

# M4P55 Commutative Algebra

Lectured by Prof Alexei Skorobogatov

Typed by David Kurniadi Angdinata

Autumn 2019

**Syllabus**

## Contents

<b>0</b>	<b>Introduction</b>	<b>3</b>
<b>1</b>	<b>Rings and ideals</b>	<b>4</b>
<b>2</b>	<b>Polynomials and formal power series</b>	<b>5</b>
<b>3</b>	<b>Zero-divisors, nilpotents, units</b>	<b>5</b>
<b>4</b>	<b>Prime ideals and maximal ideals</b>	<b>6</b>
<b>5</b>	<b>Nilradical and the Jacobson radical</b>	<b>7</b>
<b>6</b>	<b>Localisation of rings</b>	<b>9</b>
<b>7</b>	<b><math>\text{Spec } R</math> as a topological space</b>	<b>12</b>
<b>8</b>	<b>Determinants</b>	<b>14</b>
<b>9</b>	<b>Modules</b>	<b>14</b>

## 0 Introduction

Lecture 1  
Thursday  
03/10/19

The prerequisites are

- groups,
- rings,
- fields, and
- a solid linear algebra.

This course is good for

- algebraic geometry, and
- algebraic number theory.

The following are books.

- M Reid, Undergraduate commutative algebra, 1995
- M F Atiyah and I G Macdonald, Introduction to commutative algebra, 1969

The following is the structure of the course.

- Generalities on rings, such as ideals, and examples.
- Localisation of rings between a ring  $R$  and the fraction field  $K$  of  $R$ , such as  $\mathbb{Z}$  and  $\mathbb{Q}$ .
- Finiteness conditions of Noetherian rings and Artinian rings.
- Integral closure and normal rings, such as  $\mathbb{Z}[i] \subset \mathbb{Q}(i)$  and  $\mathbb{Z}[\sqrt{-3}] \subset \mathbb{Z}\left[\frac{1+\sqrt{-3}}{2}\right] \subset \mathbb{Q}(\sqrt{-3})$ .
- Discrete valuation rings.
- Completion of rings with topology.

# 1 Rings and ideals

**Definition 1.1.** A **commutative ring** is a set  $(A, +, \cdot, 0, 1)$  such that

1.  $(A, +, 0)$  is an abelian group,
2. for all  $x, y, z \in A$ ,
  - $(x \cdot y) \cdot z = x \cdot (y \cdot z)$ ,
  - $x \cdot y = y \cdot x$ ,
  - $x \cdot (y + z) = x \cdot y + x \cdot z$ , and
3. for all  $x \in A$ ,  $x \cdot 1 = 1 \cdot x = x$ .

**Remark 1.2.**

- One is uniquely determined by 3, since  $1' = 1' \cdot 1 = 1$ .
- If  $1 = 0$ , then  $0 = x \cdot 0 = x \cdot 1 = x$ , since

$$x \cdot 0 = x \cdot (0 + 0) = x \cdot 0 + x \cdot 0,$$

so  $x \cdot 0 = 0$ . So every element is zero. Hence  $R = \{0\}$ .

**Definition 1.3.** A **homomorphism of rings**  $f : A \rightarrow B$  is a map such that for all  $x, y \in A$ ,

$$f(x + y) = f(x) + f(y), \quad f(xy) = f(x)f(y), \quad f(1) = 1.$$

**Example.** If  $A \subset B$  is closed under  $+$  and  $\cdot$ , and  $1 \in A$ , then

$$\begin{array}{ccc} A & \longrightarrow & B \\ x & \longmapsto & x \end{array}$$

is a homomorphism.

**Remark 1.4.**

- A composition of homomorphisms is a homomorphism.
- An **isomorphism** is a bijective homomorphism.

**Definition 1.5.** A subset  $I$  of a ring  $A$  is an **ideal** if  $I$  is a subgroup of the additive group  $(A, +)$  which is closed under multiplication by elements of  $A$ , so  $xI \subset I$  for any  $x \in A$ . Sometimes this is written as  $I \triangleleft A$ . In this case the **quotient group**  $A/I$  is naturally a ring, where  $(x + I)(y + I)$  is defined as  $xy + I$ .

**Proposition 1.6.** Let  $I$  be an ideal of a commutative ring  $A$ . Then there is a natural bijection between the ideals  $J \subset A$  such that  $I \subset J$  and the ideals of  $A/I$ .

*Proof.* Let

$$\begin{array}{ccc} A & \longrightarrow & A/I \\ x & \longmapsto & x + I \end{array}$$

be the natural surjective map. Send  $J$  to its image under this map. □

**Definition 1.7.** If  $f : A \rightarrow B$  is a homomorphism, then

$$\text{Ker } f = \{x \in A \mid f(x) = 0\}$$

is an ideal in  $A$ , and

$$\text{Im } f = f(A) \cong A / \text{Ker } f \subset B.$$

## 2 Polynomials and formal power series

**Definition 2.1.** Let  $R$  be a ring. The **polynomial ring** with coefficients in  $R$  is

$$R[x] = \{a_0 + \cdots + a_n x^n \mid a_i \in R, n \in \mathbb{Z}_{\geq 0}\}.$$

The addition is coefficient-wise, and the multiplication is given by the formula

$$\left(\sum_{i \geq 0} a_i x^i\right) \left(\sum_{j \geq 0} b_j x^j\right) = \sum_{i \geq 0} \left(\sum_{j+k=i, j \geq 0, k \geq 0} a_j b_k\right) x^i,$$

where all but finitely many coefficients are zero. Define

$$R[x_1, \dots, x_n] = R[x_1] \cdots [x_n] = \left\{ \sum_{i_1, \dots, i_n \geq 0} a_{i_1, \dots, i_n} x_1^{i_1} \cdots x_n^{i_n} \mid a_{i_1, \dots, i_n} \in R \right\},$$

where all but finitely many coefficients  $a_{i_1, \dots, i_n}$  are equal to zero.

**Definition 2.2.** The **ring of formal power series** with coefficients in  $R$  is

$$R[[t]] = \{a_0 + a_1 t + \dots \mid a_i \in R\}.$$

The addition is coefficient-wise, and the multiplication is given by the formula

$$\left(\sum_{i \geq 0} a_i t^i\right) \left(\sum_{j \geq 0} b_j t^j\right) = \sum_{i \geq 0} \left(\sum_{j+k=i, j \geq 0, k \geq 0} a_j b_k\right) t^i.$$

Define

$$R[[t_1, \dots, t_n]] = R[[t_1]] \cdots [[t_n]].$$

In  $R[[t]]$  many products equal one unlike in  $R[t]$ , for example  $(1-t)(1+t+\dots) = 1$ .

## 3 Zero-divisors, nilpotents, units

**Definition 3.1.** Let  $A$  be a ring. An element  $x \in A$  is a **zero-divisor** if  $x \neq 0$  but  $xy = 0$  for some  $y \neq 0$  in  $A$ . A ring without zero-divisors is called an **integral domain**. An element  $x \in A$  is **nilpotent** if  $x^n = 0$  for some  $n \in \mathbb{Z}_{>0}$ . A **unit**  $x \in A$  is an element such that  $xy = 1$  for some  $y \in A$ . The units of  $A$  form a group under multiplication, denoted by  $A^*$ , or  $A^\times$ .

**Definition 3.2.** Let  $x \in A$ . Then the set

$$\langle x \rangle = \{xy \mid y \in A\}$$

is an ideal. Such ideals are called **principal ideals**.

**Remark.**  $x \in A^*$  if and only if  $\langle x \rangle = A$ , and  $R$  is a field if and only if  $R^* = R \setminus \{0\}$ .

**Proposition 3.3.** Let  $A$  be a non-zero ring. Then the following are equivalent.

1.  $A$  is a field.
2. There are no ideals in  $A$  other than  $\langle 0 \rangle$  and  $A$ .
3. Every non-zero homomorphism  $f : A \rightarrow B$  is injective.

*Proof.*

1  $\implies$  2 Clear.

2  $\implies$  3  $\text{Ker } f \subset A$  is an ideal. Since  $f \neq 0$ ,  $\text{Ker } f \neq A$ . Hence  $\text{Ker } f = 0$ .

3  $\implies$  1 Take any  $x \neq 0$  in  $A$ . Look at  $\langle x \rangle$ . Define  $B = A/\langle x \rangle$ . Then take  $f : A \rightarrow B$  to be the natural surjective map. If  $f$  is not identically zero, we get a contradiction with 3.

□

## 4 Prime ideals and maximal ideals

**Definition 4.1.** An ideal  $I \subset A$  is called **prime** if  $I \neq A$  and if whenever  $xy \in I$ , then  $x \in I$  or  $y \in I$ . An ideal  $J \subset A$  is called **maximal** if there is no ideal  $J'$  such that  $J \subsetneq J' \subsetneq A$ .

**Notation.** The set of prime ideals of  $A$  is called the **spectrum** of  $A$  and is denoted by  $\text{Spec } A$ .

**Lemma 4.2.** An ideal  $I \subset A$  is prime if and only if  $A/I$  is an integral domain.

*Proof.* Obvious. □

**Lemma 4.3.** An ideal  $J \subset A$  is maximal if and only if  $A/J$  is a field.

*Proof.* Obvious. □

**Proposition 4.4.** If  $f : A \rightarrow B$  is a ring homomorphism and  $I \subset B$  is a prime ideal, then  $f^{-1}(I)$  is a prime ideal of  $A$ .

*Proof.* It is easy to see that  $f^{-1}(I)$  is an ideal in  $A$ . Suppose  $xy \in f^{-1}(I)$  for some  $x, y \in A$ . Then  $f(x)f(y) = f(xy) \in I$ . Since  $I$  is prime,  $f(x) \in I$  or  $f(y) \in I$ , so  $x \in f^{-1}(I)$  or  $y \in f^{-1}(I)$ . □

So we get a canonical map

$$\begin{aligned} f^* : \text{Spec } B &\longrightarrow \text{Spec } A \\ I \subset B &\longmapsto f^{-1}(I) \subset A \end{aligned}$$

**Remark 4.5.** If  $f : A \rightarrow B$  is a ring homomorphism, then  $f^{-1}(\mathfrak{p})$ , where  $\mathfrak{p} \subset B$  is a prime ideal, is a prime ideal. But this is false for maximal ideals. Let  $A = \mathbb{Z}$ , let  $B = \mathbb{Q}$ , and let  $f(x) = x$ . Then  $\langle 0 \rangle \subset \mathbb{Q}$  is a maximal ideal and  $f^{-1}(\langle 0 \rangle) = \langle 0 \rangle \subset \mathbb{Z}$  is not a maximal ideal. For example,  $\langle 0 \rangle \subsetneq \langle 2 \rangle \subsetneq \mathbb{Z}$ .

**Theorem 4.6.** Let  $A$  be a non-zero ring. Then  $A$  has at least one maximal ideal. In particular,  $\text{Spec } A$  is not empty.

The proof is based on Zorn's lemma. Let  $S$  be a set. Then a **partial order** is a binary relation  $\leq$  such that

- $x \leq x$  for all  $x \in S$ ,
- $x \leq y \leq z$  implies that  $x \leq z$ , and
- $x \leq y$  and  $y \leq x$  imply that  $x = y$ ,

where not all pairs are comparable. A **chain**  $T \subset S$  is a subset in which every two elements are comparable.

**Lemma 4.7** (Zorn). Suppose that  $S$  is a partially ordered set such that every chain  $T \subset S$  has an upper bound, that is an element  $t \in S$  such that  $x \leq t$  for all  $x \in T$ . Then  $S$  has a maximal element, that is there exists  $s \in S$  such that if  $x \in S$  and  $x \geq s$ , then  $x = s$ .

Zorn's lemma is equivalent to the axiom of choice.

*Proof of Theorem 4.6.* Let  $\Sigma$  be the set of all ideals of  $A$  which are not equal to  $A$ . Then  $\langle 0 \rangle \in \Sigma$ , so  $\Sigma \neq \emptyset$ . Equip  $\Sigma$  with partial order given by inclusion. Enough to check the assumption of Zorn's lemma. Suppose  $T$  is a chain of ideals, so it is a collection of ideals  $J_i$  for  $i \in T$ . Consider instead

$$I = \bigcup_{i \in T} J_i.$$

Claim that  $T$  is a chain implies that  $I$  is an ideal. Then  $x \in I$  implies that  $x \in J_i$  for some  $i$ . Take any  $x, y \in I$ . Then  $x \in J_i$  and  $y \in J_k$  for some  $i, k \in T$ , so  $T$  is a chain, hence  $i \leq k$  or  $k \leq i$ , so  $J_i \subset J_k$  or  $J_k \subset J_i$ . Without loss of generality assume  $J_i \subset J_k$ . Then  $x, y \in J_k$ , so  $x + y \in J_k \subset I$ . Clearly,  $I$  is an upper bound. □

Lecture 3  
Wednesday  
09/10/19

**Corollary 4.8.** *Any ideal of  $A$  is contained in a maximal ideal of  $A$ .*

*Proof.* If  $I \subset A$  is an ideal, apply Theorem 4.6 to  $A/I$ . □

**Corollary 4.9.** *Any non-unit of  $A$  is contained in a maximal ideal.*

*Proof.* Apply Corollary 4.8 to  $\langle a \rangle$ . □

**Example.** The maximal ideals of  $\mathbb{Z}$  are  $\langle p \rangle$ , where  $p$  is prime.

**Definition 4.10.** A ring  $A$  is **local** if  $A$  has exactly one maximal ideal.

**Example.** Any field is a local ring. If  $k$  is a field, then  $k[[t]]$  is a local ring.

**Lemma 4.11** (Prime avoidance). *Let  $A$  be a ring and let  $\mathfrak{p} \subset A$  be a prime ideal. Suppose that  $I_1, \dots, I_n$  are ideals in  $A$  such that  $\bigcap_{j=1}^n I_j \subset \mathfrak{p}$ . Then  $I_j \subset \mathfrak{p}$  for some  $j$ . If, moreover,  $\bigcap_{j=1}^k I_j = \mathfrak{p}$ , then  $I_j = \mathfrak{p}$  for some  $j$ .*

*Proof.* Suppose that  $I_j$  is not a subset of  $\mathfrak{p}$  for any  $j$ . Then there exists  $x_j \in I_j$  such that  $x_j \notin \mathfrak{p}$ . Hence

$$x_1, \dots, x_n \in I_1 \dots I_n \subset \bigcap_{j=1}^n I_j \subset \mathfrak{p},$$

so  $x_1(x_2 \dots x_n) \in \mathfrak{p}$ . Then  $x_1 \notin \mathfrak{p}$  implies that  $x_2 \dots x_n \in \mathfrak{p}$ . Since  $\mathfrak{p}$  is prime we get a contradiction. For the second claim, we know that some  $I_j \subset \mathfrak{p}$ . But  $\mathfrak{p} = \bigcap_{j=1}^k I_j \subset I_k$  for all  $k$ . Hence  $\mathfrak{p} = I_j$ . □

## 5 Nilradical and the Jacobson radical

**Proposition 5.1.** *The set  $\mathcal{N}(A)$  consisting of all nilpotents of the ring  $A$  and zero is an ideal. Then  $\mathcal{N}(A)$  is called the **nilradical** of  $A$ . The quotient  $A/\mathcal{N}(A)$  has no nilpotents.*

*Proof.* Suppose  $x \in A$  is nilpotent, so  $x^n = 0$ . For any  $a \in A$ ,  $(ax)^n = a^n x^n = 0$ . Let  $x$  and  $y$  be nilpotents. Say  $x^n = y^m = 0$ . Then

$$(x+y)^{n+m} = \sum_{i,j \geq 0, i+j=n+m} a_{ij} x^i y^j, \quad a_{ij} \in A.$$

Clearly, either  $i \geq n$  or  $j \geq m$ . Then  $a_{ij} x^i y^j = 0$ . Therefore,  $(x+y)^{n+m} = 0$ , hence  $x+y \in \mathcal{N}(A)$ . If  $x + \mathcal{N}(A)$  is nilpotent in  $A/\mathcal{N}(A)$ , then  $x^n + \mathcal{N}(A) = \mathcal{N}(A)$  is the trivial coset. Hence  $x^n \in \mathcal{N}(A)$ . Thus  $(x^n)^m = 0$  for some  $m$ . □

**Definition 5.2.** A ring  $A$  such that  $\mathcal{N}(A) = 0$  is called a **reduced ring**.

**Proposition 5.3.**  $\mathcal{N}(A)$  is the intersection of all prime ideals of  $A$ .

*Proof.*

- ⊂ Let  $I$  be the intersection of all prime ideals of  $A$ . Let  $f \in A$  be such that  $f^n = 0$ . Take any prime ideal  $\mathfrak{p} \subset A$ . We know that  $f^n = 0 \in \mathfrak{p}$ . Then  $f(f \dots f) \in \mathfrak{p}$  and  $\mathfrak{p}$  prime implies that  $f \in \mathfrak{p}$ , so  $f \in I$ .
- ⊃ Let us prove the converse. Suppose  $f$  is not nilpotent, so  $f^n \neq 0$  for all  $n \geq 1$ . We will show that there exists a prime ideal  $\mathfrak{p} \subset A$  that does not contain  $f$ . Let us consider all ideals of  $A$  that do not contain  $f^m$ , where  $m \in \mathbb{Z}_{>0}$ . Let  $\Sigma$  be the set of ideals  $J \subset A$  such that

$$J \cap \{f^m \mid m \geq 1\} = \emptyset.$$

The zero ideal  $\langle 0 \rangle$  is in  $\Sigma$ . So  $\Sigma \neq \emptyset$ . Equip  $\Sigma$  with a partial order given by inclusion. Applying Zorn's lemma we obtain that  $\Sigma$  contains a maximal element. Call it  $\mathfrak{p}$ . By construction,  $\mathfrak{p} \cap \{f^m \mid m \geq 1\} = \emptyset$ , so  $f \notin \mathfrak{p}$ . It remains to prove that  $\mathfrak{p}$  is prime. Enough to prove that if  $x \notin \mathfrak{p}$  and  $y \notin \mathfrak{p}$ , then  $xy \notin \mathfrak{p}$ . Consider the ideal  $\mathfrak{p} + \langle x \rangle \supsetneq \mathfrak{p}$ . Since  $\mathfrak{p}$  is maximal in  $\Sigma$ , thus  $\mathfrak{p} + \langle x \rangle$  is not in  $\Sigma$ . By definition of  $\Sigma$  there exists  $n \geq 1$  such that  $f^n \in \mathfrak{p} + \langle x \rangle$ . Similarly, there exists  $m \geq 1$  such that  $f^m \in \mathfrak{p} + \langle y \rangle$ . Then  $(\mathfrak{p} + \langle x \rangle)(\mathfrak{p} + \langle y \rangle) \subset \mathfrak{p} + \langle xy \rangle$ . In particular,  $f^{n+m} = f^n \cdot f^m \in \mathfrak{p} + \langle xy \rangle$ . If  $xy \in \mathfrak{p}$ , then  $f^{n+m} \in \mathfrak{p}$ , which is not possible. Therefore,  $xy \notin \mathfrak{p}$ . So  $\mathfrak{p}$  is a prime ideal that does not contain  $f$ . □

Lecture 4  
Thursday  
10/10/19

**Definition 5.4.** The **Jacobson radical**  $\mathcal{J}(A)$  is the intersection of all maximal ideals of  $A$ .

**Proposition 5.5.**  $x \in \mathcal{J}(A)$  if and only if  $1 - xy \in A^*$  for all  $y \in A$ .

*Proof.*

$\Rightarrow$  Let  $x \in \mathcal{J}(A)$ . Suppose there exists  $y \in A$  such that  $1 - xy$  is not a unit. By Corollary 4.9 every non-unit is contained in a maximal ideal. Say  $M \subset A$  is a maximal ideal and  $1 - xy \in M$ . But  $x \in \mathcal{J}(A) \subset M$ . Then  $1 = (1 - xy) + xy \in M$ , but then  $M \neq A$ . A contradiction.

$\Leftarrow$  Given  $x \in A$  such that  $1 - xy \in A^*$  for all  $y \in A$ , we must have  $x \in \mathcal{J}(A)$ . If  $x \notin \mathcal{J}(A)$ , then there exists a maximal ideal  $M \subset A$  such that  $x \notin M$ . Then  $M + \langle x \rangle = A \ni 1$ . Thus  $1 = m + xy$ , where  $y \in A$ . But by assumption  $1 - xy \in A^*$ , so  $m \in A^*$ . But then  $M = A$ . A contradiction.

□

**Definition 5.6.** Let  $I$  be an ideal of  $A$ . The **radical** of  $I$  is the set

$$\text{rad } I = \{x \in A \mid \exists n \geq 1, x^n \in I\}.$$

**Proposition 5.7.** The radical of  $I$  is the intersection of all prime ideals of  $A$  that contain  $I$ .

*Proof.* Apply Proposition 5.3 to  $A/I$ .

□

**Definition 5.8.** Let  $I$  be an indexing set. For each  $i \in I$  we are given a ring  $R_i$ . Consider the product set  $\prod_{i \in I} R_i$ . This is  $(x_i)_{i \in I}$  for  $x_i \in R_i$ . Define

$$0 = (0)_{i \in I} \in \prod_{i \in I} R_i, \quad 1 = (1)_{i \in I} \in \prod_{i \in I} R_i.$$

Define addition and multiplication coordinate-wise, so

$$(a_i)_{i \in I} + (b_i)_{i \in I} = (a_i + b_i)_{i \in I}, \quad (a_i)_{i \in I} \cdot (b_i)_{i \in I} = (a_i \cdot b_i)_{i \in I}, \quad (a_i)_{i \in I}, (b_i)_{i \in I} \in \prod_{i \in I} R_i.$$

Then  $\prod_{i \in I} R_i$  is a ring, the **product of rings**.

A warning is if  $I$  has at least two elements, then  $\prod_{i \in I} R_i$  has zero-divisors.

**Example.**  $R_1 \times R_2$  has  $(1, 0) \cdot (0, 1) = (0, 0) = 0$ .

If  $h_i : R \rightarrow R_i$  is a ring homomorphism for  $i \in I$ , then  $(h_i)_{i \in I}$  is a ring homomorphism  $R \rightarrow \prod_{i \in I} R_i$ .

**Remark 5.9.** Let  $\mathfrak{p}_i$  for  $i \in I$  be all prime ideals of  $R$ . Let  $h_i : R \rightarrow R/\mathfrak{p}_i$ . Then

$$h = (h_i)_{i \in I} : R \rightarrow \prod_{i \in I} R/\mathfrak{p}_i$$

is a homomorphism, and

$$\text{Ker } h = \bigcap_{i \in I} \text{Ker } h_i = \bigcap_{i \in I} \mathfrak{p}_i = \mathcal{N}(R).$$

So there is an injective map

$$R/\mathcal{N}(R) \hookrightarrow \prod_{i \in I} R/\mathfrak{p}_i,$$

a product of integral domains. Now take  $f_j : R \rightarrow R/M_j$ , so if we take the indexing set  $J$  to be the set of all maximal ideals of  $R$ , then we obtain an injective map

$$R/\mathcal{J}(R) \hookrightarrow \prod_{j \in J} R/M_j,$$

a product of fields.

Lecture 5  
Tuesday  
15/10/19



## 6 Localisation of rings

**Example.** Fix a prime  $p$ . Then

$$\mathbb{Z} \subset \left\{ \frac{m}{p^k} \mid m \in \mathbb{Z}, k \in \mathbb{Z}_{\geq 0} \right\} \subset \mathbb{Q}.$$

**Definition 6.1.** A subset  $S$  of a ring  $A$  is called a **multiplicative set** if  $1 \in S$  and  $0 \notin S$ , and  $S$  is closed under multiplication.

**Example 6.2.**

- Let  $a \in A$  be a non-nilpotent. Then  $\{1, a, \dots\}$  is a multiplicative set.
- Let  $\mathfrak{p} \subsetneq A$  be a prime ideal. Then  $A \setminus \mathfrak{p}$  is a multiplicative set. Indeed, if  $x \notin \mathfrak{p}$  and  $y \notin \mathfrak{p}$  then  $xy \notin \mathfrak{p}$  by the definition of a prime ideal.
- If we have a family  $\mathfrak{p}_i$  for  $i \in I$  of prime ideals, then  $A \setminus \bigcup_{i \in I} \mathfrak{p}_i$  is a multiplicative set.
- $A^*$  is a multiplicative set.
- All non-zero-divisors in  $A$  form a multiplicative set.
- Let  $I \subsetneq A$  be an ideal. Then  $1 + I = \{1 + x \mid x \in I\}$  is a multiplicative set.

**Definition 6.3.** Consider  $A \times S$  and the equivalence relation on  $A \times S$  defined as

$$(a, s) \sim (b, t) \iff \exists u \in S, u(at - bs) = 0.$$

Check that this is indeed an equivalence relation.<sup>1</sup> The following is some notation.

- The equivalence class of  $(a, s)$  is written as  $a/s$ . For example, if  $t \in S$ , then  $a/s = at/st$ .
- The set of equivalence classes is denoted by  $S^{-1}A$ .

Define

$$\frac{a}{s} + \frac{b}{t} = \frac{at + bs}{st}, \quad \frac{a}{s} \cdot \frac{b}{t} = \frac{ab}{st}.$$

Need to check that these operations are well-defined.<sup>2</sup> Define  $\frac{0}{1}$  as the zero of  $S^{-1}A$ , and  $\frac{1}{1}$  as the one of  $S^{-1}A$ . Then  $S^{-1}A$  is a ring, the **localisation of  $A$  with respect to a multiplicative set  $S$** .

**Lemma 6.4.** *There is a ring homomorphism*

$$\begin{aligned} f : A &\longrightarrow S^{-1}A \\ x &\longmapsto \frac{x}{1} \end{aligned}.$$

*This  $f$  is injective if and only if  $S$  has no zero-divisors.*

*Proof.* If  $S$  contains a zero-divisor, say  $u$ , then there exists  $a \in A$  for  $a \neq 0$  such that  $ua = 0$ . Then

$$f(a) = \frac{a}{1} = \frac{au}{u} = \frac{0}{u} = 0.$$

So  $\text{Ker } f$  contains  $a$ , hence  $f$  is not injective. If  $f$  has no zero-divisors, then  $u \cdot a = u(a - 0) \neq 0$  if  $a \neq 0$  and any  $u \in S$ . Hence  $f(a) \neq 0$ .  $\square$

If  $A$  is an integral domain, then  $\text{Ker } f = 0$ . So  $A \hookrightarrow S^{-1}A$ .

<sup>1</sup>Exercise

<sup>2</sup>Exercise

**Example.** Let  $R = \mathbb{Z}$ .

- If  $S = \{1, a, \dots\}$ , then

$$S^{-1}\mathbb{Z} = \left\{ \frac{n}{a^m} \mid n \in \mathbb{Z}, m \in \mathbb{Z}_{\geq 0} \right\}.$$

- If  $S = \mathbb{Z} \setminus p\mathbb{Z}$ , then

$$S^{-1}\mathbb{Z} = \left\{ \frac{n}{m} \mid p \nmid m \right\}.$$

- If  $S = \mathbb{Z} \setminus \bigcup_{p_i \text{ prime}} p_i \mathbb{Z}$ , then

$$S^{-1}\mathbb{Z} = \left\{ \frac{n}{m} \mid p_i \nmid m \right\}.$$

- If  $S = \mathbb{Z}^* = \{\pm 1\}$ , then  $S^{-1}\mathbb{Z} = \mathbb{Z}$ .
- If  $S = \{\text{all non-zero elements}\}$ , then  $S^{-1}\mathbb{Z} = \mathbb{Q}$ .
- If  $S = \{1 + I \mid I \subset \mathbb{Z} \text{ ideal}\} = \{1 + nk \mid k \in \mathbb{Z}\}$ , then

$$S^{-1}\mathbb{Z} = \left\{ \frac{m}{1 + nk} \mid m, k \in \mathbb{Z} \right\},$$

where  $n$  is fixed.

**Example.** Let  $R = k[x]$ , where  $k$  is a field.

- If  $S = k[x]^* = k^*$ , then  $S^{-1}k[x] = k[x]$ .
- If  $S = \{\text{all non-zero elements}\}$ , then

$$S^{-1}k[x] = k(x) = \left\{ \frac{f(x)}{g(x)} \mid g(x) \text{ arbitrary non-zero polynomial} \right\}.$$

**Example 6.5.** Let  $k$  be a field, and let  $A = k[x, y] / \langle xy \rangle$ . Note that  $A$  has zero-divisors, since  $xy = 0$  in  $A$ , but  $x \neq 0$  in  $A$  and  $y \neq 0$  in  $A$ . Then  $S = \{1, x, \dots\}$  is a multiplicative set, since  $x^n \neq 0$  in  $A$  for  $n = 1, 2, \dots$ , because no power of the polynomial  $x$  is in  $\langle xy \rangle$ . What is  $S^{-1}A$ ? Let  $f : A \rightarrow S^{-1}A$ . Then  $a \in \text{Ker } f$  if and only if  $a/1 = 0/1$ , if and only if  $u \cdot (a \cdot 1 - 0 \cdot 1) = 0$  for some  $u \in S$ , if and only if  $ua = 0$ . Let  $a \neq 0$ . Then  $u = 1$  is not interesting. Take  $u = x$  and  $a = y$ , then  $xy = 0$ , hence  $y \in \text{Ker } f$ . Then  $f$  is a homomorphism, hence  $\text{Ker } f$  is an ideal. So  $\langle y \rangle = yA \subset \text{Ker } f$ . In general,

$$a = \sum_{i,j \geq 0} a_{ij} x^i y^j \equiv a_{00} + \sum_{i \geq 1} a_{i0} x^i + \sum_{j \geq 1} a_{0j} y^j \pmod{\langle xy \rangle}.$$

Then  $\text{Ker } f = yA = \langle y \rangle$ , since  $\sum_{j \geq 1} a_{0j} y^j$  goes to zero, since it is annihilated by  $x$ , and  $x^n \cdot \sum_{i \geq 0} a_i x^i$  is never zero in  $A$ . Thus  $f(A) = k[x]$ , and

$$S^{-1}A = \left\{ \frac{f(x)}{x^n} \mid f(x) \in k[x], n \geq 0 \right\} = k[x, x^{-1}] = \left\{ \sum_{i \in \mathbb{Z}, a_i = 0 \text{ for almost all } i} a_i x^i \mid a_i \in k \right\}.$$

**Lemma 6.6** (Universal property of localisation). *Let  $A$  be a ring, and  $S \subset A$  a multiplicative set. Let  $g : A \rightarrow B$  be a ring homomorphism such that  $g(s)$  is a unit in  $B$  for all  $s \in S$ . Then there exists a unique ring homomorphism  $h : S^{-1}A \rightarrow B$  such that  $g = h \circ f$  where  $f : A \rightarrow S^{-1}A$  is the canonical map, so*

$$\begin{array}{ccc} A & & \\ f \downarrow & \searrow g & \\ S^{-1}A & \xrightarrow{\exists! h} & B \end{array}.$$

Lecture 7  
Thursday  
17/10/19

*Proof.* Define

$$\begin{aligned} h &: S^{-1}A \longrightarrow B \\ \frac{a}{s} &\longmapsto \frac{g(a)}{g(s)}, \quad a \in A, \quad s \in S. \end{aligned}$$

This is well-defined, that is if  $a/s = b/t$  then  $g(a)g(s)^{-1} = g(b)g(t)^{-1}$ .<sup>3</sup> This is a ring homomorphism.<sup>4</sup> Now easy to check that

$$(h \circ f)(a) = h\left(\frac{a}{1}\right) = \frac{g(a)}{g(1)} = \frac{g(a)}{1} = g(a), \quad a \in A.$$

Moreover, if  $h' : S^{-1}A \rightarrow B$  and  $g = h' \circ f$  then for all  $a \in A$  we have  $(h' \circ f)(a) = g(a)$ . Since  $h'$  is a ring homomorphism, for all  $s \in S$ ,  $h'(1/s) = 1/h'(s/1) = 1/g(s)$ . Hence

$$h'\left(\frac{a}{s}\right) = h'\left(\frac{a}{1}\right)h'\left(\frac{1}{s}\right) = \frac{h'(f(a))}{h'(f(s))} = \frac{g(a)}{g(s)} = h\left(\frac{a}{s}\right).$$

□

For all ideal  $I \subseteq A$ , set

$$S^{-1}I = \left\{ \frac{i}{s} \in S^{-1}A \mid i \in I, s \in S \right\},$$

the ideal of  $S^{-1}A$  generated by  $f(I)$ .

**Proposition 6.7.** *Let  $S \subset A$  be a multiplicative subset, and let  $I_1, \dots, I_n$  be ideals of  $A$ . Then*

1.  $S^{-1}(I_1 + \dots + I_n) = S^{-1}I_1 + \dots + S^{-1}I_n$ ,
2.  $S^{-1}(I_1 \dots I_n) = S^{-1}I_1 \dots S^{-1}I_n$ ,
3.  $S^{-1}(\bigcap_{i=1}^n I_i) = \bigcap_{j=1}^n S^{-1}I_j$ , and
4.  $S^{-1}(\text{rad } I) = \text{rad } S^{-1}I$  for every ideal  $I$ .

*Proof.* Exercise.<sup>5</sup>

□

There is a map

$$\{\text{ideals } I \text{ of } A\} \rightarrow \{\text{ideals } S^{-1}I \text{ of } S^{-1}A\}.$$

**Proposition 6.8.** *Every ideal of  $S^{-1}A$  is of the form  $S^{-1}I$  for some ideal  $I \subseteq A$ .*

*Proof.* Let  $J$  be any ideal of  $S^{-1}A$ . Define  $I = f^{-1}J$ . Know  $I$  is an ideal of  $A$ . Claim that  $J = S^{-1}I$ . Say  $a/s \in J$ . Since  $J$  is an ideal,  $s(a/s) \in J$ , so  $a/1 \in J$ , so  $a \in I$ . Hence  $a/s \in S^{-1}I$ . So  $J \subseteq S^{-1}I$ . Conversely,  $f(I) = f(f^{-1}(J)) \subseteq J$ . Thus  $S^{-1}I \subseteq J$ . □

**Theorem 6.9.** *The only prime ideals of  $S^{-1}A$  are of the form  $S^{-1}\mathfrak{p}$  where  $\mathfrak{p}$  is a prime ideal of  $A$  such that  $\mathfrak{p} \cap S = \emptyset$ . Hence there is a bijection*

$$\{ \text{prime ideals of } S^{-1}A \} \quad \longleftrightarrow \quad \{ \text{prime ideals of } A \text{ that do not intersect } S \}.$$

*Proof.* Prove  $S^{-1}\mathfrak{p}$  is prime if  $\mathfrak{p}$  is prime and  $\mathfrak{p} \cap S = \emptyset$ . Say  $a/s \cdot b/t \in S^{-1}\mathfrak{p}$  for  $a/s, b/t \in S^{-1}A$ . This implies  $v(abu - cst) = 0$  for some  $u, v \in S$  and  $c \in \mathfrak{p}$ . Hence  $abuv = cstv \in \mathfrak{p}$ , so  $ab \in \mathfrak{p}$ , as  $u$  and  $v$  are units, so  $a \in \mathfrak{p}$  or  $b \in \mathfrak{p}$ . Hence  $S^{-1}\mathfrak{p}$  is prime. Next note that  $f^{-1}(S^{-1}\mathfrak{p}) = \mathfrak{p}$ , assuming  $\mathfrak{p} \cap S = \emptyset$ . For if  $a \in A$  lies in  $S^{-1}\mathfrak{p}$  then by definition there exists  $s \in S$  such that  $sa \in \mathfrak{p}$ . Then  $s$  is a unit and so  $a \in \mathfrak{p}$ . Hence  $\mathfrak{p}$  is uniquely determined by  $S^{-1}\mathfrak{p}$ . Now let  $\mathfrak{q}$  be an arbitrary prime ideal of  $S^{-1}A$ . Then certainly  $\mathfrak{q} = S^{-1}I$  for  $I = f^{-1}(\mathfrak{q})$ . But the preimage of a prime ideal is prime. So  $I$  is prime. Moreover,  $I \cap S = \emptyset$  as no  $s \in S$  is in  $\mathfrak{q}$ , since  $\mathfrak{q}$  is prime, so  $\mathfrak{q}$  contains no units. □

---

<sup>3</sup>Exercise

<sup>4</sup>Exercise

<sup>5</sup>Exercise

## 7 Spec $R$ as a topological space

Lecture 8  
Tuesday  
22/10/19

A set  $X$  with a collection  $\mathcal{U}$  of subsets  $U \subset X$  is called a **topological space** if the following properties hold.

1.  $\mathcal{U}$  contains  $\emptyset$  and  $X$ .
2. If  $U$  and  $U'$  are in  $\mathcal{U}$ , then  $U \cap U'$  is in  $\mathcal{U}$ .
3. If  $U_i$  are in  $\mathcal{U}$ , where  $i$  is an element of an indexing set  $S$ , then  $\bigcup_{i \in S} U_i$  is in  $\mathcal{U}$ .

Then the elements of  $\mathcal{U}$  are called **open subsets** of  $X$ . The following is an equivalent definition. A set  $X$  with a family  $\mathcal{V}$  of subsets  $V \subset X$  is called a **topological space** if the following properties hold.

1.  $\mathcal{V}$  contains  $\emptyset$  and  $X$ .
2. If  $V$  and  $V'$  are in  $\mathcal{V}$ , then  $V \cup V'$  is in  $\mathcal{V}$ .
3. If  $V_i$  are in  $\mathcal{V}$ , where  $i$  is an element of an indexing set  $S$ , then  $\bigcap_{i \in S} V_i$  is in  $\mathcal{V}$ .

Then the elements of  $\mathcal{U}$  are called **closed subsets** of  $X$ . For the equivalence, if  $U$  is in  $\mathcal{U}$ , then define the closed subsets as  $X \setminus U$  for  $U$  in  $\mathcal{U}$ , and vice versa. Let  $R$  be a ring with unity. Let  $I \subset R$  be an ideal. Let  $V_I$  be the set of all prime ideals in  $R$  that contain  $I$ . Define  $U_I = \text{Spec } R \setminus V_I$ .

**Proposition 7.1.** *The collection of subsets  $V_I \subset \text{Spec } R$ , for all ideals  $I \subset R$ , satisfies 1, 2, 3 of closed subsets, hence defines a topology on  $\text{Spec } R$ .*

*Proof.*

1. If  $I = 0$  is the zero ideal, then  $V_0 = \text{Spec } R$ , all prime ideals of  $R$ . If  $I = R$ , then no prime ideals of  $R$  contain  $R$ , so  $V_R = \emptyset$ , so 1 holds.
2. It is enough to check that  $V_I \cup V_J = V_{IJ} = V_{I \cap J}$ . Note that  $IJ \subset I \cap J$ . An element of  $V_I$  is a prime ideal  $\mathfrak{p} \supset I$ , so  $\mathfrak{p} \supset IJ$ . Conversely, let  $\mathfrak{p}$  be a prime ideal such that  $IJ \subset \mathfrak{p}$ . Claim that  $I \subset \mathfrak{p}$  or  $J \subset \mathfrak{p}$ . Suppose not. Then there exists  $x \in I$  such that  $x \notin \mathfrak{p}$  and there exists  $y \in J$  such that  $y \notin \mathfrak{p}$ . Then  $xy \in IJ \subset \mathfrak{p}$ . This contradicts the definition of prime ideals. So the claim is proved. Thus 2 holds.
3.  $J_i$  for  $i \in S$  is a collection of ideals. Claim that  $\bigcap_{i \in S} V_{J_i} = V_J$ , where  $J = \sum_{i \in S} J_i$  is the smallest ideal of  $R$  containing all  $J_i$  for  $i \in S$ . The elements of  $J$  are finite sums, where each summand is in some  $J_i$ . If  $\mathfrak{p} \supset J_i$  for  $i \in S$ , then  $\mathfrak{p} \supset J$ . Conversely, if  $\mathfrak{p} \supset J \supset J_i$ , then  $\mathfrak{p} \supset J_i$  for all  $i \in S$ .

□

Recall that if  $f : A \rightarrow B$  is a homomorphism of rings, then  $f^* : \text{Spec } B \rightarrow \text{Spec } A$  sends any prime ideal  $\mathfrak{p} \subset B$  to the inverse image  $f^{-1}(\mathfrak{p})$ , which is a prime ideal in  $A$ . This breaks down for maximal ideals.

**Example.** Take  $f : \mathbb{Z} \rightarrow \mathbb{Q}$ , then  $f^{-1}(0) = 0$ , which is not maximal in  $\mathbb{Z}$ .

A map of topological spaces is **continuous** if the inverse image of any open set is open. Equivalently, the inverse images of closed sets are closed.

**Proposition 7.2.**  *$f^*$  is a continuous map.*

*Proof.* Let  $I$  be an ideal in  $A$ . We need to show that  $(f^*)^{-1}(V_I) = V_J$  for some ideal  $J$  in  $B$ . Let  $J$  be the smallest ideal in  $B$  containing  $f(I)$ .

- ⊂ Fix  $\mathfrak{p}$  in  $V_I$ , a prime ideal in  $A$  such that  $\mathfrak{p} \supset I$ . The elements of the left hand side that are mapped to  $\mathfrak{p}$  by  $f^*$  are the prime ideals  $\mathfrak{q} \subset B$  such that  $\mathfrak{p} = f^{-1}(\mathfrak{q})$ . We have  $I \subset \mathfrak{p}$ , so  $f(I) \subset f(\mathfrak{p}) \subset \mathfrak{q}$ , so  $J \subset \mathfrak{q}$ , by definition of  $J$ .
- ⊃ Take any prime ideal  $\mathfrak{q} \subset B$  such that  $J \subset \mathfrak{q}$ . We have  $I \subset f^{-1}(f(I)) \subset f^{-1}(J) \subset f^{-1}(\mathfrak{q})$ , so  $f^{-1}(\mathfrak{q})$  is a prime ideal in  $A$  containing  $I$ . This ideal is exactly  $f^*(\mathfrak{q})$ , so  $f^*(\mathfrak{q})$  is in  $V_I$ . Since  $\mathfrak{q} \in (f^*)^{-1}(f^*(\mathfrak{q})) \subset (f^*)^{-1}(V_I)$ , so we are done.

□

The following are particular cases.

- Assume  $f$  is surjective. Then  $B \cong A/\text{Ker } f$ . Then

$$\begin{aligned} \{\text{prime ideals in } B\} &\longrightarrow \{\text{prime ideals in } A \text{ containing } \text{Ker } f\} \\ \mathfrak{p} \subset B &\longmapsto f^{-1}(\mathfrak{p}) \end{aligned} .$$

So in this case  $f^*$  is injective and its image is  $V_{\text{Ker } f}$ .

- Let  $S$  be a multiplicative set in  $A$ . Let  $f : A \rightarrow S^{-1}A$  be the associated canonical map. By Theorem 6.9 the prime ideals of  $S^{-1}A$  are  $S^{-1}\mathfrak{p}$ , where  $\mathfrak{p}$  is a prime ideal in  $A$  such that  $\mathfrak{p} \cap S = \emptyset$ . Thus  $f^* : \text{Spec } S^{-1}A \rightarrow \text{Spec } A$  is injective and its image consists of  $\mathfrak{p} \subset A$  such that  $\mathfrak{p} \cap S = \emptyset$ .

**Example.**

- Let  $k$  be a field. Then  $\text{Spec } k$  is one point.
- Let  $R = k[x]$ , an integral domain. This is a PID, so every ideal is  $\langle p(x) \rangle$ , where  $p(x) \in k[x]$  is monic. Then  $\langle p(x) \rangle$  is prime if and only if  $p(x)$  is irreducible, so

$$\text{Spec } k[x] = \{\langle 0 \rangle\} \cup \{\langle p(x) \rangle \mid p(x) \text{ is monic and irreducible}\} .$$

In particular, if  $k$  is algebraically closed, such as  $k = \mathbb{C}$ , then

$$\text{Spec } k[x] = \{\langle 0 \rangle\} \cup \{\langle x - a \rangle \mid a \in k\} .$$

- Let  $R = \mathbb{Z}$ , a PID. Then

$$\text{Spec } \mathbb{Z} = \{\langle 0 \rangle\} \cup \{\langle p \rangle \mid p \text{ is a prime number}\} .$$

- Let  $R = \mathbb{Z}[i]$  be the Gaussian integers, a PID. The tautological map  $f : \mathbb{Z} \rightarrow \mathbb{Z}[i]$  gives rise to  $f^* : \text{Spec } \mathbb{Z}[i] \rightarrow \text{Spec } \mathbb{Z}$ . Take a usual prime  $p$  and decompose  $p$  into a product of primes in  $\mathbb{Z}[i]$ .
  - $2 = (1+i)(1-i) = -i(1+i)^2$ , where  $1+i$  is a prime in  $\mathbb{Z}[i]$ .
  - If  $p \equiv 1 \pmod{4}$ , then  $p = (a+bi)(a-bi)$ . In this case  $a+bi$  and  $a-bi$  are not associated primes.
  - If  $p \equiv 3 \pmod{4}$ , then  $p$  stays prime in  $\mathbb{Z}[i]$ .

Then

$$\begin{array}{ccc} \text{Spec } \mathbb{Z}[i] & \longrightarrow & \text{Spec } \mathbb{Z} \\ \langle 0 \rangle & \longmapsto & \langle 0 \rangle \\ \langle 1+i \rangle & \longmapsto & \langle 2 \rangle \quad \text{ramified} \\ \langle 3 \rangle & \longmapsto & \langle 3 \rangle \quad \text{inert} \\ \langle 1+2i \rangle, \langle 1-2i \rangle & \longmapsto & \langle 5 \rangle \quad \text{split} \end{array} .$$

- Let  $R$  be an integral domain and let  $k$  be the fraction field of  $R$ , so  $f : R \hookrightarrow k$ . Then  $\text{Spec } k = \{\langle 0 \rangle\}$  and  $f^* : \text{Spec } k \rightarrow \text{Spec } R$ .
- Let  $k$  be a field, so  $f : k \hookrightarrow k[x]$ . Then  $f^* : \text{Spec } k[x] \rightarrow \text{Spec } k$ . If  $\mathfrak{p} \subset k[x]$ , then  $\mathfrak{p} \cap k = \{\langle 0 \rangle\}$ , otherwise if  $\mathfrak{p}$  contains a unit of  $k[x]$  then  $\mathfrak{p} = k[x]$ , a contradiction.

Usually, every point of a topological space is a closed subset. But this is not always true. Recall that if  $Y$  is a subset of a topological space  $X$ , then the **closure** of  $Y$  is the smallest closed subset of  $X$  containing  $Y$ . It is the same as the intersection of all closed subsets containing  $Y$ . Claim that if  $\mathfrak{p} \subseteq R$  is a prime ideal, then the closure of  $\mathfrak{p}$  is  $V_{\mathfrak{p}}$ . Any closed subset of  $\text{Spec } R$  containing  $\mathfrak{p}$  is  $V_J$ , where  $J \subset \mathfrak{p}$ . This  $V_J$  visibly contains  $V_{\mathfrak{p}}$ . Hence  $V_{\mathfrak{p}}$  is the intersection of all such  $V_J$ .

**Example.** In  $\text{Spec } \mathbb{Z}$ , the point  $\langle p \rangle$  is closed, because  $V_{\langle p \rangle} = \{\langle p \rangle\}$ . The point  $\langle 0 \rangle$  is not closed, as  $V_{\langle 0 \rangle} = \text{Spec } \mathbb{Z}$ . The closure of  $\langle 0 \rangle$  is all of  $\text{Spec } \mathbb{Z}$ .

**Example.** Let  $R = k[[t]] = \{a_0 + a_1 t + \dots \mid a_i \in k\}$ , a local ring. Its unique maximal ideal is  $\langle t \rangle$ . This is also a unique non-zero prime ideal.<sup>6</sup> All ideals are  $\langle 0 \rangle$  and  $\langle t^n \rangle$ . Then  $\text{Spec } k[[t]] = \{\langle 0 \rangle, \langle t \rangle\}$ . Similarly,  $\langle 0 \rangle$  is not a closed point, since its closure is  $\text{Spec } k[[t]]$ , and  $\langle t \rangle$  is a closed point.

<sup>6</sup>Exercise

## 8 Determinants

Lecture 10  
Thursday  
24/10/19

Let  $R$  be a commutative ring with unity. Let  $A$  be a matrix  $A = (a_{ij})_{i,j=1}^n$  for  $a_{ij} \in R$ . Then

$$\det A = \sum_{\pi \in \mathcal{S}_n} \operatorname{sgn} \pi \cdot a_{1\pi(1)} \cdots a_{n\pi(n)} \in R,$$

where  $\operatorname{sgn} : \mathcal{S}_n \rightarrow \{\pm 1\}$ . Let

$$M_{ij} = \det(A \text{ without } j\text{-th column and } i\text{-th row}) \in R.$$

Then

$$(-1)^{j+1} a_{i1} M_{j1} + \cdots + (-1)^{j+n} a_{in} M_{jn} = \begin{cases} \det A & i = j \\ 0 & i \neq j \end{cases}.$$

Define the **adjoint matrix** of  $A$  as the  $n \times n$  matrix  $A^\vee$  with entries  $(A^\vee)_{ij} = (-1)^{i+j} M_{ji}$ , so

$$A^\vee = \left( (-1)^{i+j} M_{ji} \right)^\top.$$

Then  $A \cdot A^\vee = A^\vee \cdot A = \det A \cdot I_n$ , where  $I_n$  is the identity matrix.

## 9 Modules

**Definition 9.1.** Let  $A$  be a commutative ring with unity. An  **$A$ -module**  $M$  is an abelian group with an additional structure  $A \times M \rightarrow M$  such that

$$\lambda(x + y) = \lambda x + \lambda y, \quad (\mu + \lambda)x = \mu x + \lambda x, \quad \mu(\lambda x) = (\mu\lambda)x, \quad 1x = x, \quad \lambda, \mu \in R, \quad x, y \in M.$$

**Example 9.2.**

- If  $R$  is a field, then an  $R$ -module is the same as a vector space.
- If  $R = \mathbb{Z}$ , then an  $R$ -module is the same as an abelian group. Remark that if  $G$  is an abelian group then  $n \cdot g = g + \cdots + g$ .
- If  $R$  is any ring, then subgroups of  $R$  that are  $R$ -modules are the same as ideals.
- If  $k$  is a field, then  $k[x]$ -modules are vector spaces  $V$  over  $k$  equipped with a linear transformation  $L : V \rightarrow V$ . Here  $x$  acts on  $V$  as  $L$ .

**Definition 9.3.** If  $M$  and  $N$  are  $R$ -modules, then a **homomorphism of  $R$ -modules**  $f : M \rightarrow N$  is a homomorphism of abelian groups such that  $f(rx) = rf(x)$  for all  $x \in M$  and all  $r \in R$ .

**Definition 9.4.** Let  $\operatorname{Hom}_R(M, N)$  be the set of  $R$ -module homomorphisms  $M \rightarrow N$ .

This is an abelian group. Moreover, it is an  $R$ -module. If  $r \in R$  and  $f \in \operatorname{Hom}_R(M, N)$  then  $r \cdot f$  sends  $x \in M$  to  $rf(x) \in N$ . Warning that if  $R$  is not commutative  $\operatorname{Hom}_R(M, N)$  is just an abelian group.

**Definition 9.5.** Let  $M$  and  $N$  be submodules of an  $R$ -module. Define

$$(N : M) = \{r \in R \mid rM \subset N\}.$$

This is an ideal in  $R$ .

**Example.** The **annihilator** of  $M$  is

$$(0 : M) = \{r \in R \mid rM = 0\} = \operatorname{Ann} M.$$

**Definition 9.6.** An  $R$ -module  $M$  is **finitely generated** if there are elements  $x_1, \dots, x_n \in M$  such that for any  $m \in M$  there are  $r_1, \dots, r_n \in R$  such that  $m = r_1x_1 + \dots + r_nx_n$ .

**Example.** There is a **free** finitely generated module

$$R^{\oplus n} = \{(t_1, \dots, t_n) \mid t_i \in R\},$$

with coordinate-wise addition and multiplication.

**Remark.** Any finitely generated  $R$ -module is a quotient of a free finitely generated  $R$ -module. Indeed, define

$$\begin{aligned} f_i &: R^{\oplus n} \longrightarrow M \\ (t_1, \dots, t_n) &\longmapsto t_1x_1 + \dots + t_nx_n. \end{aligned}$$

Comment that  $JM$  is the smallest submodule of  $M$  containing all elements  $rm$  for  $r \in J$  and  $m \in M$ , so

$$JM = \{\text{finite sums } r_1m_1 + \dots + r_nm_n\} \subset M.$$

**Lemma 9.7.** Let  $A$  be a ring. Let  $M$  be a finitely generated  $A$ -module. Let  $J \subset A$  be an ideal such that  $JM = M$ . Then there is an  $a \in J$  such that  $(1 - a)M = 0$ .

*Proof.* If  $M = 0$ , then it is fine. Suppose  $M \neq 0$  and  $m_1, \dots, m_n$  are generators of  $M$ . Then  $m_i \in M = JM$ , so

$$\begin{aligned} m_1 &= x_{11}m_1 + \dots + x_{1n}m_n \\ &\vdots \\ m_n &= x_{n1}m_1 + \dots + x_{nn}m_n, \end{aligned}$$

for  $x_{ij} \in J$ . Define  $X = (x_{ij})_{i,j=1}^n$ . Then

$$\begin{pmatrix} m_1 \\ \vdots \\ m_n \end{pmatrix} = X \begin{pmatrix} m_1 \\ \vdots \\ m_n \end{pmatrix} \iff (\mathbf{I}_n - X) \begin{pmatrix} m_1 \\ \vdots \\ m_n \end{pmatrix} = 0.$$

Consider the adjoint matrix  $(\mathbf{I}_n - X)^\vee$ . Then

$$(\mathbf{I}_n - X)^\vee (\mathbf{I}_n - X) \begin{pmatrix} m_1 \\ \vdots \\ m_n \end{pmatrix} = 0 \iff \det(\mathbf{I}_n - X) \begin{pmatrix} m_1 \\ \vdots \\ m_n \end{pmatrix} = 0.$$

We have  $\det(\mathbf{I}_n - X) \in A$ . Then  $\det(\mathbf{I}_n - X)$  is a product of diagonal entries  $\prod_{i=1}^n (1 - x_{ii})$ , plus other terms but every non-diagonal term contains at least one factor in  $J$ , so is in  $J$ . Finally,  $\det(\mathbf{I}_n - X) = 1 - a$ , where  $a \in J$ . Now,  $(1 - a)m_i = 0$  for  $i = 1, \dots, n$ . Hence  $(1 - a)M = 0$ .  $\square$

**Remark.** If  $M$  is not finitely generated then this is false, such as  $A = \mathbb{Z}$  and  $M = \mathbb{Q}$ . If  $p$  is a prime, then  $p\mathbb{Q} = \mathbb{Q}$ . So for  $J = \langle p \rangle$  we have  $JM = M$ . But no non-zero integer annihilates  $\mathbb{Q}$ , since  $\mathbb{Q}$  is not a finitely generated  $\mathbb{Z}$ -module.

**Corollary 9.8.** Let  $R$  be a ring and let  $M$  be a finitely generated  $R$ -module. If  $f : M \rightarrow M$  is a surjective  $R$ -module endomorphism, then  $f$  is an isomorphism.

*Proof.* Define  $A = R[t]$ . Let us equip  $M$  with the structure of an  $A$ -module. Define  $t \cdot m = f(m)$  for  $m \in M$ . This makes sense because  $f(rx) = rf(x)$  for all  $r \in R$ . Then  $M$  is finitely generated also as an  $A$ -module. If  $f(M) = M$ , then  $tM = M$ . Take  $J = \langle t \rangle \subset A$ . By Lemma 9.7 there exists  $a \in \langle t \rangle$  such that  $(1 - a)M = 0$ . Take  $v \in M$  such that  $f(v) = 0$ . Then  $tv = 0$ , so  $av = 0$ . Since  $(1 - a)v = 0$ , we conclude  $v = 0$ .  $\square$

Lecture 11  
Tuesday  
29/10/19

**Theorem 9.9** (Nakayama's lemma). *Let  $A$  be a ring and let  $J \subset A$  be an ideal contained in the Jacobson radical  $\mathcal{J}(A)$ . If  $M$  is a finitely generated  $A$ -module such that  $JM = M$ , then  $M = 0$ .*

*Proof.* Lemma 9.7 implies that there exists  $a \in J$  such that  $(1 - a)M = 0$ . But  $a \in \mathcal{J}(A)$ , so  $1 - a$  is a unit in  $A$ . Then there exists  $u \in A$  such that  $u(1 - a) = 1$ . Hence  $M = u(1 - a)M = 0$ .  $\square$

**Corollary 9.10.** *Let  $A$  be a ring and  $J$  an ideal contained in the Jacobson radical of  $A$ . Suppose  $M$  is an  $A$ -module, and  $N \subset M$  is a submodule such that  $M/N$  is a finitely generated  $A$ -module. Then  $M = N + JM$  implies  $M = N$ .*

*Proof.* Apply Nakayama's lemma to  $M/N$ . Indeed, we have  $M/N = J(M/N)$ , so  $M/N = 0$ .  $\square$

Recall a ring is local when it has a unique maximal ideal. The quotient is called the **residue field**.

**Example.** For  $k$  a field,  $k[[t]] \supset \langle t \rangle$  and  $k[[t_1, \dots, t_n]] \supset \langle t_1, \dots, t_n \rangle$  are local rings. <sup>7</sup>

If  $A$  is a ring with a prime ideal  $\mathfrak{p}$ , and  $S = A \setminus \mathfrak{p}$ , then  $S^{-1}A$  is a local ring.

**Example.** If  $A = \mathbb{Z}$  and  $\mathfrak{p} = \langle p \rangle$ , then  $\langle p \rangle \supset \mathbb{Z}_{\langle p \rangle} = \{a/b \mid (b, p) = 1\}$ .

**Theorem 9.11.** *Let  $R$  be a local ring with maximal ideal  $J$  and residue field  $k = R/J$ . Let  $M$  be a finitely generated  $R$ -module.*

1.  $M/JM$  is a finite-dimensional vector space over  $k$ .
2. Let  $v_1, \dots, v_n$  be a basis of  $M/JM$  as a vector space over  $k$ . Choose  $\tilde{v}_1, \dots, \tilde{v}_n \in M$  to be representatives of  $v_1, \dots, v_n$  respectively. That is,  $v_i = \tilde{v}_i + JM$ . Then  $\tilde{v}_1, \dots, \tilde{v}_n$  generate  $M$  as an  $R$ -module. Moreover, this is a minimal set of generators of  $M$ . That is, no proper subset generates  $M$ .
3. All minimal sets of generators of  $M$  are obtained in this way. In particular, all such sets have  $n$  elements.

*Proof.*  $J$  is the Jacobson radical of  $A$ .

1. Any quotient of a finitely generated  $R$ -module is a finitely generated  $R$ -module. Hence  $M/JM$  is a finitely generated  $R$ -module. But if  $x \in J$  then  $x \cdot M/JM = 0$ . So  $R$  acts on  $M/JM$  via the quotient  $k = R/J$ . One says that the action of  $R$  descends to an action of  $k$ . Thus  $M/JM$  is a  $k$ -module, which is finitely generated. In other words,  $M/JM$  is a finite-dimensional  $k$ -vector space.
2. Consider  $N = R\tilde{v}_1 + \dots + R\tilde{v}_n = \{r_1\tilde{v}_1 + \dots + r_n\tilde{v}_n \mid r_i \in R\} \subset M$ . Then  $M/JM$  is generated by  $v_1, \dots, v_n$ , hence  $M = N + JM$ , since  $M/JM = N/JN$ . By Corollary 9.10 we have  $M = N$ . If a proper subset of  $\tilde{v}_1, \dots, \tilde{v}_n$  generates  $M$ , then a proper subset of  $v_1, \dots, v_n$  generates an  $n$ -dimensional vector space, a contradiction.

$\square$

---

<sup>7</sup>Exercise