NOTE FOR COMMUNICATIVE ALGEBRA

BOWEN LIU

Abstract. It's a lecture note I typed for seminar organized by CUHKSZ and SDU, which is about communicative algebra. This notes will only contain main definitions, propositions and theorems without proof. Readers can refer to Atiyah's Introduction to communicative 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 such that

1. A is an abelian group with respect to addition;
2. Multiplication is associative and distributive over addition;

We shall consider only rings which are communicative:

3. Multiplication is communicative;

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 communicative rings with an identity element. In particular, this 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 1.1.3. Although for a group homomorphism f we automatically have $f(0) = 0$, if we only ask $f(xy) = f(x)f(y)$, 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 ring $xy = 0$ won't implies $x = 0$ or $y = 0$.

Definition 1.1.4 (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 1.1.5. 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)**.** For an ideal $\mathfrak{a}$ 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 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. An ideal $\mathfrak{p}$ is prime if and only if $A/\mathfrak{p}$ is an integral domain; An ideal $\mathfrak{m}$ is maximal if and only if $A/\mathfrak{m}$ is a field.

Proposition 1.4.2. Let $f : A \to B$ be a ring homomorphism, then for a prime ideal $\mathfrak{p}$ in B, then $f^{-1}(\mathfrak{p})$ is a prime ideal in A. Furthermore, we have

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

However, this may fail for maximal ideal. For example

Example 1.4.3. Let $A = \mathbb{Z}, B = \mathbb{Q}$ and $f : \mathbb{Z} \to \mathbb{Q}$ 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 1.4.4 (local ring)**.** A ring with exactly one maximal ideal is called a local ring.

Proposition 1.4.5. For local rings, we have:

1. Let A be a ring and $\mathfrak{m} \neq (1)$ be an ideal of A such that every $x \in A - \mathfrak{m}$ is a unit in A. Then A is local and $\mathfrak{m}$ is its maximal ideal.
2. Let A be a ring and $\mathfrak{m}$ 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)**.** The set of $\mathfrak{N}$ of all nilpotent elements in a ring A is an ideal, called the nilradical of A.

Proposition 1.5.2. The nilradical of A is the intersection of all the prime ideals of A.

Definition 1.5.3 (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 1.5.4. $x \in \mathfrak{R}$ 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 $\mathfrak{a}+\mathfrak{b} = (1)$.

Let A be a ring and $\mathfrak{a}_1, \ldots, \mathfrak{a}_n$ ideals of A. Define a homomorphism

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

Proposition 1.6.2 (Chinese remainder theorem)**.** We have the following statements:

1. If a_i, a_j are coprime whenever $i \neq j$, then $\prod a_i = \bigcap a_i$.
2. ϕ is surjective $\Leftrightarrow$ a_i, a_j are coprime whenever $i \neq j$.
3. ϕ is injective $\Leftrightarrow \bigcap a_i = (0)$.

Proposition 1.6.3. Let $\mathfrak{p}_1, \ldots, \mathfrak{p}_n$ be prime ideals and let $\mathfrak{a}$ be an ideal contained in $\bigcup_{i=1}^n \mathfrak{p}_i$. Then $\mathfrak{a} \subseteq \mathfrak{p}_i$ for some i.

Proof. Prove it by induction on n. It's clear when $n = 1$. If $n > 1$ and the result is true for $n-1$. Assume $\mathfrak{a} \nsubseteq \mathfrak{p}_i$ for each i, then by induction for each i there exists $x_i \in \mathfrak{a}_i$ such that $x_i \in \mathfrak{p}_i$ 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

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

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

Proposition 1.6.4. Let $\mathfrak{a}_1, \ldots, \mathfrak{a}_n$ be ideals and let $\mathfrak{p}$ 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.

Definition 1.6.5 (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 1.6.6. Some properties about ideal quotient:

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 communicative, then 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. So $x \in \bigcap_i (\mathfrak{a}_i : \mathfrak{b})$.

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 1.6.7 (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 1.6.8. Some properties about radical of an ideal:

1. $r(\mathfrak{a}) \supseteq \mathfrak{a}$
2. $r(r(\mathfrak{a})) = r(\mathfrak{a})$
3. $r(\mathfrak{ab}) = r(\mathfrak{a} \cap \mathfrak{b}) = r(\mathfrak{a}) \cap r(\mathfrak{b})$
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

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

Then by (2) we obtain

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

which implies $r(\mathfrak{ab}) = r(\mathfrak{a} \cap \mathfrak{b})$. 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 1.6.9. 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 1.6.8, it suffices to show $r(\mathfrak{a} + \mathfrak{b}) = (1)$. And by (5) of Exercise 1.6.8, 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 $f : A \to B$ 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 explict. $\mathfrak{a}^e$ is the set of all sums $\sum y_i f(x_i)$ 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 $\mathbb{Z} \to \mathbb{Z}[i]$, and consider the extension of prime ideal of $\mathbb{Z}$, the situations is as follows:

1. $(2)^e = ((1+i)^2)$;
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 $\mathbb{Z}[i]$.

Proposition 1.7.3. Properties of contraction and extension:

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 1.7.4. Let $f : A \to B$ 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.**

Problem 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 1.5.4 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. □

Problem 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 $f = a_0 + a_1x + \cdots + a_nx^n \in A[x]$. Prove that

1. f is a unit in $A[x] \Leftrightarrow a_0$ is a unit in A and $a_1, \ldots, a_n$ are nilpotent.
2. f is nilpotent $\Leftrightarrow a_0, a_1, \ldots, a_n$ 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 $(a_0, a_1, \ldots, a_n) = (1)$. Prove that if $f, g \in A[x]$, then fg is primitive $\Leftrightarrow f$ and g are primitive.

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

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

and multiply a_n^r we obtain

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

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 Problem 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; Convesely, if a_0 is unit and $a_1, \ldots, a_n$ is nilpotent. We can imagine that if you power f enough times, then we will obtain unit. Or you can see $\sum_{i=1}^{n} a_i x^i$ is nilpotent, then unit plus nilpotent is also unit.

For (2)[1]. If $a_0, \ldots, a_n$ are nilpotent, then clearly f is; Convesely, if f is nilpotent, then clearly a_n is nilpotent, and we have $f - a_nx^n$ 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; Convesely choose a $g = \sum_{i=0}^{m} b_i x^i$ of least degree m such that $fg = 0$, then we have $a_nb_m = 0$, hence $a_ng = 0$, since $a_ngf = 0$ and has degree less than m. Then consider

$$0 = fg - a_nx^ng = (f - a_nx^n)g$$

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

[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 (4). Note that $(a_0, \ldots, a_n) = 1$ is equivalent to there is no maximal ideal $\mathfrak{m}$ contains $a_0, \ldots, a_n$, 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

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

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. □

Problem 1.8.3. Generalize the results of Problem 1.8.2 to a polynomial ring $A[x_1, \ldots, x_r]$ in several indeterminates.

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.

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 Problem 1.8.2 still holds in this case. □

Problem 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 1.5.4, we have $1 - fg$ is unit for any $g \in A[x]$. Choose g to be x, then by (1) of Problem 1.8.1 we know that all coefficients of f is nilpotent in A, and by (2) of Problem 1.8.1, f is nilpotent. This completes the proof. □

Problem 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; Convesely, 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

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

□

Problem 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 1.5.4 we have $x \notin \mathfrak{R}$, a contradiction. □

Problem 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 Problem: 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 $x \in \mathfrak{R}$. □

Problem 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. Clealy 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 $x \notin \mathfrak{p}_i, y \notin \mathfrak{p}_j$. WLOG 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 1.8.9. 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 1.6.4 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.

□

Problem 1.8.10. 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 $\mathfrak{a}$; Convesely, 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. □

Problem 1.8.11. Let A be a ring, $\mathfrak{N}$ its nilradical. Show that the following 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 1.4.5 to conclude. □

Problem 1.8.12. 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 Problem 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. □

Problem 1.8.13. 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 1.5.4 we must have $e \notin \mathfrak{R} = \mathfrak{m}$, a contradiction. □

Problem 1.8.14 (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 indeterminates 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. □

Problem 1.8.15. 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. □

Problem 1.8.16 (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 $\mathrm{Spec}(A)$.

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 $\mathfrak{a} \subseteq r(\mathfrak{a})$; Convesely, 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 1.6.8, we have $r(\mathfrak{a}\mathfrak{b}) = r(\mathfrak{a}\cap\mathfrak{b}) = r(\mathfrak{a})\cap r(\mathfrak{b})$. Then (1) implies

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

But $V(r(\mathfrak{a}) \cap r(\mathfrak{b})) = V(\mathfrak{a}) \cup V(\mathfrak{b})$. Indeed, clearly $V(\mathfrak{a}) \cup V(\mathfrak{b}) \subseteq V(r(\mathfrak{a}) \cap r(\mathfrak{b}))$; Convesely, 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 1.6.4 tells the answer. □

Problem 1.8.17. 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.

□

Problem 1.8.18. 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 (that is, every open covering of X has a finite subcovering).
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 $X = \mathrm{Spec}(A)$.

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 Problem 1.8.16

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

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 $X_f = X$; Convesely, 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. □

Problem 1.8.19. 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 $X = \mathrm{Spec}(A)$. 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 $\mathrm{Spec}(A) \Leftrightarrow \mathfrak{p}_x$ is maximal;
2. $\overline{\{x\}} = V(\mathfrak{p}_x)$
3. $y \in \overline{\{x\}} \Leftrightarrow \mathfrak{p}_x \subseteq \mathfrak{p}_y$;
4. X is a T_0-space (this means that if x, y are distinct points of X, then 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). 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; Convesely, 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 $x \neq y$. □

Problem 1.8.20. 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 $\mathrm{Spec}(A)$ 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 Problem 1.8.18 we know that $X_f \cap X_g = X_{fg}$, and (2) of Problem 1.8.18 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. □

Problem 1.8.21. 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 $X = \mathrm{Spec}(A)$, then the irreducible components of X are the closed sets $V(\mathfrak{p})$, where $\mathfrak{p}$ is a minimal prime ideal of A

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 $U \cap Y_i \neq \varnothing, V \cap Y_j \neq \varnothing$. WLOG 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 seperating these two points, thus it's not irreducible.

For (4). In fact we can derive from the proof of Problem 1.8.20 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 $V(\mathfrak{p}) \subseteq V(\mathfrak{p}')$. □

Problem 1.8.22 (morphism of spectrum)**.** Let $\phi : A \to B$ be a ring homomorphism. Let $X = \mathrm{Spec}(A)$ and $Y = \mathrm{Spec}(B)$. Then ϕ induces a mapping $\phi^* : Y \to X$. 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 $\phi^{*-1}(V(\mathfrak{a})) = V(\mathfrak{a}^e)$.
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 $\psi : B \to C$ 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 $\phi : A \to B$ 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 $\mathfrak{a}^e \subseteq \mathfrak{b}^{ce} \subseteq \mathfrak{b}$; Convesely, 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 communicative diagram

$$\begin{array}{ccc} \operatorname{Spec} B & \xrightarrow{\phi^*} & V(\mathfrak{a}) \subset X \\ {\scriptstyle \widetilde{\phi}^*}\downarrow & \nearrow_{p^*} & \\ \operatorname{Spec}(A/\mathfrak{a}) & & \end{array}$$

where p^* is defined by mapping $\mathfrak{p}/\mathfrak{a}$ to $\mathfrak{p}$. $p^* : \operatorname{Spec}(A/\mathfrak{a}) \to V(\mathfrak{a})$ 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 $\mathrm{Spec}(A/\mathfrak{a})$, 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 $p^* : \mathrm{Spec}(A/\mathfrak{a}) \to V(\mathfrak{a})$ 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 $\mathrm{Spec}\, A$ are two sets such that one contains another, but closed sets in $\mathrm{Spec}\, B$ are two disjoint sets. □

Problem 1.8.23. Let $A = \prod_{i=1}^n A_i$ be the direct product of rings A_i. Show that $\mathrm{Spec}(A)$ is the disjoint union of open (and closed) subspaces X_i, where X_i is canonically homeomorphic with $\mathrm{Spec}\,(A_i)$. Conversely, let A be any ring. Show that the following statements are equivalent:

1. $X = \mathrm{Spec}(A)$ 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 Problem 1.8.22, we obtain a homeomorphism $X_i = V(\ker p_i) \cong \mathrm{Spec}(A_i)$. We claim $\{X_i\}$ covers A and $X_i \cap X_j$ for distinct i, j. Note that we can write X_i explictly 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 $X = \mathrm{Spec}(A)$ 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 1.8.24. 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. □

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 Problem 1.8.13 implies there is no nontrivial idempotent. □

Problem 1.8.25. Let A be a Boolean ring, and let $X = \mathrm{Spec}(A)$.

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 Problem 1.8.19 we have $x = y$, a contradiction. □

Problem 1.8.26. Let A be a ring. The subspace of $\mathrm{Spec}(A)$ consisting of the maximal ideals of A, with the induced topology, is called the maximal spectrum of A and is denoted by $\mathrm{Max}(A)$.

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 Max $(C(X))$, we have therefore deflned a mapping $\mu : X \to \widetilde{X}$, 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 argumsent) 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. For (1). It's clear.

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 $\mathrm{Spec}(C(X))$.

□

Problem 1.8.27 (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.

As in Exercise 1.2.28, for each $x \in X$ let m_x be the ideal of all $f \in P(X)$ such that $f(x) = 0$; it is a maximal ideal of $P(X)$. Hence, if $\widetilde{X} = \mathrm{Max}(P(X))$, we have defined a mapping $\mu : X \to \widetilde{X}$, 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 surjectite. This is one form of Hilbert's Nullstellensatz (sce Chapter 7).

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

Corollary 1.8.28. 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 clearify 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 we have $\varphi : P(X) \to P(X)/\mathfrak{m} \cong k$, 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 $x = (x_1, \ldots, x_n)$. □

Problem 1.8.29 (regular mapping)**.** Let $f_1, \ldots, f_m$ be elements of $k[t_1, \ldots, t_n]$. They determine a polynomial mapping $\phi : k^n \to k^m$: 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 $\phi : X \to Y$ is said to be regtular 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 $\phi : X \to Y$, 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 $f : P(Y) \to P(X)$, 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. □

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 2.1.2. Equivalently, M is an abelian group with a ring homomorphism $A \to E(M)$, where $E(M)$ is the ring of endomorphisms of the abelian groups.

Remark 2.1.3. If you're familiar with representation theory, a representation of a group G is a group homomorphism $\rho : G \to \mathrm{GL}(V)$, 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 $\widetilde{\rho} : k[G] \to \mathrm{GL}(V)$, where $\widetilde{\rho}$ is obtained from ρ by extending linearly. Convesely, 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 2.1.4 (morphism of modules)**.** Let M, N be A-modules. A mapping $f : M \to N$ is an A-module homomorphism if it's a group homomorphism which commutes with the action of A.

Notation 2.1.5. We use $\mathrm{Hom}(M, N)$ to denote the set of all A-module homomorphisms between M and N.

Remark 2.1.6. There is a natural A-module structure on $\mathrm{Hom}(M, N)$, given by

$$(f + g)(x) := f(x) + g(x)$$
$$(af)(x) := af(x)$$

Definition 2.1.7 (submodule)**.** A submodule M' of M is a subgroup of M which is closed under the action of A.

Definition 2.1.8 (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 2.2.2. 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 2.2.3. 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 2.2.4. 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 2.2.5 (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 2.2.4 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 $M = x^{-1}xM = 0$. □

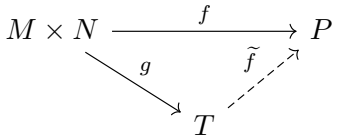
Corollary 2.2.6. Let M be a finitely generated A-module, N a submodule of M, $\mathfrak{a} \subseteq \mathfrak{R}$. Then $M = \mathfrak{a}M + N$ implies $M = N$.

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 2.2.7. 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 $g : M \times N \to T$ such that for any A-module P and any A-bilinear map $f : M \times N \to T$, there exists a unique A-module homomorphism $\widetilde{f}$ such that the following diagram commutes:



Notation 2.3.2. 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 2.3.3. 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

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

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

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

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 2.3.4. 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 2.3.5. 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

$$f_x : N \times P \to (M \otimes_A N) \otimes_B P$$
$$(y, z) \mapsto (x \otimes y) \otimes z$$

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

$$f_x(yb, z) = (x \otimes yb) \otimes z = (x \otimes y)b \otimes z = ((x \otimes y) \otimes z))b = f_x(y, z)b$$
$$f_x(y, zb) = (x \otimes y) \otimes zb = ((x \otimes y) \otimes z))b = f_x(y, z)b$$

So each f_x induces a B-linear map $\widetilde{f_x} : N \otimes_B P \to (M \otimes_A N) \otimes_B P$, by taking $y \otimes z$ to $(x \otimes y) \otimes z$. Allowing x to vary we obtain a bi-additive map $g : A \times (N \otimes_B P) \to (M \otimes_A N) \otimes_B P$. 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 $\widetilde{g} : (M \otimes_A N) \otimes_B P \to M \otimes_A (N \otimes_B P)$, 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 $f : A \to B$ 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 2.1.3. 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.

Convesely, 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 are equivalent:

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

Exercise 2.5.2. If $f : A \to B$ 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 $f : A \to B$.

Remark 2.6.2. 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.

For example, the group-ring $k[G]$ we mentioned before is a k-algebra in fact, and sometimes is called group-algebra.

Definition 2.6.3 (finite algebra)**.** A ring homomorphism $f : A \to B$ is finite, and B is a finite A-algebra, if B is finite generated as A-module.

Definition 2.6.4 (finite generated algebra)**.** A ring homomorphism $f : A \to B$ is finite type, and B is a finitely generated A-algebra, if there exists an A-algebra homomorphism from a polynomial ring $A[t_1, \ldots, t_n]$ onto B.

Remark 2.6.5. 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.

Maybe we will see this later: if B is integral and finite over A, then B is finitely generated over B.

2.7. **Tensor product of Algebras.** Let B, C be two A-algebras, $f : A \to B, g : A \to C$ 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 $\mu : D \times D \to D$ such that

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

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

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

Problem 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. In fact, we can 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

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

it's well-defined and bilinear, then we obtain a linear map $f : \mathbb{Z}/m\mathbb{Z} \otimes \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/\gcd(m,n)\mathbb{Z}$ such that

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

Consider the following map

$$g : \mathbb{Z}/\gcd(m,n)\mathbb{Z} \to \mathbb{Z}/m\mathbb{Z} \otimes \mathbb{Z}/n\mathbb{Z}$$
$$z + \gcd(m,n)\mathbb{Z} \mapsto (z + m\mathbb{Z}) \otimes (1 + n\mathbb{Z})$$

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

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

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

Problem 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. □

Problem 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 Problem 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. □

Problem 2.8.4. Let $M_i (i \in I)$ be any family of A-modules, and let 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 Atiyah's book. □

Problem 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 Problem 2.8.4 we obtain $A[x]$ is flat. □

Problem 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

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

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

From this Problem, hope you can get a feeling of a use of tensor product: a kind of changing domain of coefficients. □

Problem 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 Problem 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 $\mathbb{Q}[x]$. □

Problem 2.8.8. Some properties about flatness:

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. □

Problem 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. □

Problem 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 $u : M \to N$ 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 $\mu(M) = N$. □

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

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

Proof. Let $\mathfrak{m}$ be a maximal ideal of A and let $\phi : A^m \to A^n$ be an isomorphism. Then $1 \otimes \phi : (A/\mathfrak{m}) \otimes A^m \to (A/\mathfrak{m}) \otimes A^n$ is an isomorphism between vector spaces of dimensions m and n over the field $k = A/\mathfrak{m}$. Hence $m = n$. For $\phi : A^m \to A^n$ is surjective, we can use the same method to prove $m \geq n$. But this method fails for the case ϕ is injective, since tensor is just a right exact functor. □

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

Proof. Let $e_1, \ldots, e_n$ be a basis of A^n and choose $u_i \in M$ such that $\phi(u_i) = e_i$ for $1 \leq i \leq n$. 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, thus this exact sequence splits, that is M is the direct sum of $\ker(\phi)$ and the submodule generated by $u_1, \ldots, u_n$. Then $\ker(\phi)$ is finitely generated, since M is. □

Problem 2.8.13. Let $f : A \to B$ 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 $g : N \to N_B$ 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. □

Problem 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 systerm $\mathbf{M} = (M_i, \mu_{ij})$ 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 $\mu : C \to M$ 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. □

Problem 2.8.15. In the situation of Problem 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 arbitary 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 $\{i_k\} \backslash \{i\}$, and denote it by i_l. Note that i_l coordinate vanishes, so either $x_{i_l} = 0$ or $x_{i_l} = \mu_{ii_l}(x_i)$, since $i \leq i_l$ is the only one less than i_l. In later case, we may write the following

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

   Repeat finite many times to conclude.

Now we have

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

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

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

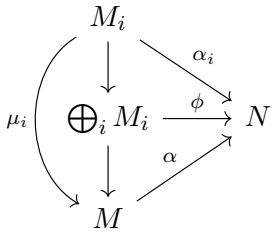
This completes the proof. □

Problem 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 $\alpha : M \to N$ 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 $\phi : \bigoplus_i M_i \to N$, 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 $\alpha : M \to N$ induced by ϕ, and it's clear $\alpha_i = \alpha \circ \mu_i$. What we have done can be shown as follows:



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

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

□

Problem 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 Problem 2.8.15, we know that every element of inverse 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 repeatations, 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

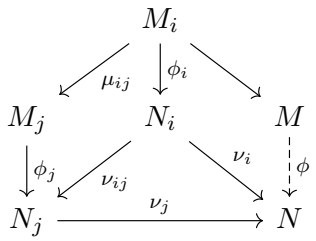
$$\varinjlim M_i = \bigcup_i M_i = M$$

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

Problem 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 $\phi : \mathbf{M} \to \mathbf{N}$ 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 communicative diagram



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

Problem 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[2].

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

Proof. To be explict, 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 Problem 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 $\operatorname{im} f \subseteq \ker g$; Convesely, take $x \in \ker g \subset N$, by Problem 2.8.15 we write it as $\nu_i(x_i)$ for some $x_i \in N_i$. But $g \circ \nu_i(x_i) = g_i(x_i) = 0$ implies $x_i = f_i(y_i)$ for some $y_i \in M_i$. Consider $\mu_i(y_i)$, we have

$$f \circ \mu_i(y_i) = \nu_i \circ f_i(y_i) = \nu_i(x_i) = x$$

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

Problem 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 $\mu_i \otimes 1 : M_i \otimes N \to M \otimes N$, hence by Problem 2.8.16 a homomorphism $\psi : P \to M \otimes N$. 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 $\mu_i \times 1 : M_i \times N \to M \times N$ is the direct limit of the first direct system. Indeed, if $\alpha_i : M_i \times N \to L$ is the direct limit of direct system $(M_i \times N, \mu_{ij} \times 1)$, then there exists a mapping $\alpha : L \to M \times N$ 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 $\mu_i \times 1 : M_i \times N \to M \times N$ is direct limit. We use $\nu_i : M_i \otimes N \to P$ to denote the second direct limit.

A homomorphism between direct system $g_i : M_i \times N \to M_i \otimes N$, that's the canonical bilinear mapping. Passing to the limit we obtain a mapping $g : M \times N \to P$. Clealy g is A-bilinear, since each g_i is a A-blinear one. Hence define a homomorphism $\phi : M \otimes N \to P$. 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. □

Problem 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 Problem 2.8.14. Regarding each A_i as a $\mathbf{Z}$-module we can then form the direct limit $A = \varinjlim A_1$. 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 Problem 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. □

Problem 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 $\alpha_i(a_i) = \alpha_j(\alpha_{ij}(a_i)) \in \varinjlim \mathfrak{R}_i$. □

Problem 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

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

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

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

□

Problem 2.8.24 (Flatness and Tor)**.** If M is an A-module, the following 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. □

Problem 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 arbitary A-module M and consider the long exact sequence induced by this short exact sequence

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

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

Problem 2.8.26. Let N be an A-module. Then N is flat if and only if $\mathrm{Tor}_1^A(A/\mathfrak{a}, N) = 0$ 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

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

It's clear M/M' is finitely generated. Thus N is flat if $\mathrm{Tor}_1^A(M, N) = 0$ 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 $\mathrm{Tor}_1(M, N) = 0$ for all cyclic A-modules M[3]. So by Problem 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 $\mathrm{Tor}_1^A(M, N) = 0$. We can show $\mathrm{Tor}_1^A(M, N) = 0$ for all finitely generated A-modules M by this method. Thus N is flat if $\mathrm{Tor}_1(M, N) = 0$ 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 $\mathrm{Tor}_1^A(A/\mathfrak{a}, N) = 0$ 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 $\mathrm{Tor}_1^A(A/\mathfrak{a}, N) = 0$ for all finitely generated ideal $\mathfrak{a}$. □

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

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

[3] 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

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

the mapping α is injective. Hence $\mathrm{im}(\beta) = 0$, since from the communicativity of the diagram we have $\alpha \circ \beta = 0$. But $\beta = 1 \otimes \pi$, where $\pi : A \to A/(x)$ 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). Let $x \in A$. 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 1.8.12, 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 arbitary A-module N, from Problem 2.8.26 it suffices to check $\mathrm{Tor}_1^A(A/\mathfrak{a}, N) = 0$ 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 $\mathrm{Tor}_1^A(A/\mathfrak{a}, N) = 0$. □

Problem 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 homomorphic 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 Problem 2.8.27 we have A is absolutely flat.

For (3). Consider the surjective mappings $f : A \to B$ 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:

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

That's what we called reduction of a fraction in $\mathbb{Q}$.

In fact, fraction is a method to make all elements in $A\backslash\{0\}$ to be unit, that is you can find a inverse of it. In fact, it's the most economic way to do this.

More generally, we can do the same thing for any multiplicatively closed subset.

Definition 3.1.1 (multiplicatively closed subset)**.** Let A be a ring. A multiplicatively 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 $f : A \to B$ be a ring homomorphism, and $S \subset A$ a multiplicatively closed subset. B is called the localization of A with respect to B, if

1. $f(x)$ is unit for all $x \in S$;
2. If $g : A \to C$ 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 3.1.3. This definition given by 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 explict construction of localization, which is quite similar to what we have done in fraction. Define a relation $\sim$ on $A \times S$ as follows

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

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 multiplicatively 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 classses.

Now let's give a ring structure as follows

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

Exercise 3.1.4. Verify that these definitions are independent of the choices of representatives (a, s) and (b, t), and $S^{-1}A$ is a communicative ring with identity.

There is a natural homomorphism $f : A \to S^{-1}A$, 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 $g : A \to C$ 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 3.1.5. It's natural to ask $f : A \to S^{-1}A$, 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 $f : A \to B$, the extension of $\mathfrak{a}$ is $A\mathfrak{a}$, that is the set of all sums $\sum y_i f(x_i)$ where $x_i \in \mathfrak{a}$ and $y_i \in B$.

In particular, if we take $f : A \to S^{-1}A$ to be localization, and denote this extension by $S^{-1}\mathfrak{a}$. More explictly, for any $y \in S^{-1}\mathfrak{a}$, then 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 multiplicatively 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. $\mathfrak{a} \subset A$ is a contracted ideal if and only if on 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 $x/1 \in \mathfrak{b}$, thus $x \in \mathfrak{b}^c$ and there for $x/s \in \mathfrak{b}^{ce}$. But we already know $\mathfrak{b}^{ce} \subseteq \mathfrak{b}$. Thus $\mathfrak{b} = \mathfrak{b}^{ce}$.

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. $x \in \bigcup_{s\in S}(\mathfrak{a} : s)$.

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 $S^{-1}A$; Convesely, 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 gemeotry and explain the relation between localization and local ring.

Example 3.2.2. Let $\mathfrak{p}$ be a prime ideal of A. Then $S = A - \mathfrak{p}$ is multiplicatively 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 $S^{-1}\mathfrak{p}$, and denote it by $\mathfrak{p}A_\mathfrak{p}$. Indeed, take any arbitary 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 1.4.5, 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.

Remark 3.2.3. 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 $\mathfrak{p}$.

It's a philosophy. In algebraic gemeotry, we regard a prime ideal as a point. You can imagine localization at this prime ideal $\mathfrak{p}$ gemeotrically 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 3.2.4. Let $f \in A$ be an element which is not nilpotent. Consider multiplicatively 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.

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 classses.

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

Yau Mathematical Sciences Center, Tsinghua University, Beijing, 100084, P.R. China,
Email address: liubw22@mails.tsinghua.edu.cn