $sx=0$, so it's clear to see $x/1$ is also zero in $A_{\mathfrak{p}'}$. Thus $S_{\mathfrak{p}}(0)\subseteq S_{\mathfrak{p}'}(0)$.

For (4). If $x\neq 0\in\bigcap_{\mathfrak{p}\in D(A)}S_{\mathfrak{p}}(0)$, then $(0:x)\neq(1)$, so we must have $(0:x)\subseteq\mathfrak{p}$ for some prime ideal $\mathfrak{p}$. But this implies $sx\neq 0$ for any $s\in A-\mathfrak{p}$, that is $x/1\neq 0\in A_{\mathfrak{p}}$, a contradiction to $x\in S_{\mathfrak{p}}(0)$ □

Exercise 4.3.11. If $\mathfrak{p}$ is a minimal prime ideal of A, show that $S_{\mathfrak{p}}(0)$ is the smallest $\mathfrak{p}$-primary ideal. Let $\mathfrak{a}$ be the intersection of the ideals $S_{\mathfrak{p}}(0)$ as $\mathfrak{p}$ runs through the minimal prime ideals of A. Show that $\mathfrak{a}$ is contained in the nilradical of A. Suppose that the zero ideal is decomposable. Prove that $\mathfrak{a}=0$ if and only if every prime ideal of 0 is isolated.

Proof. For the first part: From (2) of Exercise 4.3.10, we know that $r(S_{\mathfrak{p}}(0))=\mathfrak{p}$ for a minimal prime ideal. Now let's show it's primary and smallest:

(1) It's primary. If $xy\in S_{\mathfrak{p}}(0)$ such that $x\notin S_{\mathfrak{p}}(0)$, then there exists $s\in A-\mathfrak{p}$ such that $sxy=0$, but $x\notin S_{\mathfrak{p}}(0)$ implies $\operatorname{ann}(x)\subseteq\mathfrak{p}$, so $sy\in\mathfrak{p}$, but $s\notin\mathfrak{p}$, so $y\in\mathfrak{p}$, since $\mathfrak{p}$ is prime.
(2) It's smallest. For any $x\in S_{\mathfrak{p}}(0)$ and $\mathfrak{p}$-primary ideal $\mathfrak{q}$, there exists $s\in A-\mathfrak{p}$ such that $sx=0\in\mathfrak{q}$. But $s\notin\mathfrak{p}=r(\mathfrak{q})$ implies $x\in\mathfrak{q}$. Thus $S_{\mathfrak{p}}(0)\subseteq\mathfrak{q}$ for any $\mathfrak{p}$-primary ideal $\mathfrak{q}$.

For the second part: If $\mathfrak{a} = \bigcap_{\mathfrak{p} \text{ is minimal}} S_{\mathfrak{p}}(0)$, then we can see that $r(\mathfrak{a}) = \mathfrak{N}$ by taking radical, thus $\mathfrak{a} \subseteq r(\mathfrak{a}) \subseteq \mathfrak{N}$.

For the third part: If zero ideal is decomposable, that is $0 = \bigcap_{i=1}^{n} \mathfrak{q}_i$ such that $r(\mathfrak{q}_i) = \mathfrak{p}_i$, and all $\mathfrak{p}_i$ are exactly all minimal primes since there is no embedded prime ideal. So $\mathfrak{a} \subseteq \bigcap_{i=1}^{n} \mathfrak{q}_i = 0$, since $S_{\mathfrak{p}}(0)$ is smallest $\mathfrak{p}$-primary ideal. Conversely, if $\mathfrak{a} = 0$, then intersection in the second part gives a primary decomposition of $\mathfrak{p}$, Without lose of generality we may assume any two of them appearing in the intersection won't contain each other. In this decomposition we can see every prime ideal of 0 is isolated from (3) of Exercise 4.3.10.

□

Exercise 4.3.12. Let A be a ring, S a multiplicative closed subset of A. For any ideal $\mathfrak{a}$ let $S(\mathfrak{a})$ denote the contraction of $S^{-1}\mathfrak{a}$ in A. The ideal $S(\mathfrak{a})$ is called the saturation of $\mathfrak{a}$ with respect to S. Prove that

(1) $S(\mathfrak{a}) \cap S(\mathfrak{b}) = S(\mathfrak{a} \cap \mathfrak{b})$
(2) $S(r(\mathfrak{a})) = r(S(\mathfrak{a}))$
(3) $S(\mathfrak{a}) = (1) \Leftrightarrow \mathfrak{a}$ meets S
(4) $S_1\left(S_2(\mathfrak{a})\right) = \left(S_1 S_2\right)(\mathfrak{a})$.

If $\mathfrak{a}$ has a primary decomposition, prove that the set of ideals $S(\mathfrak{a})$ (where S runs through all multiplicative closed subsets of A) is finite.

Proof. (1) and (2) are clear since we know contraction commutes with intersection and radical. (3) is also clear, since $\mathfrak{a}$ meets S if and only if $S^{-1}\mathfrak{a} = (1) \in S^{-1}A$ if and only if $S(\mathfrak{a}) = (1)$.

For (4).

If $\mathfrak{a}$ has a primary decomposition as $\mathfrak{a} = \bigcap_{i=1}^{n} \mathfrak{q}_i$ such that $\mathfrak{p}_i = r(\mathfrak{q}_i)$. Then we have

$$S(\mathfrak{a}) = \bigcap_{i=1}^{n} S(\mathfrak{q}_i)$$

So it suffices to show for each $\mathfrak{p}$-primary ideal $\mathfrak{q}$, it only has finite possibilities. In fact, only two possibilities: From Proposition 4.2 we have:

(1) If $S \cap \mathfrak{p} \neq \varnothing$, then $S(\mathfrak{q}) = (1)$.
(2) If $S \cap \mathfrak{p} = \varnothing$, then $S(\mathfrak{q}) = \mathfrak{q}$

□

Exercise 4.3.13. Let A be a ring and $\mathfrak{p}$ a prime ideal of A. The n-th symbolic power of $\mathfrak{p}$ is defined to be the ideal

$$\mathfrak{p}^{(n)} = S_{\mathfrak{p}}(\mathfrak{p}^n)$$

where $S_{\mathfrak{p}} = A - \mathfrak{p}$. Show that

(1) $\mathfrak{p}^{(n)}$ is a $\mathfrak{p}$-primary ideal.
(2) if $\mathfrak{p}^n$ has a primary decomposition, then $\mathfrak{p}^{(n)}$ is its $\mathfrak{p}$-primary component.
(3) if $\mathfrak{p}^{(m)}\mathfrak{p}^{(n)}$ has a primary decomposition, then $\mathfrak{p}^{(m+n)}$ is its $\mathfrak{p}$-primary component.

(4) $\mathfrak{p}^{(n)} = \mathfrak{p}^n \Leftrightarrow \mathfrak{p}^{(n)}$ is $\mathfrak{p}$-primary.

Proof. For (1). It's easy to see $r(\mathfrak{p}^{(n)}) = \mathfrak{p}$, since

$$r(\mathfrak{p}^{(n)}) = r(S_\mathfrak{p}(\mathfrak{p}^n)) = S_\mathfrak{p}(r(\mathfrak{p}^n)) = S_\mathfrak{p} = \mathfrak{p}$$

To see $\mathfrak{p}^{(n)}$ is primary: Take $xy \in \mathfrak{p}^n$, that is $xy/1 \in S^{-1}\mathfrak{p}^n$, so there exists $s \in S$ such that $sxy \in \mathfrak{p}^n$. If $y \in A - \mathfrak{p} = S$, so $sy \in S$, thus $x/1 \in S^{-1}\mathfrak{p}^n$, which implies $x \in \mathfrak{p}^{(n)}$.

For (2). If $\mathfrak{p}^n$ has a minimal primary decomposition as $\mathfrak{p}^n = \bigcap_{i=1}^n \mathfrak{q}_i$, then we must have

$$S_\mathfrak{p}^{-1}\mathfrak{p}^n = S^{-1}\mathfrak{q}_i$$

for some $\mathfrak{q}_i$. Indeed, since $r(\mathfrak{p}^n) = \mathfrak{p}$, thus prime ideals associated to $\mathfrak{p}^n$ must be $\{\mathfrak{p}, \mathfrak{p}_1, \dots, \mathfrak{p}_{n-1}\}$ such that $\mathfrak{p} \subseteq \mathfrak{p}_i$ for each i. But By Proposition 4.2, we know that if $\mathfrak{p}_i$ meets $S = A - \mathfrak{p}$, then $S^{-1}\mathfrak{q}_i = (1)$, thus $S_\mathfrak{p}^{-1}\mathfrak{p}^n = S^{-1}\mathfrak{q}_i$, for the only $\mathfrak{q}_i$ such that $r(\mathfrak{q}_i) = \mathfrak{p}$. So clearly we have $\mathfrak{p}^{(n)} = S_\mathfrak{p}(\mathfrak{p}^n) = \mathfrak{q}_i$.

For (3).

For (4). Clearly if $\mathfrak{p}^{(n)} = \mathfrak{p}^n$, then $\mathfrak{p}^n$ is $\mathfrak{p}$-primary by (1). Conversely, if $\mathfrak{p}^n$ is $\mathfrak{p}$-primary, and (2) implies $\mathfrak{p}^{(n)}$ is a $\mathfrak{p}$-primary component of $\mathfrak{p}^n$, thus $\mathfrak{p}^{(n)} = \mathfrak{p}^n$. □

Exercise 4.3.14. Let $\mathfrak{a}$ be a decomposable ideal in a ring A and let $\mathfrak{p}$ be a maximal element of the set of ideals $(\mathfrak{a} : x)$, where $x \in A$ and $x \notin \mathfrak{a}$. Show that $\mathfrak{p}$ is a prime ideal belonging to $\mathfrak{a}$.

Proof. Note that first uniqueness theorem implies that prime ideals associated to $\mathfrak{a}$ are exactly prime ideals in the set of $r(\mathfrak{a} : x)$. So if $(\mathfrak{a} : x)$ is a prime ideal, then $r(\mathfrak{a} : x) = (\mathfrak{a} : x)$ is prime, thus it's an associated primes ideal. So it suffices to show maximal element of the set of ideals $(\mathfrak{a} : x)$ is prime. Indeed, first note that since $(\mathfrak{a} : x)$ is maximal, then $(\mathfrak{a} : xy) = (\mathfrak{a} : x)$ for any $xy \notin \mathfrak{a}$. So if $yz \in (\mathfrak{a} : x)$ and $y \notin (\mathfrak{a} : x)$, then $z \in (\mathfrak{a} : xy) = (\mathfrak{a} : x)$, which implies it's prime. □

Exercise 4.3.15. Let $\mathfrak{a}$ be a decomposable ideal in a ring A, let Σ be an isolated set of prime ideals belonging to $\mathfrak{a}$, and let $\mathfrak{q}_\Sigma$ be the intersection of the corresponding primary components. Let f be an element of A such that, for each prime ideal $\mathfrak{p}$ belonging to $\mathfrak{a}$, we have $f \in \mathfrak{p} \Leftrightarrow \mathfrak{p} \notin \Sigma$, and let S_f be the set of all powers of f. Show that $\mathfrak{q}_\Sigma = S_f(\mathfrak{a}) = (\mathfrak{a} : f^n)$ for all large n.

Proof. It's a quite interesting Exercise, for a decomposable ideal, the prime ideals associated to it may contain some embedded prime ideal. So how can we get the intersection of isolated primary components? and that's $\mathfrak{q}_\Sigma$ in the Exercise. And good tool is localization, according to Proposition 4.2.

If $\mathfrak{a} = \bigcap_{i=1}^n \mathfrak{q}_i$ with associated prime ideals $\mathfrak{p}_i$. Without lose of generality, we may assume $\mathfrak{p}_i, 1 \leq i \leq m$ are isolated prime ideals and $\mathfrak{p}_i, m+1 \leq i \leq n$

are embedded ones. Since $S_f \cap \mathfrak{p}_i \neq \varnothing$ by the choice of f, thus we have

$$S_f^{-1}\mathfrak{a} = \bigcap_{i=1}^{m} S_f^{-1}\mathfrak{q}_i$$

and thus

$$S_f(\mathfrak{a}) = \bigcap_{i=1}^{m} \mathfrak{q}_i = \mathfrak{q}_\Sigma$$

□

Exercise 4.3.16. If A is a ring in which every ideal has a primary decomposition, show that every ring of fractions $S^{-1}A$ has the same property.

Proof. Just note that every ideal of $S^{-1}A$ is an extended one. □

Exercise 4.3.17. Let A be a ring with the following property.

(L1) For every ideal $\mathfrak{a} \neq (1)$ in A and every prime ideal $\mathfrak{p}$, there exists $x \notin \mathfrak{p}$ such that $S_\mathfrak{p}(\mathfrak{a}) = (\mathfrak{a} : x)$, where $S_\mathfrak{p} = A - \mathfrak{p}$.

Then every ideal in A is an intersection of (possibly infinitely many) primary ideals.

Proof. Let $\mathfrak{a}$ be an ideal $\neq (1)$ in A, and let $\mathfrak{p}_1$ be a minimal element of the set of prime ideals containing $\mathfrak{a}$. Then $\mathfrak{q}_1 = S_{\mathfrak{p}_1}(\mathfrak{a})$ is $\mathfrak{p}_1$-primary by Exercise 4.3.11, and by assumption we have $\mathfrak{q}_1 = (\mathfrak{a} : x)$ for some $x \notin \mathfrak{p}_1$. We claim that $\mathfrak{a} = \mathfrak{q}_1 \cap (\mathfrak{a} + (x))$. Indeed, $\mathfrak{a} \subseteq \mathfrak{q}_1 \cap (\mathfrak{a} + (x))$, since $\mathfrak{a} \subseteq \mathfrak{q}_1$ and $\mathfrak{a} \subseteq \mathfrak{a} + (x)$. Conversely, take any element $a + bx \in \mathfrak{a} + (x)$, and if it lies in $\mathfrak{q}_1 = (\mathfrak{a} : x)$, we will see $bx^2 \in \mathfrak{a} \subseteq \mathfrak{q}_1$. But $x \notin \mathfrak{p}_1 = r(\mathfrak{q}_1)$ so we have $b \in \mathfrak{q}_1$ since $\mathfrak{q}_1$ is primary, thus $bx \in \mathfrak{a}$, which implies $a + bx \in \mathfrak{a}$, this shows $\mathfrak{q}_1 \cap (\mathfrak{a} + (x)) \subseteq \mathfrak{a}$.

Now consider the following set consisting of ideals

$$\Sigma = \{\mathfrak{b} \mid \mathfrak{b} \cap \mathfrak{q}_1 = \mathfrak{a}, x \notin \mathfrak{p}_1 = r(\mathfrak{q}_1)\}$$

where $\mathfrak{q}_1 = (\mathfrak{a} : x)$. It's not empty since $\mathfrak{a} + (x) \in \Sigma$. So by Zorn lemma there exists a maximal element, denoted by $\mathfrak{a}_1$. Repeat the construction starting with $\mathfrak{a}_1$ and so on. At the n-th stage we have $\mathfrak{a}_1 = \mathfrak{q}_1 \cap \cdots \cap \mathfrak{q}_n \cap \mathfrak{a}_n$, where $\mathfrak{q}_i$ are primary ideals, $\mathfrak{a}_n$ is maximal element in some sets. If at any stage we have $\mathfrak{a}_n = (1)$, the process stops, in this case we do have a primary decomposition of $\mathfrak{a}$, otherwise we just can write $\mathfrak{a}$ as an intersection (maybe infinite) of primary ideals.

So as you can see, some kind of finiteness is crucial in the existence of primary decomposition, and that's exactly what next Exercise or chain condition we will see later talk about. □

Exercise 4.3.18. Consider the following condition on a ring A:

(L2) Given an ideal $\mathfrak{a}$ and a descending chain $S_1 \supseteq S_2 \supseteq \cdots \supseteq S_n \supseteq \cdots$ of multiplicative closed subsets of A, there exists an integer n such that $S_n(\mathfrak{a}) = S_{n+1}(\mathfrak{a}) = \cdots$.

Prove that the following statements are equivalent.
(1) Every ideal in A has a primary decomposition.
(2) A satisfies (L1) and (L2).

Proof. For (1) to (2). If $\mathfrak{a}$ has a minimal primary decomposition $\mathfrak{a}=\bigcap_{i=1}^n \mathfrak{q}_i$ with $r(\mathfrak{q}_i)=\mathfrak{p}_i$.

(L1) For any prime ideal $\mathfrak{p}$, we may assume $\mathfrak{p}_i \subseteq \mathfrak{p}$ for $1 \leq i \leq m$ and $\mathfrak{p}_i \nsubseteq \mathfrak{p}$ for $m+1 \leq i \leq n$. So it's clear to see $S_{\mathfrak{p}}(\mathfrak{a})=\bigcap_{i=1}^m \mathfrak{q}_i$. For any $x \in A$, note that
$$(\mathfrak{a}: x)=(\bigcap_{i=1}^m(\mathfrak{q}_i: x)) \cap(\bigcap_{i=m+1}^n(\mathfrak{q}_i: x))$$
So it suffices to choose x such that $x \notin \mathfrak{p}_i, 1 \leq i \leq m$ and $x \in \mathfrak{q}_i, m+1 \leq i \leq n$. Such x do exists: For any $m+1 \leq i \leq n$, we have $\mathfrak{q}_i \nsubseteq \mathfrak{p}$, since $\mathfrak{p}_i \nsubseteq \mathfrak{p}$, thus there exists $x_i \in \mathfrak{q}_i$ and $x_i \notin \mathfrak{p}$. Let $x=\prod_{i=m+1}^n x_i$ to conclude.

(L2) The set of ideals $S(\mathfrak{a})$ where S runs over all multiplicative closed subsets of A is finite. So for any descending chain of $S_1 \supseteq S_2 \supseteq \cdots \supseteq \ldots$ of multiplicative closed subsets of A, there exists a n such that $S_n(\mathfrak{a})=S_{n+1}(\mathfrak{a})$, otherwise a contradiction to finiteness.

For (2) to (1). With the notation of the proof of Exercise 4.3.17. Let $S_n=S_{\mathfrak{p}_1} \cap \cdots \cap S_{\mathfrak{p}_n}$ then S_n meets $\mathfrak{a}_n$, hence $S_n\left(\mathfrak{a}_n\right)=(1)$, and therefore $S_n(\mathfrak{a})=\mathfrak{q}_1 \cap \cdots \cap \mathfrak{q}_n$. Now use (L2) to implies this construction must terminate after a finite number of steps, that is
$$\mathfrak{q}_1 \cap \cdots \cap \mathfrak{q}_n=\mathfrak{q}_1 \cap \cdots \cap \mathfrak{q}_n \cap \mathfrak{q}_{n+1}$$
for some $n>0$. Then
$$\begin{aligned}
\mathfrak{a} & =\mathfrak{q}_1 \cap \cdots \cap \mathfrak{q}_n \cap \mathfrak{a}_n \\
& =\mathfrak{q}_1 \cap \cdots \cap \mathfrak{q}_n \cap \mathfrak{q}_{n+1} \cap \mathfrak{a}_n \\
& =\mathfrak{q}_1 \cap \cdots \cap \mathfrak{q}_n \cap \mathfrak{q}_{n+1}
\end{aligned}$$
since $\mathfrak{a}_n \subseteq \mathfrak{q}_{n+1}$ by construction. □

Exercise 4.3.19.

Proof. □

Exercise 4.3.20.

Proof. □

Exercise 4.3.21.

Proof. □

Exercise 4.3.22.

Proof. □

Exercise 4.3.23.

Proof. $\square$

Exercise 4.3.24.

Proof. $\square$

5. Integral dependence and Valuations

5.1. **Integral dependence.**

Definition 5.1.1 (integral)**.** Let B be a ring and A a subring of B. An element $x \in B$ is said to be integral over A if x is a root of monic polynomial with coefficients in A.

Definition 5.1.2 (integral mapping)**.** A ring homomorphism $f\colon A \to B$ is called integral, if B is integral over $f(A)$.

Proposition 5.1.1. The following statements are equivalent.
(1) $x \in B$ is integral over A.
(2) $A[x]$ is a finitely generated A-module.
(3) $A[x]$ is contained in a subring C of B such that C is a finitely generated A-module.
(4) There exists a faithfully $A[x]$-module M which is finitely generated as A-module.

Corollary 5.1.1. The set of elements of B which are integral over A is a subring of B containing A.

Definition 5.1.3 (integral closure)**.** Let C denote the set of all elements of B which are integral over A.
(1) If $C = A$, then A is said to be integrally closed in B.
(2) If $C = B$, then B is said to be integral over A.

Definition 5.1.4 (integrally closed)**.** A domain R is called integrally closed domain, if it's integral closed in its field of fractions.

Proposition 5.1.2. If $A \subseteq B \subseteq C$ are rings and if B is integral over A, and C is integral over B, then C is integral over A.

Proposition 5.1.3. Let $A \subseteq B$ be rings, B integral over A.
(1) If $\mathfrak{b}$ is an ideal of B and $\mathfrak{a} = \mathfrak{b}^c$, then $B/\mathfrak{b}$ is integral over $A/\mathfrak{a}$.
(2) If S is a multiplicative closed subset of A, then $S^{-1}B$ is integral over $S^{-1}A$.

5.2. **Going-up.**

Proposition 5.2.1. Let $A \subseteq B$ be integral domains, B integral over A. Then B is a field if and only if A is a field.

Corollary 5.2.1. Let $A \subseteq B$ be rings, B integral over A. Let $\mathfrak{q}$ be a prime ideal of B and $\mathfrak{p}$ is its contraction. Then $\mathfrak{q}$ is maximal if and only if $\mathfrak{p}$ is.

Corollary 5.2.2. Let $A \subseteq B$ be rings, B integral over A. Let $\mathfrak{q}, \mathfrak{q}'$ be prime ideals of B such that $\mathfrak{q} \subseteq \mathfrak{q}'$ but their contractions are same, then $\mathfrak{q} = \mathfrak{q}'$.

Theorem 5.2.1. Let $A \subseteq B$ be rings, B integral over A, and let $\mathfrak{p}$ be a prime ideal of A. Then there exists a prime ideal $\mathfrak{q}$ such that $\mathfrak{q}^c = \mathfrak{p}$.

Theorem 5.2.2 (going-up)**.** Let $A \subseteq B$ be rings, B integral over A. Let $\mathfrak{p}_1 \subseteq \cdots \subseteq \mathfrak{p}_n$ be a chain of prime ideals of A and $\mathfrak{q}_1 \subseteq \cdots \subseteq \mathfrak{q}_m$ where $m < n$ a chain of prime ideals of B such that $\mathfrak{q}_i^c = \mathfrak{p}_i$ for $1 \leq i \leq m$. Then the chain $\mathfrak{q}_1 \subseteq \cdots \subseteq \mathfrak{q}_m$ can be extended to a chain $\mathfrak{q}_1 \subseteq \cdots \subseteq \mathfrak{q}_n$ such that $\mathfrak{q}_i^c = \mathfrak{p}_i$ for $1 \leq i \leq n$.

5.3. **Integrally closed integral domains and Going-down.**

Definition 5.3.1 (integrally closed)**.** An integral domain is said to be integrally closed, if it's integrally closed in its field of fractions.

Proposition 5.3.1. Let A be an integral domain. Then the following statements are equivalent.

(1) A is integrally closed.
(2) $A_{\mathfrak{p}}$ is integrally closed for each prime ideal $\mathfrak{p}$.
(3) $A_{\mathfrak{m}}$ is integrally closed for each maximal ideal $\mathfrak{m}$.

Proof. Let K be the field of fractions of A, C the integral closure of A in K. Then A is integrally closed if and only if $i\colon A \to C$ is surjective. But surjectivity is a local property. □

Definition 5.3.2 (integral over an ideal)**.** Let $A \subseteq B$ be rings and let $\mathfrak{a}$ be an ideal of A. An element of B is said to be integral over $\mathfrak{a}$ if it satisfies an equation of integral dependence over A in which all the coefficients lie in $\mathfrak{a}$.

Lemma 5.3.1. Let C be the integral closure of A in B and let $\mathfrak{a}^e$ denote the extension of $\mathfrak{a}$ in C. Then the integral closure of $\mathfrak{a}$ in B is the radical of $\mathfrak{a}^e$.

Proof. If $x \in B$ is integral over $\mathfrak{a}$, it's clearly integral over A, thus $x \in C$. Furthermore, there exists an equation

$$x^n = -(a_1x^{n-1} + \cdots + a_n)$$

with $a_1, \ldots, a_n \in \mathfrak{a}$. Thus $x^n \in \mathfrak{a}^e$, extension of $\mathfrak{a}$ in C, which implies $x \in r(\mathfrak{a}^e)$. Conversely, if $x^n = \sum_{i=1}^n a_ix_i$ for some $n > 0$, where $a_i \in \mathfrak{a}, x_i \in C$. Note that $M = A[x_1, \ldots, x_n]$ is a finitely generated A-module, and clearly $x^nM \subseteq M$, thus by Proposition 2.2.2 we know x^n is integral over $\mathfrak{a}$, so is x. □

Proposition 5.3.2. Let $A \subseteq B$ be integral domains, A integrally closed, and let $x \in B$ be integral over an ideal $\mathfrak{a}$ of A. Then x is algebraic over the field of fractions K of A, and if its minimal polynomial over K is $t^n + a_1t^{n-1} + \cdots + a_n$, then $a_1, \ldots, a_n \in r(\mathfrak{a})$.

Proof. If $x \in B$ is integral over $\mathfrak{a}$, an ideal of A, there exists an equation with minimal degree

$$x^n + a_1x^{n-1} + \cdots + a_n = 0 \tag{5.1}$$

where $a_i \in \mathfrak{a} \subseteq A \subseteq K$. So it's clear x is algebraic over K, and (5.1) is the minimal polynomial of x over K. Let L be a field extension of K which containing all conjugates $x_1, \dots, x_n$ of x, that is roots of (5.1), thus all x_i is integral over $\mathfrak{a}$. By vieta's formula, the coefficients a_i are polynomials in terms of x_i, thus also integral over $\mathfrak{a}$, since x_i's are. In other words, a_i's are in the integral closure of $\mathfrak{a}$ in B.

But A is integrally closed, thus in Lemma 5.3.1 we have $C = A$ and the extension of $\mathfrak{a}$ in C is $\mathfrak{a}$ itself. Thus the integral closure of $\mathfrak{a}$ in B is exactly $r(\mathfrak{a})$. □

Theorem 5.3.1 (going-down)**.** Let $A \subseteq B$ be integral domains, A is integrally closed, B integral over A. Let $\mathfrak{p}_1 \supseteq \cdots \supseteq \mathfrak{p}_n$ be a chain of prime ideals of A, and let $\mathfrak{q}_1 \supseteq \cdots \supseteq \mathfrak{q}_m$ with $m < n$ be a chain of prime ideals of B such that $\mathfrak{q}_i^c = \mathfrak{p}_i$ for $1 \leq i \leq m$. Then the chain $\mathfrak{q}_1 \supseteq \cdots \supseteq \mathfrak{q}_m$ can be extended to a chain $\mathfrak{q}_1 \supseteq \cdots \supseteq \mathfrak{q}_n$ such that $\mathfrak{q}_i^c = \mathfrak{p}_i$ for $1 \leq i \leq n$.

Proof. It suffices to prove the case $m = 1, n = 2$. Consider the following composition

$$A \to B \to B_{\mathfrak{q}_1}$$

If we can show $\mathfrak{p}_2$ is the contraction of a prime ideal of $B_{\mathfrak{q}_1}$, then we complete the proof, since prime ideals of $B_{\mathfrak{q}_1}$ are just those contained in $\mathfrak{q}_1$. Or equivalently, $B_{\mathfrak{q}_1}\mathfrak{p}_2 \cap A = \mathfrak{p}_2$.

Every $x \in B_{\mathfrak{q}_1}\mathfrak{p}_2$ is of the form y/s, where $y \in B\mathfrak{p}_2$ and $s \in B - \mathfrak{q}_1$. By Lemma 5.3.1, we know that the integral closure of $\mathfrak{p}_2$ of B is radical of $B\mathfrak{p}_2$, thus y is integral over $\mathfrak{p}_2$. Hence by Proposition 5.3.2 its minimal equation over K is of the form

$$y^r + u_1 y^{r-1} + \cdots + u_r = 0 \tag{5.2}$$

with $u_1, \dots, u_r \in \mathfrak{p}_2$.

Now suppose that $x \in B_{\mathfrak{q}_1}\mathfrak{p}_2 \cap A$. Then $s = yx^{-1}$ with $x^{-1} \in K$. So that the minimal equation for s over K is obtained by dividing (5.2) by x^r, therefore

$$s^r + v_1 s^{r-1} + \cdots + v_r = 0 \tag{5.3}$$

where $v_i = u_i/x^i$. Consequently

$$x^i v_i = u_i \in \mathfrak{p}_2$$

But $s \in B$ is integral over A, hence each v_i is in A. Suppose $x \notin \mathfrak{p}_2$. Then we have $v_i \in \mathfrak{p}_2$ for each i since $\mathfrak{p}_2$ is prime, hence (5.3) implies $s^r \in B\mathfrak{p}_2 \subseteq B\mathfrak{p}_1 \subseteq \mathfrak{q}_1$, that is $s \in \mathfrak{q}_1$, a contradiction. So $x \in \mathfrak{p}_2$, that is $B_{\mathfrak{q}_1} \cap A \subseteq \mathfrak{p}_2$, reverse inclusion is clear. □

Proposition 5.3.3. Let A be an integrally closed domain, K its field of fractions, L a finite separable algebraic extension of K, B the integral closure of A in L. Then there exists a basis $v_1, \dots, v_n$ of L over K such that $B \subseteq \sum_{j=1}^n Av_j$.

5.4. **Valuation rings.**

Definition 5.4.1 (valuation ring)**.** Let B be an integral domain, K its field of fractions. B is a valuation ring of K if for each $x \neq 0 \in K$, either $x \in B$ or $x^{-1} \in B$.

Proposition 5.4.1. For a valuation ring B.

(1) B is a local ring.
(2) If B' is a ring such that $B \subseteq B' \subseteq K$, then B' is a valuation ring of K.
(3) B is integrally closed.

Proof. For (1). Let $\mathfrak{m}$ be the set of non-units of B, it suffices to check $\mathfrak{m}$ is an ideal. □

Let K be a field, Ω an algebraically closed field. Let Σ be the set of all pairs (A, f), where A is a subring of K and f is a homomorphism of A into Ω. Σ is partially ordered as follows:

$$(A, f) \leq (A', f') \Longleftrightarrow A \subseteq A', f'|_A = f$$

Let (B, g) be a maximal element of Σ. In fact B is a valuation ring of K. Let's show step by step.

Lemma 5.4.1. *B is a local ring with maximal ideal $\mathfrak{m} = \ker g$.*

Lemma 5.4.2. *Let x be a non-zero element of K. Let $B[x]$ be the subring of K generated by x over B, and let $\mathfrak{m}[x]$ be the extension of $\mathfrak{m}$ in $B[x]$. Then either $\mathfrak{m}[x] \neq B[x]$ or $\mathfrak{m}[x^{-1}] \neq B[x^{-1}]$.*

Theorem 5.4.1. *Let (B, g) be a maximal element of Σ. Then B is a valuation ring of the field K.*

Proof. We need to show if $x \neq 0 \in K$, then either $x \in B$ or $x^{-1} \in B$. By Lemma 5.4.2, we may assume $\mathfrak{m}[x] \neq B' = B[x]$. Then $\mathfrak{m}[x]$ is contained in a maximal ideal $\mathfrak{m}'$ of B', and we have $\mathfrak{m}' \cap B = \mathfrak{m}$, since $\mathfrak{m}' \cap B$ is a proper ideal containing $\mathfrak{m}$. Hence embedding $B \to B'$ induces an embedding of $k = B/\mathfrak{m} \to k' = B'/\mathfrak{m}'$. Note that $k' = k[\overline{x}]$ where $\overline{x}$ is the image of x in k' □

Corollary 5.4.1. *Let A be a subring of a field K. Then the integral closure $\overline{A}$ of A in K is the intersection of all the valuation rings of K which contain A.*

Proof. It's clear $\overline{A}$ lies in the intersection of all valuation rings which contain A, since valuation ring is integrally closed. Conversely, if $x \notin \overline{A}$. Then $x \notin A' = A[x^{-1}]$. Hence x^{-1} is a non-unit in A' and is therefore contained in a maximal ideal $\mathfrak{m}'$ of A'. □

Corollary 5.4.2. *Let k be a field and B a finitely generated k-algebra. If B is a field then it is a finite algebraic extension of k.*

5.5. **Part of solutions of Chapter 5.**

Exercise 5.5.1. Let $f\colon A\to B$ be an integral homomorphism of rings. Show that $f^*\colon \operatorname{Spec}B\to\operatorname{Spec}A$ is a closed mapping.

Proof. Firstly, consider $A\xrightarrow{f} f(A)\xrightarrow{i} B$, where i is an inclusion. According to (4) of Exercise 1.8.21, one has $\operatorname{Spec}f(A)$ is homeomorphic to a closed subset of $\operatorname{Spec}A$, thus it suffices to show $i^*\colon \operatorname{Spec}B\to\operatorname{Spec}f(A)$ is a closed mapping, that is we may assume $A\subseteq B$, as a subring.

For an closed sets $V(\mathfrak{b})$ of $\operatorname{Spec}B$, we claim

$$f^*(V(\mathfrak{b}))=V(f^{-1}(\mathfrak{b}))$$

thus it's closed mapping. Indeed, note that $V(\mathfrak{b})=\{\mathfrak{q}\supseteq\mathfrak{b}\mid \mathfrak{q}\text{ is prime}\}$, then it's clear $f^*(\mathfrak{q})=f^{-1}(\mathfrak{q})\supseteq f^{-1}(\mathfrak{b})$ and it's prime, thus $f^*(V(\mathfrak{b}))\subseteq V(f^{-1}(\mathfrak{b}))$. Conversely, for any prime $\mathfrak{p}$ containing $f^{-1}(\mathfrak{b})$, by Theorem 5.2.2, that is going-up theorem, there exists $\mathfrak{q}\supseteq\mathfrak{b}$ such that $\mathfrak{q}^c=\mathfrak{p}$, this implies reverse inclusion. □

Exercise 5.5.2. Let A be a subring of a ring B such that B is integral over A, and let $f\colon A\to\Omega$ be a homomorphism of A into an algebraically closed field Ω. Show that f can be extended to a homomorphism of B into Ω.

Proof. Since Ω is a field, thus $\ker f$ is a prime ideal, denoted by $\mathfrak{p}$. By Theorem 5.2.1, there exists a prime ideal $\mathfrak{q}$ of B such that its contraction is $\mathfrak{p}$ since B is integral over A. Furthermore, Proposition 5.1.3 implies $B/\mathfrak{q}$ is integral over $A/\mathfrak{p}$. So if we extend $\widetilde{f}\colon A/\mathfrak{p}\to\Omega$ to $\widetilde{f}'\colon B/\mathfrak{q}\to\Omega$, we can also extend $f\colon A\to\Omega$ to $f'\colon B\to\Omega$, that is we reduce our case to A,B are integral domains and f is injective.

Let $S=A\backslash\{0\}$, then consider the localization $S^{-1}B$, by (2) of Proposition 5.1.3 one has $S^{-1}B$ is also integral over $\operatorname{Frac}A$. By Proposition 5.2.1 one has $S^{-1}B$ is a field, and it equals to $\operatorname{Frac}B$ since it's contained in $\operatorname{Frac}B$. That's $\operatorname{Frac}B$ is integral over $\operatorname{Frac}A$, which implies $\operatorname{Frac}B$ is an algebraic extension of $\operatorname{Frac}A$. Thus we can firstly extend $f\colon A\to\Omega$ to $\widetilde{f}\colon \operatorname{Frac}A\to\Omega$, namely by $a_1/a_2\mapsto f(a_1)/f(a_2)$, and the following lemma completes the proof.

Lemma 5.5.1. Let $f\colon k\to\Omega$ be a homomorphism of fields, where Ω is an algebraically closed field. For any algebraic extension k', there is a homomorphism $f'\colon k'\to\Omega$ which extends f.

□

Exercise 5.5.3. Let $f\colon B\to B'$ be a homomorphism of A-algebras, and let C be an A-algebra. If f is integral, prove that $f\otimes 1\colon B\otimes_A C\to B'\otimes_A C$ is integral.

Proof. For any element $\sum_{i=1}^n b_i'\otimes c_i\in B'\otimes_A C$, it suffices to check $b_i'\otimes c_i$ is integral over $f(B)\otimes_A C$ for any i, since integral closure is a subring of $B'\otimes_A C$. For $b'\in B'$, there exists a polynomial

$$x^n+a_1x^{n-1}+\cdots+a_n=0$$

such that b' is a root of it, where $a_i \in f(B)$. So for $b' \otimes c \in B' \otimes_A C$, consider the following polynomial

$$x^n + (a_1 \otimes c)x^{n-1} + (a_2 \otimes c^2)x^{n-2} + \cdots + a_n \otimes c^n$$

Then

$$\begin{aligned}(b' \otimes c)^n + (a_1 \otimes c)(b' \otimes c)^{n-1} + \cdots + a_n \otimes c^n &= (b')^n \otimes c^n + a_1 b' \otimes c^n + \cdots + a_n \otimes c^n \\ &= ((b')^n + a_1(b')^{n-1} + \cdots + a_n) \otimes c^n \\ &= 0 \otimes c^n \\ &= 0\end{aligned}$$

Thus $b' \otimes c$ is integral over $f(B) \otimes C$, since for each i, we have $a_i \otimes c \in f(B) \otimes C$. In particular, localization preserves integral, since $S^{-1}B$ can be seen as $S^{-1}A \otimes_A B$. □

Exercise 5.5.4. Let A be a subring of a ring B such that B is integral over A. Let $\mathfrak{n}$ be a maximal ideal of B and let $\mathfrak{m} = \mathfrak{n} \cap A$ be the corresponding maximal ideal of A. Is $B_{\mathfrak{n}}$ necessarily integral over $A_{\mathfrak{m}}$?

Proof. No. Consider the case $A = k[x^2 - 1]$ and $B = k[x]$, where k is a field, and consider the maximal ideal $\mathfrak{n} = (x-1)$ of B. It's clear $\mathfrak{m} = (x-1) \cap k[x^2-1] = (x^2-1)$ since $(x^2-1) \subseteq (x-1)$ in B, and the localization of A with respect to $\mathfrak{m}$ is itself, since the complement of $\mathfrak{m}$ is just k. But $1/(x+1) \in B_{\mathfrak{n}}$ will not satisfy any monic polynomials with coefficients in A, since $1/(x+1)$ never kills $x^2 - 1$. □

Exercise 5.5.5. Let $A \subseteq B$ be rings, B integral over A.

(1) If $x \in A$ is a unit in B, then it is a unit in A.
(2) The Jacobson radical of A is the contraction of the Jacobson radical of B.

Proof. For (1). For $x \in A$, if x is a unit in B, that is there exists $y \in B$ such that $xy = 1$. But B is integral over A, which implies there exists $a_0, \dots, a_{n-1} \in A$ such that

$$y^n + a_{n-1}y^{n-1} + \cdots + a_1 y + a_0 = 0$$

So multiply x^n on each side we obtain

$$1 + a_{n-1}x + \cdots + a_1 x^{n-1} + a_0 x^n = 0$$

so we have

$$-x(a_{n-1} + \cdots + a_0 x^{n-1}) = 1$$

that is x is a unit in A.

For (2). Note that if B is integral over A, then for every maximal ideal $\mathfrak{m}$ of B, we have $\mathfrak{m} \cap A$ is an maximal ideal of A. Furthermore, every prime ideal of A is contracted, so in particular, every maximal ideal of A can be written as $\mathfrak{m} \cap A$ where $\mathfrak{m}$ is a maximal ideal of B. So it's clear to see

$$\mathfrak{R}_B \cap A = \bigcap (\mathfrak{m} \cap A) = \mathfrak{R}_A$$

where intersection runs over all maximal ideals of B. $\square$

Exercise 5.5.6. Let $B_1, \dots, B_n$ be integral A-algebras. Show that $\prod_{i=1}^n B_i$ is an integral A-algebra.

Proof. Firstly, let $\varphi_i\colon A \to B_i$ be the homomorphism making B_i into A-algebra, thus consider $\prod_{i=1}^n \varphi_i\colon A \to \prod_{i=1}^n B_i$, which makes $\prod_{i=1}^n B_i$ into an A-algebra. Now it suffices to show B is an integral A-algebra. Choose an element $b = (b_1, \dots, b_n) \in \prod_{i=1}^n B_i$, then for each b_i we have a polynomial with coefficients in $f_i(A)$, denoted by f_i, then consider

$$f(x_1, \dots, x_n) := (\prod_{i=1}^n f_i(x_1), \dots, \prod_{i=1}^n f_i(x_n))$$

it's clear $f(b) = 0$, this completes the proof. $\square$

Exercise 5.5.7. Let A be a subring of a ring B, such that the set $B \setminus A$ is closed under multiplication. Show that A is integrally closed in B.

Proof. Let $b \in B$ which is integral over A, then it satisfies a monic polynomial, that is

$$b^n + a_{n-1}b^{n-1} + \cdots + a_1 b + a_0 = 0$$

where $a_i \in A$. Note that $b(b^{n-1} + a_{n-1}b^{n-2} + \cdots + a_1) \in A$, thus if $b \notin A$, then we have $b^{n-1} + a_{n-1}b^{n-2} + \cdots + a_1 \in A$, since $B \setminus A$ is multiplicative closed. Repeat above process one has $b + a_1 \in A$, which implies $b \in A$, a contradiction. $\square$

Exercise 5.5.8. Show the following statements:

(1) Let A be a subring of an integral domain B, and let C be the integral closure of A in B. Let f, g be monic polynomials in $B[x]$ such that $fg \in C[x]$. Then f, g are in $C[x]$.
(2) Prove the same result without assuming that B or A is an integral domain.

Proof. For (1). Take a field containing B in which the polynomials f, g split into linear factors: say $f = \prod(x - \xi_i), g = \prod(x - \eta_j)$. Each ξ_i and each η_j is a root of fg, and $fg \in C[x]$, one has ξ_i and η_j is integral over C. By Vieta's formula one has coefficients of f and g are still integral over C, since C is a ring. Furthermore, $f, g \in C[x]$, since C is integrally closed in B. $\square$

Exercise 5.5.9. Let A be a subring of a ring B and let C be the integral closure of A in B. Prove that $C[x]$ is the integral closure of $A[x]$ in $B[x]$.

Proof. If $f \in B[x]$ is integral over $A[x]$, then there exists some $g_i \in A[x]$ such that

$$f^m + g_1 f^{m-1} + \cdots + g_m = 0$$

Consider integer r satisfies the following conditions

(1) r is larger than m and the degrees of $g_1, \dots, g_m$.
(2) If we set $f_1 = f - x^r$, then

Note that in other words (2) is to say

$$f_1^m + h_1 f_1^{m-1} + \cdots + h_m = 0$$

where $h_m = (x^r)^m + g_1(x^r)^{m-1} + \cdots + g_m \in A[x]$. Now apply Exercise 5.5.8 to the polynomials f_1 and $f_1^{m-1} + h_1 f_1^{m-2} + \cdots + h_{m-1}$ to conclude $f_1 \in C[x]$, so is f. $\square$

Exercise 5.5.10. A ring homomorphism $f\colon A \to B$ is said to have the going-up property (resp. the going-down property) if the conclusion of the going-up theorem (resp. the going-down theorem) holds for B and its subring $f(A)$.

(1) Consider the following statements:
  (a) f^* is a closed mapping.
  (b) f has the going-up property.
  (c) Let $\mathfrak{q}$ be any prime ideal of B and let $\mathfrak{p} = \mathfrak{q}^c$. Then $f^*\colon \operatorname{Spec}(B/\mathfrak{q}) \to \operatorname{Spec}(A/\mathfrak{p})$ is surjective.

  Show that $(a) \implies (b) \iff (c)$.

(2) Consider the following statements:
  (a) f^* is an open mapping.
  (b) f has the going-down property.
  (c) For any prime ideal $\mathfrak{q}$ of B, if $\mathfrak{p} = \mathfrak{q}^c$, then $f^*\colon \operatorname{Spec} B_{\mathfrak{q}} \to \operatorname{Spec} A_{\mathfrak{p}}$ is surjective.

Show that $(a) \implies (b) \iff (c)$.

Proof. For (1). $\square$

Exercise 5.5.11. Let $f\colon A \to B$ be a flat homomorphism of rings. Then f has the going-down property.

Proof. $\square$

Exercise 5.5.12. Let G be a finite group of automorphisms of a ring A, and let A^G denote the subring of G-invariants, that is of all $x \in A$ such that $\sigma(x) = x$ for all $\sigma \in G$. Prove that A is integral over A^G.

Proof. $\square$

Exercise 5.5.13. Let S be a multiplicative closed subset of A such that $\sigma(S) \subseteq S$ for all $\sigma \in G$, and let $S^G = S \cap A^G$. Show that the action of G on A extends to an action on $S^{-1}A$, and that $(S^G)^{-1}A^G \cong (S^{-1}A)^G$.

Proof. $\square$

Exercise 5.5.14. In the setting of above Exercises, let $\mathfrak{p}$ be a prime ideal of A^G, and let P be the set of prime ideals of A whose contraction is $\mathfrak{p}$. Show that G acts transitively on P. In particular, P is finite.

Proof. $\square$

Exercise 5.5.15. Let A be an integrally closed domain, K its field of fractions and L a finite Galois extension of K. Let G be the Galois group of L of K and let B be the integral closure of A in L. Show that $\sigma(B) = B$ for all $\sigma \in G$, and $A = B^G$.

Proof. $\square$

Exercise 5.5.16.

Proof. $\square$

Exercise 5.5.17.

Proof. $\square$

Exercise 5.5.18.

Proof. $\square$

Exercise 5.5.19.

Proof. $\square$

Exercise 5.5.20.

Proof. $\square$

Exercise 5.5.21.

Proof. $\square$

Exercise 5.5.22.

Proof. $\square$

Exercise 5.5.23.

Proof. $\square$

Exercise 5.5.24.

Proof. $\square$

Exercise 5.5.25.

Proof. $\square$

Exercise 5.5.26.

Proof. $\square$

Exercise 5.5.27.

Proof. $\square$

Exercise 5.5.28.

Proof. $\square$

Exercise 5.5.29.

Proof. □

Exercise 5.5.30.

Proof. □

Exercise 5.5.31.

Proof. □

6. Chain condition

Proposition 6.0.1. *M is a Noetherian A-module if and only if every submodule of M is finitely generated.*

Proof. If N is a submodule of M, and let Σ denote the set of all finitely generated submodules of N, it's clear Σ is not empty and therefore has a maximal element, say N_0. If $N_0 \neq N$, consider the submodule $N_0 + Ax$ where $x \in N, x \notin N_0$, which is a finitely generated submodule and strictly contains N_0, a contradiction.

Conversely, let $M_1 \subseteq M_2 \subseteq \dots$ be an ascending chain of submodules of M, then $N = \bigcup_{n=1}^{\infty} M_n$ is a submodule of M, hence is finitely generated, which implies the chain is stationary. $\square$

7. Noetherian rings

Recall that a ring A is Noetherian if it satisfies the following three equivalent conditions:

(1) Every non-empty set of ideals in A has a maximal element.
(2) Every ascending chain of ideals in A is stationary.
(3) Every ideal in A is finitely generated.

7.1. **Hilbert's Basis Theorem.**

Theorem 7.1.1 (Hilbert's Basis Theorem)**.** If A is Noetherian, then the polynomial ring $A[x]$ is Noetherian.

Corollary 7.1.1. Let B be a finitely generated A-algebra. If A is Noetherian, then so is B.

Proof. Note that B is a homomorphic image of a polynomial ring $A[x_1, \dots, x_n]$, which is Noetherian by Hilbert's Basis Theorem. □

Proposition 7.1.1. Let $A \subseteq B \subseteq C$ be rings. Suppose that A is Noetherian and C is finitely generated as an A-algebra. If either

(1) C is finitely generated as a B-module.
(2) C is integral over B.

Then B is finitely generated as A-algebra.

Proposition 7.1.2. Let k be a field, E a finitely generated k-algebra. If E is a field then it is a finite algebraic extension of k.

Proof. □

Corollary 7.1.2. Let k be a field, A a finitely generated k-algebra. Let $\mathfrak{m}$ be a maximal ideal of A. Then the field $A/\mathfrak{m}$ is a finite algebraic extension of k. In particular, if k is algebraically closed then $A/\mathfrak{m} \cong k$.

Proof. Just take $E = A/\mathfrak{m}$. □

References

[AM69] Michael Francis Atiyah and I. G. MacDonald. *Introduction to commutative algebra.* Addison-Wesley-Longman, 1969.

Yau Mathematical Sciences Center, Tsinghua University, Beijing, 100084, P.R. China,

Email address: liubw22@mails.tsinghua.edu.cn