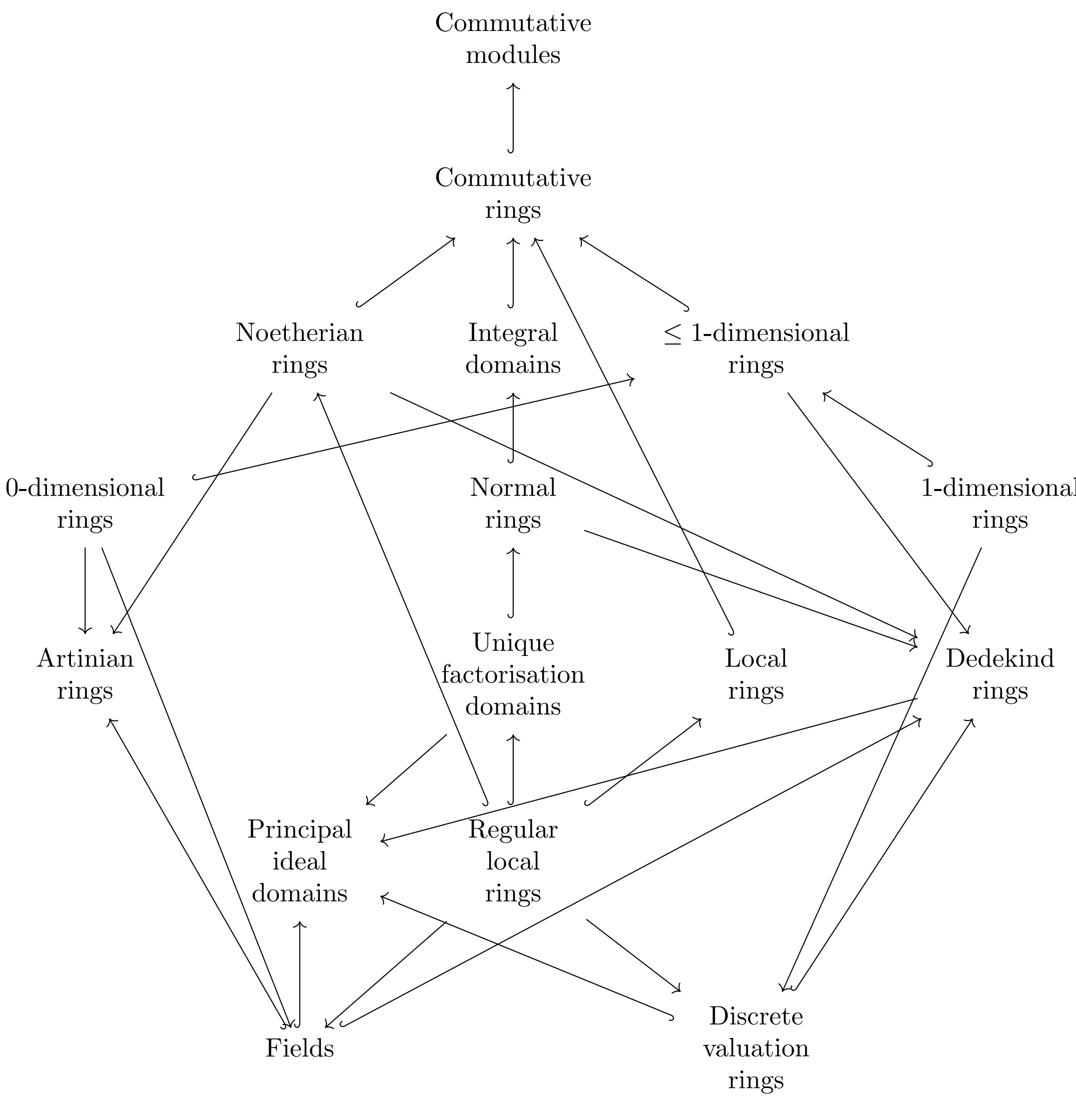
M4P55 Commutative Algebra

Lectured by Prof Alexei Skorobogatov
Typed by David Kurniadi Angdinata

Autumn 2019



Syllabus

Generalities on rings. Radicals of rings. Localisations of rings. Spectra of rings. Modules over rings. Finiteness conditions of Noetherian rings and Artinian rings. Primary decompositions of ideals in rings. Integral closure and normal rings. Discrete valuation rings. Completions of rings with topology.

Contents

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.
- Localisations 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 $\mathbb{Z}\left[\sqrt{-3}\right] \subset \mathbb{Z}\left[\frac{1+\sqrt{-3}}{2}\right] \subset \mathbb{Q}\left(\sqrt{-3}\right)$.
- Discrete valuation rings.
- Completions 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.

- 1 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 $A = \{0\}$.

Definition 1.3. A **homomorphism of rings** $f : A \to B$ is a map such that

$$f(x + y) = f(x) + f(y), \qquad f(xy) = f(x) f(y), \qquad f(1) = 1, \qquad x, y \in A.$$

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 $I \lhd A$. 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 $f : A \to B$ is a homomorphism, then

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

is an ideal in A, and

$$\operatorname{im} f = f(A) \cong A/\ker f \subset B.$$

2 Polynomials and formal power series

Lecture 2
Tuesday
08/10/19

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

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

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 equal to zero. Define

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

where all but finitely many coefficients are equal to zero.

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

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

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

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

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

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 $x \cdot \dots \cdot x = x^n = 0$ for some $n \in \mathbb{Z}_{>0}$. A **unit** $x \in A$ is an element such that $xy = 1$ for some $y \in A$. Then we write $y = x^{-1}$. 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 A is a field if and only if $A^* = A \setminus \{0\}$.

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 zero and A.*
3. *Every non-zero homomorphism $f : A \to B$ is injective.*

Proof.

$1 \implies 2$. Obvious.

$2 \implies 3$. $\ker f \subset A$ is an ideal. Since $f \neq 0$, $\ker f \neq A$. Hence $\ker f = 0$.

$3 \implies 1$. Take any $x \neq 0$ in A. Look at $\langle x \rangle$. Define $B = A / \langle x \rangle$. Then take $f : A \to B$ 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 $J \subsetneq J' \subsetneq A$.

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. ☐

Definition 4.4. The set of prime ideals of A is called the **spectrum** of A and is denoted by $\operatorname{Spec} A$.

Proposition 4.5. *If $f : A \to B$ 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
$$\begin{array}{cccc} f^* & : & \operatorname{Spec} B & \longrightarrow & \operatorname{Spec} A \\ & & I \subset B & \longmapsto & f^{-1}(I) \subset A \end{array}.$$

Lecture 3 Wednesday 09/10/19

Remark 4.6. If $f : A \to B$ 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 $0 \subset \mathbb{Q}$ is a maximal ideal and $f^{-1}(0) = 0 \subset \mathbb{Z}$ is not a maximal ideal. For example, $0 \subsetneq \langle 2 \rangle \subsetneq \mathbb{Z}$.

Theorem 4.7. *Let A be a non-zero ring. Then A has at least one maximal ideal. In particular,* $\operatorname{Spec} A$ *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 4.8 (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 4.7. Let Σ be the set of all ideals of A which are not equal to A. Then $0 \in \Sigma$, so $\Sigma \neq \emptyset$. Equip Σ with partial order given by inclusion. It is 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 since T is a chain, 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 $i, k \in T$. Since T is a chain, $i \leq k$ 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. ☐

Corollary 4.9. *Any ideal of A is contained in a maximal ideal of A.*

Proof. If $I \subset A$ is an ideal, apply Theorem 4.7 to A/I. $\square$

Corollary 4.10. *Any non-unit of A is contained in a maximal ideal.*

Proof. Apply Corollary 4.9 to $\langle a \rangle$. $\square$

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

Definition 4.11. 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 4.12 (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 $x_1 \dots x_n \in I_1 \dots I_n \subset \bigcap_{j=1}^n I_j \subset \mathfrak{p}$. Since $x_1 (x_2 \dots x_n) \in \mathfrak{p}$ and $x_1 \notin \mathfrak{p}$, $x_2 \dots x_n \in \mathfrak{p}$. 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 $\mathfrak{p} = I_j$. $\square$

5 Nilradical and the Jacobson radical

Lecture 4 Thursday 10/10/19

Proposition 5.1. *The set $\mathcal{N}(A)$ consisting of all nilpotents of the ring A and zero is an ideal, 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

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

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. $\square$

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

Proposition 5.2. *$\mathcal{N}(A)$ is the intersection of all prime ideals of A.*

Proof.

- $\subset$ 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 $f \in I$.
- $\supset$ 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 Σ be the set of ideals $J \subset A$ such that $J \cap \{f^m \mid m \geq 1\} = \emptyset$. The zero ideal is in Σ. So $\Sigma \neq \emptyset$. Equip Σ with a partial order given by inclusion. Applying Zorn's lemma we obtain that Σ 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. It is 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 Σ, thus $\mathfrak{p} + \langle x \rangle$ is not in Σ. By definition of Σ 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, $f^{n+m} = f^n f^m \in \mathfrak{p} + \langle xy \rangle$. 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.

$\square$

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

Proposition 5.3. *$x \in \mathcal{J}(A)$ if and only if $1 - xy \in A^*$ for all $y \in A$.*

Proof.

$\implies$ Let $x \in \mathcal{J}(A)$. Suppose there exists $y \in A$ such that $1 - xy$ is not a unit. By Corollary 4.10 every non-unit is contained in a maximal ideal. Say $\mathfrak{m} \subset A$ is a maximal ideal and $1 - xy \in \mathfrak{m}$. But $x \in \mathcal{J}(A) \subset \mathfrak{m}$. Then $1 = (1 - xy) + xy \in \mathfrak{m}$, but then $\mathfrak{m} \neq A$. A contradiction.

$\impliedby$ 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 $\mathfrak{m} \subset A$ such that $x \notin \mathfrak{m}$. Then $\mathfrak{m} + \langle x \rangle = A \ni 1$. Thus $1 = m + xy$, where $y \in A$. But by assumption $1 - xy \in A^*$, so $m \in A^*$. But then $\mathfrak{m} = A$. A contradiction.

□

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

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

Proposition 5.4. *The radical of I is the intersection of all prime ideals of A that contain I.*

Proof. Apply Proposition 5.2 to A/I. □

Lecture 5 Tuesday 15/10/19

Definition 5.5. Let I be an indexing set. For each $i \in I$ we are given a ring R_i. Consider the product set

$$\prod_{i \in I} R_i = \left\{ (x_i)_{i \in I} \;\middle|\; x_i \in R_i \right\}.$$

Define

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

Define addition and multiplication coordinate-wise, so

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

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

Remark 5.6. Let $\mathfrak{p}_i$ for $i \in I$ be all prime ideals of R. Let $h_i : R \to R/\mathfrak{p}_i$. Then

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

is a homomorphism, and

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

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 $f_j : R \to R/\mathfrak{m}_j$, so if we take the indexing set J to be the set of all maximal ideals of R, then we obtain an injective map

$$R/\mathcal{J}(R) \hookrightarrow \prod_{j \in J} R/\mathfrak{m}_j,$$

a product of fields.

6 Localisation of rings

Example. Fix a prime p. Then

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

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

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

Check that this is indeed an equivalence relation. [1] 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

$$\frac{a}{s} + \frac{b}{t} = \frac{at + bs}{st}, \qquad \frac{a}{s} \cdot \frac{b}{t} = \frac{ab}{st}, \qquad a, b \in A, \qquad s, t \in S.$$

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

Lemma 6.4. *There is a ring homomorphism*

$$\begin{array}{cccc} f & : & A & \longrightarrow & S^{-1}A \\ & & x & \longmapsto & \dfrac{x}{1} \end{array}.$$

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 $0 \neq a \in A$ such that $ua = 0$. Then

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

So $\ker f$ contains a, hence f is not injective. If f has no zero-divisors, then $ua = u(a - 0) \neq 0$ if $a \neq 0$ and any $u \in S$. Hence $f(a) \neq 0$. ☐

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

Lecture 6
Wednesday
16/10/19

[1] Exercise

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

- If $S = \{1, a, \dots\}$, then
$$S^{-1}\mathbb{Z} = \left\{ \frac{n}{a^m} \;\middle|\; n \in \mathbb{Z},\ m \in \mathbb{Z}_{\geq 0} \right\}.$$
- If $S = \mathbb{Z} \setminus p\mathbb{Z}$, then
$$S^{-1}\mathbb{Z} = \left\{ \frac{n}{m} \;\middle|\; p \nmid m \right\}.$$
- If $S = \mathbb{Z} \setminus \bigcup_{p_i \text{ prime}} p_i\mathbb{Z}$, then
$$S^{-1}\mathbb{Z} = \left\{ \frac{n}{m} \;\middle|\; p_i \nmid m \right\}.$$
- 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
$$S^{-1}\mathbb{Z} = \left\{ \frac{m}{1 + nk} \;\middle|\; m, k \in \mathbb{Z} \right\},$$
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
$$S^{-1}k[x] = k(x) = \left\{ \frac{f(x)}{g(x)} \;\middle|\; g(x) \ \text{arbitrary non-zero polynomial} \right\}.$$

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 $f : A \to S^{-1}A$. Then $a \in \ker f$ 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 $y \in \ker f$. Since f is a homomorphism, $\ker f$ is an ideal. So $\langle y \rangle = yA \subset \ker f$. In general,
$$a = \sum_{i,j \geq 0} a_{ij} x^i y^j \equiv a_{00} + \sum_{i \geq 1} a_{i0} x^i + \sum_{j \geq 1} a_{0j} y^j \mod \langle xy \rangle.$$
Then $\ker f = yA = \langle y \rangle$, since $\sum_{j \geq 1} a_{0j} y^j$ goes to zero, since it is annihilated by x, and $x^n \sum_{i \geq 0} a_{i0} x^i$ is never zero in A. Thus $f(A) = k[x]$, and
$$S^{-1}A = \left\{ \frac{f(x)}{x^n} \;\middle|\; f(x) \in k[x],\ n \geq 0 \right\} = k\left[x, x^{-1}\right] = \left\{ \sum_{i \in \mathbb{Z},\ a_i = 0 \ \text{for almost all} \ i} a_i x^i \;\middle|\; a_i \in k \right\}.$$

Lecture 7 Thursday 17/10/19

Lemma 6.6 (Universal property of localisation). *Let A be a ring, and $S \subset A$ a multiplicative set. Let $g : A \to B$ be a ring homomorphism such that $g(s)$ is a unit in B for all $s \in S$. Then there exists a unique ring homomorphism $h : S^{-1}A \to B$ such that $g = h \circ f$ where $f : A \to S^{-1}A$ is the canonical map, so*
$$\begin{tikzcd} A \arrow[d, "f"'] \arrow[dr, "g"] & \\ S^{-1}A \arrow[r, "\exists! h"'] & B \end{tikzcd}.$$

Proof. Define

$$\begin{array}{rcccl} h & : & S^{-1}A & \longrightarrow & B \\ & & \dfrac{a}{s} & \longmapsto & \dfrac{g(a)}{g(s)}, \qquad a \in A, \qquad s \in S. \end{array}$$

This is well-defined, that is if $a/s = b/t$ then $g(a)/g(s) = g(b)/g(t)$. [2] This is a ring homomorphism. [3] Now easy to check that

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

Moreover, if $h' : S^{-1}A \to B$ 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 ideals $I \subset A$, set

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

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. $S^{-1}(I_1 \cdot \dots \cdot I_n) = S^{-1}I_1 \cdot \dots \cdot S^{-1}I_n$,
3. $S^{-1}\left(\bigcap_{i=1}^n I_i\right) = \bigcap_{j=1}^n S^{-1}I_j$, *and*
4. $S^{-1}(\operatorname{rad} I) = \operatorname{rad} S^{-1}I$ *for every ideal I.*

Proof. Exercise. [4] □

There is a map

$$\{\text{ideals } I \text{ of } A\} \to \left\{\text{ideals } S^{-1}I \text{ of } S^{-1}A\right\}.$$

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

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 $J \subset S^{-1}I$. Conversely, $f(I) = f\left(f^{-1}(J)\right) \subset J$. Thus $S^{-1}I \subset J$. □

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*

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

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 $f^{-1}\left(S^{-1}\mathfrak{p}\right) = \mathfrak{p}$, 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 $sa \in \mathfrak{p}$. Since s is a unit, $a \in \mathfrak{p}$. 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. □

[2] Exercise
[3] Exercise
[4] 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 $\mathrm{U}_I = \operatorname{Spec} R \setminus \mathrm{V}_I$.

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

Proof.

1. If $I = 0$ is the zero ideal, then $\mathrm{V}_0 = \operatorname{Spec} R$, all prime ideals of R. If $I = R$, then no prime ideals of R contain R, so $\mathrm{V}_R = \emptyset$, so 1 holds.
2. It is enough to check that $\mathrm{V}_I \cup \mathrm{V}_J = \mathrm{V}_{IJ} = \mathrm{V}_{I \cap J}$. 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. Let J_i for $i \in S$ be a collection of ideals. Claim that $\bigcap_{i \in S} \mathrm{V}_{J_i} = \mathrm{V}_J$, 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 $i \in S$.

$\square$

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

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

Then $f^* : \operatorname{Spec} B \to \operatorname{Spec} A$ sends $\mathfrak{p} \subset B$ to $f^{-1}(\mathfrak{p})$, which is prime in A. 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 $(f^*)^{-1}(\mathrm{V}_I) = \mathrm{V}_J$ for some ideal J in B. Let J be the smallest ideal in B containing $f(I)$.

- $\subset$ 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.
- $\supset$ 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 $\mathfrak{q} \in (f^*)^{-1}(f^*(\mathfrak{q})) \subset (f^*)^{-1}(\mathrm{V}_I)$, so we are done.

$\square$

Lecture 9 Wednesday 23/10/19

The following are particular cases.

- Assume f is surjective. Then $B \cong A/\ker f$, so
$$\begin{array}{rcl} \{\text{prime ideals in } B\} & \longrightarrow & \{\text{prime ideals in } A \text{ containing } \ker f\} \\ \mathfrak{p} \subset B & \longmapsto & f^{-1}(\mathfrak{p}) \end{array}.$$
So in this case f^* is injective and its image is $\mathrm{V}_{\ker f}$.
- Let S be a multiplicative set in A. Let $f : A \to S^{-1}A$ 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 $f^* : \operatorname{Spec} S^{-1}A \to \operatorname{Spec} A$ 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 $\operatorname{Spec} k$ 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
$$\operatorname{Spec} k[x] = \{0\} \cup \{\langle p(x)\rangle \mid p(x) \text{ is monic and irreducible}\}.$$
In particular, if k is algebraically closed, such as $k = \mathbb{C}$, then
$$\operatorname{Spec} \mathbb{C}[x] = \{0\} \cup \{\langle x - a\rangle \mid a \in k\} = \mathbb{C} \cup \{0\}.$$
- Let $R = \mathbb{Z}$, a PID. Then
$$\operatorname{Spec} \mathbb{Z} = \{0\} \cup \{\langle p\rangle \mid p \text{ is a prime number}\}.$$
- Let $R = \mathbb{Z}[i]$ be the Gaussian integers, a PID. The tautological map $f : \mathbb{Z} \to \mathbb{Z}[i]$ gives rise to $f^* : \operatorname{Spec} \mathbb{Z}[i] \to \operatorname{Spec} \mathbb{Z}$. 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 $p \equiv 1 \mod 4$, then $p = (a+bi)(a-bi)$. In this case $a+bi$ and $a-bi$ are not associated primes.
  - If $p \equiv 3 \mod 4$, then p stays prime in $\mathbb{Z}[i]$.

  Then
$$\begin{array}{ccccl} \operatorname{Spec} \mathbb{Z}[i] & \longrightarrow & \operatorname{Spec} \mathbb{Z} & & \\ 0 & \longmapsto & 0 & & \\ \langle 1+i\rangle & \longmapsto & \langle 2\rangle & \text{ramified} & . \\ \langle 3\rangle & \longmapsto & \langle 3\rangle & \text{inert} & \\ \langle 1+2i\rangle, \langle 1-2i\rangle & \longmapsto & \langle 5\rangle & \text{split} & \end{array}$$
- Let R be an integral domain and let k be the fraction field of R, so $f : R \hookrightarrow k$. Then $\operatorname{Spec} k = \{0\}$ and $f^* : \operatorname{Spec} k \to \operatorname{Spec} R$.
- Let k be a field, so $f : k \hookrightarrow k[x]$. Then $f^* : \operatorname{Spec} k[x] \to \operatorname{Spec} k$. If $\mathfrak{p} \subset k[x]$, then $\mathfrak{p} \cap k = 0$, 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 $\mathfrak{p} \subset R$ is a prime ideal, then the closure of $\mathfrak{p}$ is $\mathrm{V}_{\mathfrak{p}}$. Any closed subset of $\operatorname{Spec} R$ containing $\mathfrak{p}$ is V_J, where $J \subset \mathfrak{p}$. This V_J visibly contains $\mathrm{V}_{\mathfrak{p}}$. Hence $\mathrm{V}_{\mathfrak{p}}$ is the intersection of all such V_J.

Example. In $\operatorname{Spec} \mathbb{Z}$, the point $\langle p\rangle$ is closed, because $\mathrm{V}_{\langle p\rangle} = \{\langle p\rangle\}$. The point zero is not closed, as $\mathrm{V}_0 = \operatorname{Spec} \mathbb{Z}$. The closure of zero is all of $\operatorname{Spec} \mathbb{Z}$.

Example. Let $R = k[[t]]$. By sheet 1, this is a local ring. Its unique maximal ideal is $\langle t\rangle$. This is also a unique non-zero prime ideal. [5] All ideals are zero and $\langle t^n\rangle$. Then $\operatorname{Spec} k[[t]] = \{0, \langle t\rangle\}$, where zero is not a closed point, since its closure is $\operatorname{Spec} k[[t]]$, and $\langle t\rangle$ is a closed point.

[5] 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 $a_{ij} \in R$.

Definition 8.1. The **determinant** of A is

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

where $\mathcal{S}_n$ is the symmetric group and $\operatorname{sgn} : \mathcal{S}_n \to \{\pm 1\}$.

Definition 8.2. The i,j**-minor** of A is

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

Proposition 8.3.

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

Definition 8.4. The **adjoint matrix** of A is the $n \times n$ matrix $A^\vee$ with entries

$$\left(A^\vee\right)_{ij} = (-1)^{i+j} \mathrm{M}_{ji} \qquad \Longleftrightarrow \qquad A^\vee = \left((-1)^{i+j} \mathrm{M}_{ij}\right)^{\intercal}.$$

Theorem 8.5 (Determinant trick)**.**

$$A \cdot A^\vee = A^\vee \cdot A = \det A \cdot \mathrm{I}_n,$$

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 $A \times M \to M$ such that

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

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 $n \cdot g = g + \dots + g$ for $n \in \mathbb{Z}_{>0}$, and $0 \cdot g = 0$ and $(-n) \cdot g = -(n \cdot g)$.
- 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 $L : V \to V$. Here x acts on V as L.

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

Then $\ker f$, $\operatorname{im} f$, and $\operatorname{coker} f = N / \operatorname{im} f$ are R-modules.

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

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 $rf(x) \in N$. A warning is 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

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

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 $m = r_1 x_1 + \dots + r_n x_n$.

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

$$\begin{array}{cccc} f & : & R^{\oplus n} & \longrightarrow & M \\ & & (t_1, \dots, t_n) & \longmapsto & t_1 x_1 + \dots + t_n x_n \end{array}.$$

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

$$JM = \{\text{finite sums } r_1 m_1 + \dots + r_k m_k\} \subset M.$$

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. Since $m_i \in M = JM$,

$$m_1 = x_{11} m_1 + \dots + x_{1n} m_n, \qquad \dots, \qquad m_n = x_{n1} m_1 + \dots + x_{nn} m_n, \qquad x_{ij} \in J.$$

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

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

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

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

We have $\det (\mathrm{I}_n - X) \in A$. Then $\det (\mathrm{I}_n - X)$ 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, $\det (\mathrm{I}_n - X) = 1 - a$, where $a \in J$. Now, $(1 - a) m_i = 0$ for $i = 1, \dots, n$. Hence $(1 - a) M = 0$. ☐

Lecture 11 Tuesday 29/10/19

Remark. If M is not finitely generated then this is false. For example, let $A = \mathbb{Z}$ 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 $f : M \to M$ 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 $f(rx) = r f(x)$ for all $r \in R$. Then M is finitely generated also as an A-module. Since $f(M) = M$, $tM = M$. 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 $v = 0$. ☐

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. By Lemma 9.7, 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 $M = u(1 - a) M = 0$. ☐

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 $M/N = 0$. ☐

Recall that 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. [6] 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, such as $A = \mathbb{Z}$ and $\mathfrak{p} = \langle p \rangle \subseteq \mathbb{Z}_{\mathfrak{p}} = \{a/b \mid (b, p) = 1\}$.

Theorem 9.11. *Let R be a local ring with maximal ideal $J \subset R$ 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 $\widetilde{v_1}, \dots, \widetilde{v_n} \in M$ to be representatives of $v_1, \dots, v_n$ respectively, that is $v_i = \widetilde{v_i} + JM$. Then $\widetilde{v_1}, \dots, \widetilde{v_n}$ 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 minimal sets of generators have n elements, where $n = \dim_k M/JM$.*

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
$$N = R\widetilde{v_1} + \dots + R\widetilde{v_n} = \{r_1\widetilde{v_1} + \dots + r_n\widetilde{v_n} \mid r_i \in R\} \subset M.$$
Since M/JM is generated by $v_1, \dots, v_n$, $M = N + JM$, since $M/JM = N/JN$. By Corollary 9.10 we have $M = N$. If a proper subset of $\widetilde{v_1}, \dots, \widetilde{v_n}$ generates M, then a proper subset of $v_1, \dots, v_n$ generates an n-dimensional vector space. A contradiction.
Lecture 12 Wednesday 30/10/19
3. Suppose $m_1, \dots, m_n$ is any minimal generating set of the R-module M. Consider $\overline{m_1}, \dots, \overline{m_n} \in M/JM$. Then $\overline{m_1}, \dots, \overline{m_n}$ span the vector space M/JM. If this is not a basis, then M/JM is spanned by a proper subset of $\overline{m_1}, \dots, \overline{m_n}$. In particular, a basis is a proper subset. By part 2 a proper subset of $m_1, \dots, m_n$ generates M. This contradicts the minimality of $m_1, \dots, m_n$.

□

The moral of the story is any finitely generated module M over a local ring R has a minimal set of generators. Then $m_1, \dots, m_n$ is a minimal set of generators of M if and only if $\overline{m_1}, \dots, \overline{m_n}$ is a basis of the k-vector space M/JM, and n is well-defined.

10 Localisation of modules

Let A be a ring with a multiplicative set $S \subset A$.

Definition 10.1. Let M be an A-module. Consider the set $M \times S$. Equip it with a relation $\sim$ such that
$$(m, s) \sim (n, t) \qquad \iff \qquad \exists u \in S,\ u(mt - ns) = 0.$$
This is an equivalence relation.

- Define $S^{-1}M$ as the set of equivalence classes.
- The equivalence class of (m, s) is written as m/s.

Turn $S^{-1}M$ into a $S^{-1}A$-module as follows. Let $0/1 \in S^{-1}M$, and
$$\frac{m}{s} + \frac{b}{t} = \frac{mt + bs}{st}, \qquad \frac{a}{s} \cdot \frac{m}{t} = \frac{am}{st}, \qquad a \in A, \qquad m \in M, \qquad s, t \in S.$$
This is the **localisation of M with respect to S**.

[6] Exercise

Now let us consider a particular kind of multiplicative set.

Definition 10.2. Let $\mathfrak{p} \subset A$ be a prime ideal. Let $S = A \setminus \mathfrak{p}$. This is a multiplicative set. Then the **localisation** $S^{-1}A$ **of** A **at** $\mathfrak{p}$ is written as $A_{\mathfrak{p}}$.

Theorem 10.3. *Let $\mathfrak{p} \subset A$ be a prime ideal. Then $A_{\mathfrak{p}}$ is a local ring with unique maximal ideal*

$$\mathfrak{p}A_{\mathfrak{p}} = \left\{ \frac{x}{y} \;\middle|\; x \in \mathfrak{p},\ y \notin \mathfrak{p} \right\}.$$

Remark. In general, a ring R with an ideal J is a local ring with maximal ideal J if and only if $R^* = R \setminus J$. Indeed, if $J \subset R$ is a maximal ideal, then for any $x \in R \setminus J$, $J + xR$ contains one. This forces x to be a unit. Conversely, if $R^* = R \setminus J$ then J is maximal and is a unique maximal ideal.

Proof. Suppose $a/s \in A_{\mathfrak{p}}^*$. Then $a/s \cdot b/t = 1/1$ for some $b \in A$ and $t \in A \setminus \mathfrak{p}$. By definition $u\,(ab - st) = 0$ for $u \in A \setminus \mathfrak{p}$, so $uab = ust \notin \mathfrak{p}$, since all factors are in $S = A \setminus \mathfrak{p}$. Therefore, $a \notin \mathfrak{p}$, hence $a/s \notin \mathfrak{p}A_{\mathfrak{p}}$. Conversely, if $a/s \notin \mathfrak{p}A_{\mathfrak{p}}$ for $s \notin \mathfrak{p}$, then $a \notin \mathfrak{p}$. Thus a/s is a unit in $A_{\mathfrak{p}}$ because $a/s \cdot s/a = 1$. ☐

Example 10.4. Let $R = \mathbb{Z}$ and $\mathfrak{p} = \langle p \rangle$. Then

$$p\mathbb{Z}_{\langle p \rangle} = \left\{ \frac{x}{y} \;\middle|\; p \mid x,\ p \nmid y \right\} \subset \left\{ \frac{x}{y} \;\middle|\; x \in \mathbb{Z},\ p \nmid y \right\} = \mathbb{Z}_{\langle p \rangle}$$

is the unique maximal ideal.

Proposition 10.5. *Let M be an A-module. Consider $M_{\mathfrak{m}} = (A \setminus \mathfrak{m})^{-1} M$, where $\mathfrak{m} \subset A$ is a maximal ideal. Then $M = 0$ if and only if $M_{\mathfrak{m}} = 0$ for any maximal ideal $\mathfrak{m} \subset A$.*

Proof.

$\Longrightarrow$ Obvious.

$\Longleftarrow$ Assume $M \neq 0$, so there exists $0 \neq x \in M$. Define

$$I = \operatorname{Ann} x = \{a \in A \mid ax = 0\},$$

so $1 \notin I$ since $x \neq 0$. Choose a maximal ideal $\mathfrak{m}$ containing I. If $M_{\mathfrak{m}} = 0$, then $x/1 = 0$. We know that $x \in \ker(M \to M_{\mathfrak{m}})$ if and only if $ux = 0$ for some $u \in A \setminus \mathfrak{m}$. A contradiction, since $I \subset \mathfrak{m}$.

☐

The following is a corollary. Let M be a finitely generated A-module. Then $m_1, \dots, m_n$ generate M if and only if $m_1, \dots, m_n$ generate the $A_{\mathfrak{m}}$-module $M_{\mathfrak{m}}$ for any maximal ideal $\mathfrak{m} \subset A$. By Theorem 9.11 applied to $A_{\mathfrak{m}}$, this is if and only if the images $\overline{m_1}, \dots, \overline{m_n}$ in $M/\mathfrak{m}M \cong M_{\mathfrak{m}}/\mathfrak{m}M_{\mathfrak{m}}$ generate the $k(\mathfrak{m})$-vector space, where $k(\mathfrak{m}) = A/\mathfrak{m}$, for every maximal ideal $\mathfrak{m} \subset A$.

Corollary 10.6. *Assume A is an integral domain with field of fractions K. In this case A is a subring of K. For any prime ideal $\mathfrak{p} \subset A$ the local ring $A_{\mathfrak{p}}$ is also a subring of K. Then*

$$A = \bigcap_{\text{all prime ideals } \mathfrak{p} \subset A} A_{\mathfrak{p}},$$

as subsets of K.

Proof. Clearly, $A \subset A_{\mathfrak{p}}$, so the left hand side is in the right hand side. Let us prove that if $x \in K$ is contained in each $A_{\mathfrak{p}}$, then $x \in A$. Consider

$$I = \{a \in A \mid ax \in A\}.$$

Visibly, I is an ideal in A. We are given that $x = m/s$, where $m \in A$ and $s \in A \setminus \mathfrak{p}$. Hence $s \in I$. So I contains an element not in $\mathfrak{p}$ for every $\mathfrak{p}$. Then $I = A$, because otherwise I is contained in some maximal ideal but maximal ideals are prime. Hence $1 \in I$, so $x \in A$. ☐

Lecture 13 is a problems class. Lecture 13 Thursday 31/10/19

Lecture 14 is a class test. Lecture 14 Tuesday 05/11/19

11 Chain conditions

Lecture 15 Wednesday 06/11/19

Lemma 11.1. *Let Σ be a partially ordered set. The following are equivalent.*

- *Every maximal non-empty subset of Σ has a maximal element, so no element of the subset is bigger.*
- *Every ascending chain of elements of Σ is stationary, so there exists $i_0 \in I$ such that $a_{i_0} = a_i$ for all $i > i_0$.*

Proof.

$\implies$ Take a maximal element of the chain, say a_{i_0}. Then for any $i \ge i_0$ we have $a_i = a_{i_0}$.

$\impliedby$ Suppose $S \subset \Sigma$ has no maximal element. Then choose any element in S, say a_1. This is not maximal, so can choose $a_2 \in S$ such that $a_1 < a_2$. Keep doing this, get an infinite chain which is not stationary, because $a_i \neq a_j$ for all $i \neq j$.

□

Definition 11.2. Let A be a ring and let M be an A-module. Then M is called **Noetherian** if any ascending chain of submodules of M is stationary. In other words, if $M_1 \subset M_2 \subset \dots \subset M$ are A-submodules, then there exists n such that $M_n = M_{n+1} = \dots$. Then M is called **Artinian** if any descending chain of submodules of M is stationary. The ring A is **Noetherian**, or **Artinian**, if such is the A-module A.

Proposition 11.3. *Let A be a ring and let M be an A-module. The following are equivalent.*

- *M is Noetherian.*
- *Every A-submodule of M is finitely generated.*

In particular, A is a Noetherian ring if and only if every ideal in A is finitely generated.

Proof.

$\implies$ Suppose that $N \subset M$ is a submodule which is not finitely generated. Let $N_1 = 0$. Since N is not finitely generated we can find $0 \neq x \in N$ such that $N_2 = Ax$, the submodule generated by x, and $N \neq N_2$. So we continue. If $0 = N_1 \subsetneq \dots \subsetneq N_m$ are constructed, then $N_m \neq N$, so there exists $y \in N$ such that $y \notin N_m$. Define $N_{m+1} = N_m + Ay$, the smallest module containing N_m and y. Since N is not finitely generated, this chain is not stationary.

$\impliedby$ Let $M_1 \subset M_2 \subset \dots \subset M$. Must prove that this chain is stationary. Define

$$N = \bigcup_{i \in I} M_i.$$

This is a submodule of M. We know that $N = Rx_1 + \dots + Rx_n$ where $x_1, \dots, x_n \in N$. Then x_k is contained in some M_{i_k}. Suppose that $i_0 = \max\{i_1, \dots, i_n\}$. Then $x_{i_1}, \dots, x_{i_n} \in M_{i_0}$, since $M_{i_1} \subset M_{i_0}, \dots, M_{i_k} \subset M_{i_0}$. But now we see that $M_{i_0} \supset N$. Since $M_{i_0} \subset N$, we must have $N = M_{i_0}$. Hence $M_{i_0} = M_{i_0+1} = \dots$.

□

Proposition 11.4. *Suppose M is an A-module. Let $N \subset M$ be a submodule. Then M is Noetherian if and only if N and M/N are both Noetherian, and M is Artinian if and only if N and M/N are both Artinian.*

Proof. The Noetherian case.

$\implies$ Suppose M is Noetherian. Ascending chains of submodules of N are ascending chains of submodules of M, so must be stationary. Let $f : M \twoheadrightarrow N$ be the canonical map. If $L_1 \subset L_2 \subset \dots$ is a chain of submodules of M/N, then $f^{-1}(L_1) \subset f^{-1}(L_2) \subset \dots$ is a chain of submodules of M. This is stationary. Since $f\left(f^{-1}(L_i)\right) = L_i$, the original chain of L_i's is stationary.

Lecture 16 Thursday 07/11/19

$\impliedby$ Now assume that N and M/N are Noetherian. We need to prove that an ascending chain $M_1 \subset M_2 \subset \dots$ of submodules of M is stationary. Then $N \cap M_1 \subset N \cap M_2 \subset \dots$ is a chain of submodules of N. Similarly, $M_1/(N \cap M_1) \subset M_2/(N \cap M_2) \subset \dots$. Indeed, $M_1 \to M_2$ is clearly injective, and $\ker(M_1 \to M_2/(N \cap M_2)) = N \cap M_1$. Therefore, $M_1/(N \cap M_1)$ injectively maps to $M_2/(N \cap M_2)$.

Then

$$\begin{tikzcd} M_1/\left(M_1 \cap N\right) \arrow[r, hook] & M_2/\left(M_2 \cap N\right) \arrow[r, hook] & \dots \arrow[r, hook] & M/N \\ M_1 \arrow[r, hook] \arrow[u, two heads] & M_2 \arrow[r, hook] \arrow[u, two heads] & \dots \arrow[r, hook] & M \arrow[u, two heads] \\ M_1 \cap N \arrow[r, hook] \arrow[u, hook] & M_2 \cap N \arrow[r, hook] \arrow[u, hook] & \dots \arrow[r, hook] & M \arrow[u, hook] \end{tikzcd}.$$

If F and G are submodules of H, then we have a natural map

$$\begin{array}{ccc} F & \longrightarrow & \left(F+G\right)/G \\ x & \longmapsto & x+G \end{array}.$$

The kernel of this map is $F \cap G$. The map $F \to \left(F+G\right)/G$ is surjective. So we have a canonical isomorphism $F/\left(F \cap G\right) \xrightarrow{\sim} \left(F+G\right)/G$. Apply this to $F = M_i$, $G = N$, and $H = M$. Then

$$\begin{tikzcd} \left(M_1+N\right)/N \arrow[r, hook] & \left(M_2+N\right)/N \arrow[r, hook] & \dots \arrow[r, hook] & M/N \\ M_1/\left(M_1 \cap N\right) \arrow[r, hook] \arrow[u, "\sim"] & M_2/\left(M_2 \cap N\right) \arrow[r, hook] \arrow[u, "\sim"] & \dots \arrow[r, hook] & M/N \arrow[u, "\sim"] \end{tikzcd}.$$

There exists $a \in \mathbb{N}$ such that $M_i \cap N = M_a \cap N$ for all $i \geq a$. There exists $b \in \mathbb{N}$ such that $\left(M_i+N\right)/N = \left(M_b+N\right)/N$ for all $i \geq b$. Define $c = \max\left\{a, b\right\}$. Then

$$\begin{tikzcd} \left(M_c+N\right)/N \arrow[r, "\sim"] & \left(M_i+N\right)/N \\ y \in M_c \arrow[r, hook] \arrow[u, two heads] & M_i \ni x \arrow[u, two heads] \\ M_c \cap N \arrow[r, "\sim"'] \arrow[u, hook] & M_i \cap N \arrow[u, hook] \end{tikzcd}.$$

Claim that $M_i = M_c$ for all $i \geq c$. It remains to show that any $x \in M_i$ is in fact in M_c. Since the top arrow is an isomorphism, and $M_c \to \left(M_c+N\right)/N$ is surjective, we can find $y \in M_c$ whose image in $\left(M_i+N\right)/N$ is equal to the image of x. Then $x - y \in M_i$ goes to zero in $\left(M_i+N\right)/N$. Thus $x - y \in M_i \cap N$. Hence $x - y \in M_c \cap N \subset M_c$. Hence $x = (x-y) + y \in M_c$. Therefore, $M_c = M_i$.

□

Corollary 11.5. *Let A be a Noetherian ring and let M be a finitely generated A-module. Then M is Noetherian. Similarly, if A is Artinian, then any finitely generated A-module is Artinian.*

Proof. Recall that any finitely generated A-module is a quotient of a free module $A^{\oplus n} = A \oplus \dots \oplus A$. Proposition 11.4 implies that since A is a submodule of $A^{\oplus 2}$ via $x \mapsto (x, 0)$, and the quotient is isomorphic to A, that $A^{\oplus 2}$ is Noetherian. Hence $A^{\oplus n}$ is Noetherian. Applying Proposition 11.4 to the surjective map $A^{\oplus n} \to M$ we prove that M is Noetherian. □

Corollary 11.6. *Let M be an A-module. If $0 = M_0 \subset \dots \subset M_n = M$ are A-submodules such that M_{i+1}/M_i is a Noetherian A-module, then M is also a Noetherian A-module. The same statement is true for Artinian modules.*

Proof. Apply Proposition 11.4. Since M_1/M_0 is Noetherian and M_2/M_1 is Noetherian, M_2 is Noetherian, etc. □

Lemma 11.7. *Let A be a Noetherian ring. Let $S \subset A$ be a multiplicative set. Then $S^{-1}A$ is Noetherian.*

Proof. By Lemma 11.1 it is enough to prove that any non-empty set of ideals of $S^{-1}A$ has a maximal element. So take J a non-empty set of ideals of $S^{-1}A$. Let

$$\begin{array}{ccccc} f & : & A & \longrightarrow & S^{-1}A \\ & & a & \longmapsto & \dfrac{a}{1} \end{array}.$$

Consider $\left\{f^{-1}\left(I\right) \mid I \in J\right\}$. This is a set of ideals of A. It has a maximal element, say I_0, since A is Noetherian. Then $I_0 = S^{-1}f\left(I_0\right)$ is a maximal element of J. □

12 Primary decomposition

Definition 12.1. An ideal $I \subsetneq R$ is called **primary** if for all $x, y \in R$ such that $xy \in I$ we have either $x \in I$ or $y^n \in I$ for some $n \geq 1$. Equivalently, every zero-divisor in R/I is a nilpotent element of R/I.

Example. If $R = \mathbb{Z}$ and p a prime number then $\langle p^n \rangle$ is a primary ideal.

Lecture 17 Tuesday 12/11/19

Proposition 12.2. *If* $\operatorname{rad} I$ *is a maximal ideal, then* I *is primary. In particular, any power of a maximal ideal is primary.*

Proof. Recall $\operatorname{rad} I$ is the intersection of all prime ideals containing I. In particular, if $\operatorname{rad} I$ is a maximal ideal, then it is a unique prime ideal containing I. Then R/I has a unique prime ideal $\operatorname{rad} I/I$, so R/I is a local ring. Hence $\mathcal{N}(R/I) = \mathcal{J}(R/I) = \operatorname{rad} I/I$. Clearly, $(R/I) \setminus (\operatorname{rad} I/I) = (R/I)^*$. Thus any element of R/I is either a unit, or a nilpotent element. Hence I is primary. If $\mathfrak{m} \subset R$ is a maximal ideal, then $\operatorname{rad} \mathfrak{m}^n = \mathfrak{m}$. ☐

Proposition 12.3. *Let* $I \subset R$ *be a primary ideal. Then* $\operatorname{rad} I$ *is a prime ideal. This is the smallest prime ideal of* R *that contains* I*.*

Remark.

$$\{\text{ideals } I \subset R \mid \operatorname{rad} I \text{ is a maximal ideal}\} \subset \{\text{primary ideals}\} \subset \{\text{ideals } I \subset R \mid \operatorname{rad} I \text{ is a prime ideal}\}.$$

Proof. Suppose $xy \in \operatorname{rad} I$, so $x^m y^m = (xy)^m \in I$, but $x \notin \operatorname{rad} I$, so $x^m \notin I$. So in R/I we have $x^m y^m = 0$ and $x^m \neq 0$. Since I is primary, every zero-divisor in R/I is nilpotent. Hence $(y^m)^n = 0$ for some $n \geq 1$. But then in R we have $y^{mn} \in I$, so $y \in \operatorname{rad} I$. This proves that $\operatorname{rad} I$ is prime. Recall that $\operatorname{rad} I$ is the intersection of all prime ideals containing I. If $\operatorname{rad} I$ is already a prime ideal, it is the smallest ideal containing I. ☐

A **primary decomposition** of an ideal $I \subset R$ is the representation

$$I = \bigcap_{m=1} J_m,$$

where $J_1, \dots, J_m$ are primary ideals of R. The aim is that any ideal in a Noetherian ring has a primary decomposition.

Example. Let $R = \mathbb{Z}$. Then $n = \prod_{i=1}^m p_i^{a_i}$, where p_i's are prime numbers, and $a_i \geq 1$, so

$$\langle n \rangle = \prod_{i=1}^m \langle p_i^{a_i} \rangle = \bigcap_{i=1}^m \langle p_i^{a_i} \rangle.$$

Clearly, $\langle p_i \rangle$ are maximal ideals of $\mathbb{Z}$. So, $\langle p_i^{a_i} \rangle$ are primary ideals of $\mathbb{Z}$.

Definition 12.4. Let $I \subsetneq R$ be an ideal. Then I is called **irreducible** if for any ideals J and K of R such that $I = J \cap K$ we have $I = J$ or $I = K$. In other words, I is irreducible if $I \neq J \cap K$, where $I \subsetneq J$ and $I \subsetneq K$.

Proposition 12.5.

1. *Any prime ideal is irreducible.*
2. *In a Noetherian ring, any irreducible ideal is primary.*

Thus

$$\{\text{prime ideals}\} \subset \{\text{irreducible ideals}\} \subset \{\text{primary ideals}\}.$$

Exercise. Show that these are strict in general.

Proof.

1. Suppose $\mathfrak{p} \subset R$ is a prime ideal such that $\mathfrak{p} = J \cap K$, where $\mathfrak{p} \neq J$ and $\mathfrak{p} \neq K$. Let $x \in J \setminus \mathfrak{p}$ and $y \in K \setminus \mathfrak{p}$. Then $xy \in JK \subset J \cap K = \mathfrak{p}$. This is a contradiction, since $\mathfrak{p}$ is prime.

2. Let I be an irreducible ideal of a Noetherian ring R. Consider R/I. Suppose $x, y \in R/I$ such that $xy = 0$ and $x \neq 0$. The task is to show that $y^n = 0$ for some $n \geq 1$. Since R is Noetherian, R/I is Noetherian. Consider
$$\operatorname{Ann} y^m = \{\alpha \in R/I \mid \alpha y^m = 0\}.$$
Then $\operatorname{Ann} y \subset \operatorname{Ann} y^2 \subset \dots \subset R/I$. There exists n such that $\operatorname{Ann} y^n = \operatorname{Ann} y^{n+i}$, for all $i \geq 0$. Claim that $\langle x \rangle \cap \langle y^n \rangle = 0$. Suppose $0 \neq a \in \langle x \rangle \cap \langle y^n \rangle$. Then $ay = 0$ and also $a = by^n$ for some $b \in R/I$. Then $0 = ay = by^{n+1}$. This says that $b \in \operatorname{Ann} y^{n+1} = \operatorname{Ann} y^n$. Hence $by^n = 0$, so $a = 0$, a contradiction. But the ideal $I \subset R$ is irreducible, hence the ideal $0 \subset R/I$ is irreducible. We know that $\langle x \rangle \neq 0$. Thus $\langle y^n \rangle = 0$, so $y^n = 0$. This finishes the proof.

□

Lecture 18 Wednesday 13/11/19

Theorem 12.6 (Noether)**.** *Every ideal in a Noetherian ring has a primary decomposition.*

Proof. We shall in fact prove that every ideal is a finite intersection of irreducible ideals. Suppose this does not hold for a Noetherian ring R. Let Σ be the set of proper ideals of R that are not finite intersections of irreducible ideals. Assume $\Sigma \neq \emptyset$. In a Noetherian ring every non-empty set of ideals has a maximal element. Take a maximal element of Σ. This is an ideal $I \subsetneq R$. Then I is not a finite intersection of irreducible ideals, in particular I is not irreducible. Thus $I = J \cap K$, where $J \supsetneq I$ and $K \supsetneq I$ are ideals of R. Since I is a maximal element of Σ, we can write $J = \bigcap_{m=1}^n J_m$ and $K = \bigcap_{s=1}^r K_s$, where each J_m and each K_s is irreducible. Hence
$$I = \left(\bigcap_{m=1}^n J_m\right) \cap \left(\bigcap_{s=1}^r K_s\right)$$
is a finite intersection of irreducible ideals. This is a contradiction. This shows that $\Sigma = \emptyset$. □

Lemma 12.7. *Let $I_1, \dots, I_n$ be primary ideals in R such that $\operatorname{rad} I_1 = \dots = \operatorname{rad} I_n$. Then $\bigcap_{j=1}^n I_j$ is also a primary ideal and*
$$\operatorname{rad} \bigcap_{j=1}^n I_j = \operatorname{rad} I_1 = \dots = \operatorname{rad} I_n.$$

Proof. Let $\mathfrak{p} = \operatorname{rad} I_j$ for $j = 1, \dots, n$, and let $I = \bigcap_{j=1}^n I_j$. Suppose $x, y \in R$ such that $xy \in I$, but $x \notin I$. Hence $x \notin I_j$ for some j. We have $xy \in I_j$ but $x \notin I_j$ thus $y \in \operatorname{rad} I_j$, since I_j is primary. So $y \in \mathfrak{p}$. Then
$$\operatorname{rad} I = \operatorname{rad} \bigcap_{j=1}^n I_j = \bigcap_{j=1}^n \operatorname{rad} I_j = \mathfrak{p},$$
by problem sheet 2 question 2(b). Hence $y \in \operatorname{rad} I$. This shows that I is primary. Moreover, $\operatorname{rad} I = \mathfrak{p}$. □

Lemma 12.8. *Let I be a primary ideal of R such that $\operatorname{rad} I$ is a prime ideal $\mathfrak{p}$. We say that I is a* ***$\mathfrak{p}$-primary ideal****. Then*
$$(I : \langle x \rangle) = \begin{cases} R & x \in I \\ \text{a } \mathfrak{p}\text{-primary ideal} & x \notin I \end{cases}.$$

Proof. If $x \in I$, then $1 \in (I : \langle x \rangle)$. Hence $(I : \langle x \rangle) = R$. Now assume $x \notin I$. Then $(I : \langle x \rangle) = \{y \in R \mid xy \in I\}$. Since I is primary, this implies $y^n \in I$ and $y \in \operatorname{rad} I = \mathfrak{p}$. So $I \subset (I : \langle x \rangle) \subset \mathfrak{p}$, so $\mathfrak{p} = \operatorname{rad} I \subset \operatorname{rad}(I : \langle x \rangle) \subset \mathfrak{p}$, so $\operatorname{rad}(I : \langle x \rangle) = \mathfrak{p}$. It remains to show that $(I : \langle x \rangle)$ is primary. Assume $yz \in (I : \langle x \rangle)$ whereas $y \notin \operatorname{rad}(I : \langle x \rangle) = \mathfrak{p}$. We must show that $z \in (I : \langle x \rangle)$. Since $yz \in (I : \langle x \rangle)$, $y(xz) = xyz \in I$. Then I is primary and $y \notin \mathfrak{p} = \operatorname{rad} I$. So no power of y is contained in I, therefore $xz \in I$, so $z \in (I : \langle x \rangle)$. □

Call a primary decomposition $I = \bigcap_{j=1}^{k} I_j$ **minimal** if

1. $\operatorname{rad} I_j \neq \operatorname{rad} I_k$ for $j \neq k$, and
2. for every $j = 1, \dots, n$, $\bigcap_{k=1,\ k \neq j}^{n} I_k \not\subset I_j$.

Can achieve 1 by Lemma 12.7.

Theorem 12.9 (First uniqueness theorem)**.** *Let $I = \bigcap_{j=1}^{n} I_j$ be a minimal primary decomposition. Write $\mathfrak{p}_j = \operatorname{rad} I_j$ for $j = 1, \dots, n$. Then the prime ideals $\mathfrak{p}_1, \dots, \mathfrak{p}_n$ are precisely recovered as the prime ideals of R of the form* $\operatorname{rad}(I : \langle x \rangle)$*, where $x \in R$. In particular, $\mathfrak{p}_1, \dots, \mathfrak{p}_n$ do not depend on the primary decomposition chosen.*

Lecture 19 Thursday 14/11/19

Proof. Take any $x \in R$. Then

$$(I : \langle x \rangle) = \left(\bigcap_{j=1}^{k} I_j : \langle x \rangle \right) = \left\{ y \in R \;\middle|\; xy \in \bigcap_{j=1}^{k} I_j \right\} = \bigcap_{j=1}^{k} \{ y \in R \mid xy \in I_j \} = \bigcap_{j=1}^{k} (I_j : \langle x \rangle).$$

Take the radicals of these ideals. Problem sheet 2 question 2(b) says that the radical of an intersection is the intersection of their radicals, so $\operatorname{rad}(I : \langle x \rangle) = \bigcap_{j=1}^{k} \operatorname{rad}(I_j : \langle x \rangle)$. Note that by Lemma 12.8

$$\operatorname{rad}(I_j : \langle x \rangle) = \begin{cases} R & x \in I_j \\ \mathfrak{p}_j & x \notin I_j \end{cases},$$

so $\operatorname{rad}(I : \langle x \rangle) = \bigcap_{x \notin I_j} \mathfrak{p}_j$. Lemma 4.12 says that $\mathfrak{p} = \bigcap_{i=1}^{m} J_i$ is prime implies that $\mathfrak{p}$ is one of the J_i's. Hence if $\operatorname{rad}(I : \langle x \rangle)$ is a prime ideal, then it is one of $\mathfrak{p}_j = \operatorname{rad}(I_j : \langle x \rangle)$ for $x \notin I_j$. So we recover all of $\mathfrak{p}_1, \dots, \mathfrak{p}_n$ and nothing else. ☐

Remark. These prime ideals $\mathfrak{p}_1, \dots, \mathfrak{p}_n$ are called the **associated primes** of I.

Example.

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

$$\{\text{prime ideals}\} = \{0\} \cup \{\text{maximal ideals}\} = \{0\} \cup \{\langle p \rangle \mid p \text{ prime}\},$$
$$\{\text{primary ideals}\} = \{\text{irreducible ideals}\} = \{0\} \cup \{\langle p^n \rangle \mid p \text{ prime}\}.$$

  For example, $\langle 4 \rangle \subsetneq \langle 2 \rangle \subsetneq \mathbb{Z}$ is irreducible.

- Let $R = k[x]$ for k a field. Then

$$\{\text{prime ideals}\} = \{0\} \cup \{\text{maximal ideals}\} = \{0\} \cup \{\langle p(x) \rangle \mid p(x) \text{ monic irreducible polynomial}\},$$
$$\{\text{primary ideals}\} = \{\text{irreducible ideals}\} = \{0\} \cup \{\langle p(x)^n \rangle \mid p(x) \text{ monic irreducible polynomial}\}.$$

- Let $R = k[x, y]$.
  - $\langle x \rangle$ is prime, since $k[x, y] / \langle x \rangle \cong k[y]$ is an integral domain.
  - $\langle x, y \rangle$ is maximal, since $k[x, y] / \langle x, y \rangle \cong k$ is a field.
  - $\langle x, y^2 \rangle$ is not prime, since $k[x, y] / \langle x, y^2 \rangle \cong k \oplus ky$ is not an integral domain, where $y^2 = 0$. Then $\operatorname{rad}\langle x, y^2 \rangle = \langle x, y \rangle$, so Proposition 12.2 implies that $\langle x, y^2 \rangle$ is primary.
  - $\langle xy \rangle$ is not prime, since $x^n, y^n \notin \langle xy \rangle$ for all $n \geq 1$ and $xy \in \langle xy \rangle$, and $k[x, y] / \langle xy \rangle$ has zero-divisors which are not nilpotent, so $\langle xy \rangle$ is also not primary. Then $\langle xy \rangle = \langle x \rangle \langle y \rangle = \langle x \rangle \cap \langle y \rangle$ is a primary decomposition, where $\langle x \rangle$ and $\langle y \rangle$ are prime, hence primary.
  - $\langle x^a y^b \rangle = \langle x^a \rangle \cap \langle y^b \rangle$ for $a, b \geq 1$ is a primary decomposition, since $\langle x^a \rangle$ and $\langle y^b \rangle$ are primary, for example since $k[x, y] / \langle x^a \rangle \cong k[y] \oplus \dots \oplus k[y] x^{a-1}$ has no non-nilpotent zero-divisors.
  - $\langle x^2, xy^2 \rangle = \langle x \rangle \langle x, y^2 \rangle$ is not primary, since y gives a zero-divisor in $k[x, y] / \langle x^2, xy^2 \rangle$ which is not nilpotent. Find a primary decomposition. [7]
  - $\langle x^2, xy, y^2 \rangle = \langle x, y \rangle^2$, so it is primary but not irreducible, since $\langle x^2, xy, y^2 \rangle = \langle x^2, y \rangle \cap \langle x, y^2 \rangle$.

[7] Exercise

13 Artinian rings and modules

Lecture 20 Tuesday 19/11/19

Definition 13.1. Let A be a ring and let M be an A-module. Then M is called a **simple** A-module if the only proper submodule of M is zero. A **composition series** is a descending chain of submodules $M = M_0 \supsetneq \dots \supsetneq M_n = 0$ such that M_i/M_{i+1} is a simple A-module for $i = 0, \dots, n-1$.

Proposition 13.2. *The following are equivalent.*

- *M is both Noetherian and Artinian.*
- *M has a composition series.*

Proof.

$\Longrightarrow$ Look at all proper submodules of M. Since M is Noetherian, this set has a maximal element. Call it M_1. It is also Noetherian, so continue and build a descending chain. Since M_1 is maximal, M/M_1 is simple. All M_i/M_{i+1} are simple. Since M is Artinian, this chain is stationary, so $M_n = 0$ for some n.

$\Longleftarrow$ Corollary 11.6 says that if M_i/M_{i+1} is both Noetherian and Artinian, then so is M. A simple module is both Noetherian and Artinian.

□

Proposition 13.3. *If M has a composition series of length n, then any composition series of M has length n.*

Proof. Let us denote by $\mathrm{l}(M)$ the smallest length of a composition series of M.

Step 1. For a proper submodule $N \subsetneq M$ we have $\mathrm{l}(N) < \mathrm{l}(M)$. Indeed, let (M_i) be a composition series of length $\mathrm{l}(M)$. Define $N_i = N \cap M_i$, so

$$\begin{array}{ccccccc} M = M_0 & \supset & \dots & \supset & M_{n-1} & \supset & M_n = 0 \\ \cup & & & & \cup & & \wr\!\| \\ N = N_0 & \supset & \dots & \supset & N_{n-1} & \supset & N_n = 0 \end{array}.$$

Then $\ker(N_i \to M_i/M_{i+1}) = N_{i+1}$, so $N_i/N_{i+1} \subset M_i/M_{i+1}$, which is simple. After eliminating repetitions we get a composition series for N of length at most $\mathrm{l}(M)$. If the length is exactly $\mathrm{l}(M)$, then $N_{n-1} = M_{n-1}$, $N_{n-2} = M_{n-2}$, etc, and finally $N = M$.

Step 2. Any proper chain of submodules of M has length at most $\mathrm{l}(M)$. Passing to a proper submodule decreases $\mathrm{l}(M)$ at least by one. So the chain contains no more than $\mathrm{l}(M)$ terms.

Step 3. So consider any composition series of M. By step 2, it has length at most $\mathrm{l}(M)$. By minimality of $\mathrm{l}(M)$, it has length equal to $\mathrm{l}(M)$.

□

Define the **length** of a Noetherian and Artinian module M to be $\mathrm{l}(M)$, the length of any composition series of M.

Exercise. Any chain of submodules of M can be made into a composition series by inserting some submodules.

Proposition 13.4. *Let M be a Noetherian and Artinian module. If $N \subset M$ is a submodule, then*

$$\mathrm{l}(M) = \mathrm{l}(N) + \mathrm{l}(M/N).$$

Proof. Exercise. [8] □

[8] Exercise

Lecture 21 Wednesday 20/11/19

Example 13.5. Suppose R is a k-algebra, that is k is a field contained in R and R is a vector space over k. For example, $R = k$ or $R = k[x_1, \dots, x_n]/I$, where I is an ideal in $k[x_1, \dots, x_n]$.

- If $\dim_k R < \infty$, then R is an Artinian ring. Indeed, ideals of R are vector subspaces, so any chain of ideals has finite length. Hence R is both Artinian and Noetherian.
- If R is a finite set, then R is Artinian and Noetherian.
- If $R = k[[x]]$, then $\langle x \rangle \supsetneq \langle x^2 \rangle \supsetneq \dots$ is an infinite descending chain. So $k[[x]]$ is not Artinian. Similarly, $k[x]$ is not Artinian.

Remark. Hilbert's basis theorem says that if R is Noetherian, then so is $R[x]$. The analogue of this does not hold for Artinian rings.

Lemma 13.6. *An Artinian integral domain is a field.*

Proof. Take $x \neq 0$ in an Artinian ring A. Consider $\langle x \rangle \supset \langle x^2 \rangle \supset \dots$, which is stationary, so for some $n \geq 0$, $\langle x^n \rangle = \langle x^{n+1} \rangle$. Therefore, $x^n = ax^{n+1}$, so $x^n (ax - 1) = 0$. Since $x^n \neq 0$, $ax = 1$, so x is invertible, that is $x \in A^*$. $\square$

Corollary 13.7. *In an Artinian ring every prime ideal is maximal.*

Corollary 13.8. *In an Artinian ring the nilradical is the same as the Jacobson radical.*

Lemma 13.9. *An Artinian ring has only finitely many maximal ideals.*

Proof. Assume this is false, so $\mathfrak{m}_1, \mathfrak{m}_2, \dots$ are pairwise different maximal ideals. Then $\mathfrak{m}_1 \supset \mathfrak{m}_1 \cap \mathfrak{m}_2 \supset \dots$ is stationary, so for some $n \geq 1$ we have $\mathfrak{m}_1 \cap \dots \cap \mathfrak{m}_n = (\mathfrak{m}_1 \cap \dots \cap \mathfrak{m}_n) \cap \mathfrak{m}_{n+1}$, so $\mathfrak{m}_1 \cap \dots \cap \mathfrak{m}_n \subset \mathfrak{m}_{n+1}$. By the prime avoidance lemma, $\mathfrak{m}_{n+1}$ contains some $\mathfrak{m}_i$, where $i \in \{1, \dots, n\}$. These are maximal ideals, hence $\mathfrak{m}_i = \mathfrak{m}_{n+1}$. This is a contradiction. $\square$

An ideal $I \subset R$ is called **nilpotent** if $I^n = 0$ for some $n \geq 1$.

Lemma 13.10. *If A is an Artinian or Noetherian ring, then the nilradical $\mathcal{N}(A)$ is a nilpotent ideal, that is $\mathcal{N}(A)^m = 0$ for some m.*

Proof.

- Assume A is Artinian. Consider $\mathcal{N}(A) \supset \mathcal{N}(A)^2 \supset \dots$. There exists $n \geq 1$ such that $\mathcal{N}(A)^n = \mathcal{N}(A)^{n+1}$. Claim that $\mathcal{N}(A)^n = 0$. Assume $\mathcal{N}(A)^n \neq 0$. Consider all ideals
$$\{I \subset A \mid I \cdot \mathcal{N}(A)^n \neq 0\}.$$
This set is non-empty. It contains $\mathcal{N}(A)$, since $\mathcal{N}(A)^{n+1} = \mathcal{N}(A)^n \neq 0$. Then A is Artinian, so this set has a minimal element. Call it I. So we have $I \cdot \mathcal{N}(A)^n \neq 0$ hence $x\mathcal{N}(A)^n \neq 0$ for some $x \in I$. We have $\langle x \rangle \mathcal{N}(A)^n \neq 0$ where $\langle x \rangle \subset I$. Then $\langle x \rangle$ belongs to our set, so by minimality of I we must have $I = \langle x \rangle$. We have $0 \neq x\mathcal{N}(A)^n = x\mathcal{N}(A)^n \mathcal{N}(A)^n$, since $\mathcal{N}(A)^n = \mathcal{N}(A)^m$, for any $m \geq n$. So $x\mathcal{N}(A)^n$ is an ideal in our set. Then $x \in I$ so $x\mathcal{N}(A)^n \subset I$. By minimality of I we must have $x\mathcal{N}(A)^n = I$. Therefore $\langle x \rangle \mathcal{N}(A)^n = I = \langle x \rangle$, so x can be written as xy for some $y \in \mathcal{N}(A)^n \subset \mathcal{N}(A)$. Thus $y^r = 0$ for some $r \geq 1$. Then $x = \dots = xy^r = 0$. This says that $I = \langle x \rangle = 0$. This is a contradiction because $I \cdot \mathcal{N}(A)^n \neq 0$. Therefore, $\mathcal{N}(A)^n = 0$.
- Now assume A is Noetherian. Then every ideal is finitely generated, in particular $\mathcal{N}(A) = \langle x_1, \dots, x_n \rangle$. Since each x_i is nilpotent there exists $m \geq 1$ such that $x_i^m = 0$ for all i. Then any product of mn elements of $\mathcal{N}(A)$ is $\sum_{a_1 + \dots + a_n = mn} c x_1^{a_1} \dots x_n^{a_n}$. So there exists i, for $1 \leq i \leq n$, such that $a_i \geq m$. Hence $x_1^{a_1} \dots x_n^{a_n} = 0$, so $\mathcal{N}(A)^{mn} = 0$.

$\square$

Lecture 22 Thursday 21/11/19

Corollary 13.11. *Every ideal in a Noetherian or Artinian ring contains some power of its radical.*

Proof. If A is Noetherian, then A/I is also Noetherian. We have $\operatorname{rad} I/I = \mathcal{N}(A/I)$. By Lemma 13.10 there exists $m \geq 1$ such that $\mathcal{N}(A/I)^m = 0$. Then $\operatorname{rad} I^m \subset I$. The same proof works in the Artinian case. $\square$

Lemma 13.12. *Let V be a vector space over a field k. The following are equivalent.*

- $\dim_k V < \infty$.
- *V is a Noetherian k-module.*
- *V is an Artinian k-module.*

Proof. Obvious. □

Lemma 13.13. *Let A be a ring. Let $I_1, \dots, I_n$ be maximal ideals of A, possibly with repetitions. Suppose $I_1 \dots I_n = 0$. Then A is Noetherian if and only if A is Artinian.*

Proof.

$\implies$ Define $M_r = I_1 \dots I_r$ for $r = 1, \dots, n$, so

$$A \supset M_1 = I_1 \supset \dots \supset M_n = \prod_{r=1}^n I_r = 0.$$

Since A is a Noetherian A-module, every subquotient module is also Noetherian. In particular, M_i/M_{i+1} is a Noetherian A-module. Since $I_{r+1}M_r = M_{r+1}$, I_{r+1} acts trivially on M_r/M_{r+1}. Therefore, M_r/M_{r+1} is naturally an A/I_{r+1}-module. But A/I_{r+1} is a field. Call it k. The A-submodules of M_r/M_{r+1} are the same as the k-submodules of M_r/M_{r+1}. By Lemma 13.12 M_r/M_{r+1} is an Artinian k-module hence M_r/M_{r+1} is an Artinian A-module. Now Proposition 11.4 implies that A is Artinian.

$\impliedby$ Similar.

□

Definition 13.14. The **Krull dimension** of a ring A is the supremum of all $n \geq 0$ such that A has an ascending chain of prime ideals $\mathfrak{p}_0 \subsetneq \dots \subsetneq \mathfrak{p}_n$. If the supremum does not exist, the dimension is infinite. It is denoted $\dim A$.

Example.

- Any field has dimension zero.
- If A is Artinian, then every prime ideal is maximal, hence $\dim A = 0$.
- $\dim \mathbb{Z} = 1$, since $0 \subsetneq \langle p \rangle$ for p a prime number.
- If k is a field, then $\dim k[t] = 1$.
- If k is a field, then $\dim k[[t]] = 1$.
- If k is a field, then $\dim k[t_1, \dots, t_n] = n$.

Theorem 13.15. *A ring is Artinian if and only if it is Noetherian and has dimension zero.*

Proof.

$\implies$ Suppose A is Artinian. Corollary 13.7 says that every prime ideal is maximal, hence $\dim A = 0$. Lemma 13.9 says that A has only finitely many maximal ideals, say $I_1, \dots, I_n$. Then $I_1 \dots I_n \subset I_1 \cap \dots \cap I_n = \mathcal{N}(A)$. Lemma 13.10 says $\mathcal{N}(A)^m = 0$ for some $m \geq 1$. Hence $I_1^m \dots I_n^m = 0$. Lemma 13.13 now implies that A is Noetherian.

$\impliedby$ Now assume that A is Noetherian and $\dim A = 0$. By Emmy Noether's theorem the ideal zero has a primary decomposition, that is $0 = J_1 \cap \dots \cap J_n$, where J_i's are primary. Recall $\operatorname{rad} J_i$ is a prime ideal of A. Since $\dim A = 0$, this ideal is maximal. The associated primes of zero are maximal ideals. By Corollary 13.11 each J_i contains a power of $\operatorname{rad} J_i$. Therefore, the product of these powers of these maximal ideals is contained in $\prod_{i=1}^n J_i \subset \bigcap_{i=1}^n J_i = 0$. Now Lemma 13.13 implies that A is Artinian.

□

Theorem 13.16. *Every Artinian ring is a finite direct product of local Artinian rings.*

Definition 13.17. Two ideals $I, J \subset R$ are **coprime** if $I + J = R$.

Example. Two distinct maximal ideals are coprime.

Suppose $I_1, \ldots, I_n$ are ideals of R. Define

$$\begin{array}{cccc} \phi & : & R & \longrightarrow & \prod_{j=1}^n R/I_j \\ & & x & \longmapsto & (x + I_1, \ldots, x + I_n) \end{array}.$$

Lemma 13.18 (Chinese remainder theorem)**.**

- *If I_r and I_s are coprime whenever $r \neq s$, then*
$$\prod_{j=1}^n I_j = \bigcap_{j=1}^n I_j.$$
- *ϕ is surjective if and only if I_r and I_s are coprime for $r \neq s$.*
- *ϕ is injective if and only if $\bigcap_{j=1}^n I_j = 0$.*

Proof. See problem sheet 4 question 2. □

Lecture 23 is a class test. Lecture 23 Tuesday 26/11/19

Proof of Theorem 13.16. Let R be an Artinian ring. Then R has only finitely many maximal ideals, say $J_1, \ldots, J_n$. In the proof of Theorem 13.15 we have seen that for some $k \geq 1$, $\prod_{i=1}^n J_i^k = 0$. Since the J_i's are maximal ideals, we have $J_r + J_s = R$, whenever $r \neq s$. This implies $J_r^k + J_s^k = R$. Indeed, we can write $1 = x + y$ for $x \in J_r$ and $y \in J_s$, so Lecture 24 Wednesday 27/11/19

$$1 = 1^{2k} = \sum_{i=0}^{2k} \binom{2k}{i} x^i y^{2k-i}.$$

Hence $i \geq k$ or $2k - i \geq k$, so $x^i \in J_r^k$ or $y^{2k-i} \in J_s^k$, so $x^i y^{2k-i} \in J_r^k$ or $x^i y^{2k-i} \in J_s^k$. Hence $1 \in J_r^k + J_s^k$. Let

$$\phi : R \to \prod_{i=1}^n R/J_i^k.$$

Then ϕ is surjective since $R = J_r^k + J_s^k$ for $r \neq s$, by Lemma 13.18, and ϕ is injective since $\bigcap_{i=1}^n J_i^k = \prod_{i=1}^n J_i^k = 0$, by Lemma 13.18.1 and we have chosen k so this holds. Therefore ϕ is an isomorphism of rings. It remains to show that each R/J_i^k is a local Artinian ring. Since R is Artinian, R/J_i^k is Artinian, so $J_i/J_i^k \subset R/J_i^k$ is a maximal ideal of R/J_i^k. The nilradical of R/J_i^k is J_i/J_i^k. Indeed, every element is J_i/J_i^k is nilpotent, since $\left(J_i/J_i^k\right)^k = 0$ in R/J_i^k. But the nilradical cannot be larger than J_i/J_i^k because this ideal is maximal. Thus $\mathcal{N}\left(R/J_i^k\right) = J_i/J_i^k$. This is the intersection of all prime ideals of R/J_i^k, so each prime ideal of R/J_i^k is equal to J_i/J_i^k. So R/J_i^k is indeed a local ring. □

Example. Let $R = k\left[x_1, \ldots, x_n\right]/I$, where I is an ideal. Any finitely generated k-algebra is like this. Then $k\left[x_1, \ldots, x_n\right]$ is Noetherian, so

$$I = \langle f_1, \ldots, f_m \rangle, \qquad f_i\left(x_1, \ldots, x_n\right) \in k\left[x_1, \ldots, x_n\right], \qquad i = 1, \ldots, m.$$

We know that R is Artinian if the dimension of the k-vector space $\dim_k R < \infty$. Then $R = \prod_{i=1}^n R/J_i^k$, for some k, where J_i's are all maximal ideals. Assume k is algebraically closed, such as $k = \mathbb{C}$. Then the maximal ideals are precisely

$$\langle x_1 - a_1, \ldots, x_n - a_n \rangle, \qquad a = \left(a_1, \ldots, a_n\right) \in k^n, \qquad f_1(a) = \cdots = f_m(a) = 0.$$

14 Integral closure and normal rings

Let R be a ring and let $A \subset R$ be a subring. In other words, R is an A-algebra.

Theorem 14.1. *Let $x \in R$. The following are equivalent.*

1. *There are $a_0, \dots, a_{n-1} \in A$ such that $x^n + a_{n-1}x^{n-1} + \dots + a_0 = 0$.*
2. *The A-module $A[x]$ is finitely generated. We have that $A[x] \subset R$, and x is not an independent variable.*
3. *There is a subring B in R such that $A \subset B$, $x \in B$, and B is finitely generated as an A-module.*

Proof.

$1 \implies 2$. $x^{n+j} = -a_{n-1}x^{n+j-1} - \dots - a_0 x^j$. By repeating this we express all powers of x as linear combinations of $1, \dots, x^{n-1}$ with coefficients in A. Hence $A[x]$ is generated by $1, \dots, x^{n-1}$.

$2 \implies 3$. Take $B = A[x]$.

$3 \implies 1$. B is finitely generated as an A-module, so suppose $y_1, \dots, y_n$ are generators of B. Then $x, y_i \in B$ and B is a subring, hence $xy_i \in B$ for $i = 1, \dots, n$. Hence $xy_i = \sum_{j=1}^n a_{ij} y_j$ for $a_{ij} \in A$. Let $\mathcal{A} = (a_{ij})_{1 \le i,j \le n}$. Consider $d = \det(x\mathrm{I}_n - \mathcal{A}) \in B$, where I_n is the identity matrix. By Theorem 8.5, the determinant trick, we have $dy_i = 0$ for $i = 1, \dots, n$. Hence $dy = 0$ for any $y \in B$. But $1 \in B$, so taking $y = 1$ we get $d = 0$, in B. Now let $f(t) = \det(t\mathrm{I}_n - \mathcal{A}) \in A[t]$ be a characteristic polynomial of $\mathcal{A}$. We obtain $f(x) = 0$, and $f(t)$ is monic in $A[t]$.

□

Lecture 25 Thursday 28/11/19

Definition 14.2. An element $x \in R$ is **integral** over A if $x^n + a_{n-1}x^{n-1} + \dots + a_0 = 0$, for some $a_{n-1}, \dots, a_0 \in A$. Equivalently, $A[x]$ is a finitely generated A-module. Such a polynomial is called an **integral dependence relation**. Then R is called an **integral A-algebra** if every element of R is integral over A.

Example.

- Suppose $k \subset K$ is an extension of fields. Thus K is a k-algebra. Then K is integral over k if and only if K is algebraic over k. For example, if $[K : k] = \dim_k K < \infty$, then K is integral over k.
- Let $R = k[x]$ and $A = k[x^2] \subset R$. Then R is integral over A. For example, $x \in R$ satisfies the equation $t^2 - x^2 = 0$, so x is integral over A. Show that any element of R is integral over A. [9]
- Let $R = \mathbb{Z}\left[\frac{1+\sqrt{-3}}{2}\right]$. Then $\zeta_3 = \frac{1+\sqrt{-3}}{2}$ satisfies $t^2 + t + 1 = 0$, so R is in integral over $\mathbb{Z}$. Theorem 14.1.3 says that $r \in R$ is integral as long as R contains a subring B such that $A \subset B$, $r \in B$, and B is a finitely generated A-module.
- $\mathbb{Z}\left[\frac{1}{2}\right] = \{n/2^m \mid n \in \mathbb{Z},\ m \ge 0\}$ is not an integral $\mathbb{Z}$-algebra, since $\frac{1}{2}$ is not integral over $\mathbb{Z}$.

Lemma 14.3.

1. *If $A \subset B \subset C$ are rings and C is a finitely generated B-module, and B is a finitely generated A-module, then C is a finitely generated A-module.*
2. *If $A \subset B$ are rings and $x_1, \dots, x_n \in B$ are integral over A, then $A[x_1, \dots, x_n]$ is a finitely generated A-module. Hence $A[x_1, \dots, x_n]$ is an integral A-algebra.*
3. *If $A \subset B \subset C$ are rings such that C is integral over B and B is integral over A, then C is integral over A.*
4. *If $A \subset B$ are rings, then the set of all elements in B that are integral over A is a subring of B. Denote it by $\widetilde{A}$ and call it the **integral closure** of A in B. Then $\widetilde{\widetilde{A}} = \widetilde{A}$, that is the integral closure of $\widetilde{A}$ is equal to $\widetilde{A}$.*

[9] Exercise

Proof.

1. If $c_1, \dots, c_n$ generate C as a B-module and $b_1, \dots, b_m$ generate B as an A-module, then $c_i b_j$ generate C as an A-module.

2. $A[x_1]$ is a finitely generated A-module. Next, x_2 is integral over A, hence also over $A[x_1]$. Thus $A[x_1, x_2]$ is a finitely generated $A[x_1]$-module. Using 1 we see that $A[x_1, x_2]$ is also a finitely generated A-module. Repeat and show that $A[x_1, \dots, x_n]$ is a finitely generated A-module. By Theorem 14.1.3 every element of $A[x_1, \dots, x_n]$ is integral over A, so $A[x_1, \dots, x_n]$ is an integral A-algebra.

3. Pick up any $x \in C$. Then $x^n + b_{n-1}x^{n-1} + \dots + b_0 = 0$ for $b_i \in B$. Since $b_0, \dots, b_{n-1}$ are integral over A, by 2 we get that $A[b_0, \dots, b_{n-1}]$ is a finitely generated A-module. Then $A[b_0, \dots, b_{n-1}, x]$ is also finitely generated as a module over $A[b_0, \dots, b_{n-1}]$. By 1, $A[b_0, \dots, b_{n-1}, x]$ is a finitely generated as an A-module. Now Theorem 14.1.3 says that x is integral over A.

4. Let $x, y \in B$ be integral over A. Want to prove that $-x, x+y, xy$ are integral over A. Look at $A[x, y]$. By 2 this is an integral A-algebra. Hence everything contained in $A[x, y]$, such as xy and $x+y$, are integral over A. Hence $\widetilde{A}$ is a ring. Consider $A \subset \widetilde{A} \subset \widetilde{\widetilde{A}}$, which are both integral. Now 3 says that $\widetilde{\widetilde{A}}$ is integral over A. Thus $\widetilde{\widetilde{A}} = \widetilde{A}$.

$\square$

Example. If $x = \sqrt{a}$, $y = \sqrt{b}$, and $z = \sqrt{c}$ for $a, b, c \in \mathbb{Q}$, then $\sqrt{a} + \sqrt{b} + \sqrt{c}$ is algebraic over $\mathbb{Q}$. This follows immediately from Lemma 14.3.4.

Definition 14.4. The set of elements of B which are integral over A is called the **integral closure** of A in B. Then A is called **integrally closed** in B if A equals its integral closure in B. Now let R be an integral domain. Let F be the fraction field of R, so $R \subset F$. Then R is called **normal** if R equals its integral closure in F. The integral closure of R in F is called the **normalisation**.

Lecture 26 Tuesday 03/12/19

Example. Integral closure in number theory. The integral closure of $\mathbb{Q}$ in $\mathbb{C}$ is $\overline{\mathbb{Q}}$, the algebraic numbers in $\mathbb{C}$, which is algebraically closed. Let $\mathbb{Q} \subset F$ be a finite extension of fields. Then F is called a **number field**. Let $\mathcal{O}_F$ be the integral closure of $\mathbb{Z}$ in F.

- Let $F = \mathbb{Q}(\zeta)$, where ζ is a primitive d-th root of unity. Then $\mathcal{O}_F = \mathbb{Z}[\zeta]$.
- Let $F = \mathbb{Q}(\sqrt{a})$ for $0, 1 \neq a \in \mathbb{Z}$ square-free. Then

$$\mathcal{O}_F = \begin{cases} \mathbb{Z}[\sqrt{a}] & d \equiv 2, 3 \mod 4 \\ \mathbb{Z}\left[\frac{1+\sqrt{a}}{2}\right] & d \equiv 1 \mod 4 \end{cases},$$

  so $\mathbb{Z}[\sqrt{a}] \subsetneq \mathbb{Z}\left[\frac{1+\sqrt{a}}{2}\right]$ is not normal if $d \equiv 1 \mod 4$.

Example. Integral closure in algebraic geometry. Let C be a plane curve. Non-singular curves give rise to normal rings. Let $f(x, y)$ be the equation of C. Look at $k[x, y] / \langle f(x, y) \rangle$.

- Let $R = k[x, y] / \langle x^3 - y^2 \rangle$, and let $t = y/x \in K$, the field of fractions of R. We have $t^2 = y^2/x^2 = x$ in R. So $t \notin R$ and yet t is integral over R. Note that $k[t]$ is a UFD. Any UFD is normal. [10] We have $R \subset k[t] \subset K$. Therefore, $k[t]$ is the integral closure of R.

Proposition 14.5. *An integral domain A is normal if and only if $A_{\mathfrak{p}} = (A \setminus \mathfrak{p})^{-1} A$ is normal for each prime ideal $\mathfrak{p} \subset A$, if and only if $A_{\mathfrak{m}}$ is normal for each maximal ideal $\mathfrak{m} \subset A$.*

Proof. Let $S \subset A$ be any multiplicative set. Claim that $S^{-1}A$ is normal. Since A is an integral domain, $A \subset S^{-1}A \subset K$, the field of fractions of A. Pick any $x \in K$ which is integral over $S^{-1}A$, that is $x^n + a_{n-1}x^{n-1} + \dots + a_0 = 0$, where $a_i \in S^{-1}A$, that is $a_i = b_i/s_i$, where $b_i \in A$ and $s_i \in S$. Define $y = (s_0 \dots s_{n-1})\, x$. Then y is integral over A, so $y \in A$. Hence $x \in S^{-1}A$. It remains to prove that if $A_{\mathfrak{m}}$ is normal for every $\mathfrak{m}$, then A is normal. Take any $x \in K$ which is integral over A. Since $A \subset A_{\mathfrak{m}} \subset K$, x is integral over $A_{\mathfrak{m}}$, hence $x \in A_{\mathfrak{m}}$. Thus $x \in \bigcap_{\mathfrak{m}} A_{\mathfrak{m}} = A$, by Corollary 10.6. $\square$

[10] Exercise

15 Discrete valuation rings

Example. $k[[x]]$ and $\mathbb{Z}_{\langle p \rangle}$.

Theorem 15.1. *Let R be an integral domain. The following are equivalent.*

- *R is a UFD with only one irreducible element, up to multiplication by units.*
- *R is a Noetherian local ring such that the unique maximal ideal is principal.*

Proof.

$\implies$ Choose an irreducible element. Call it t. Then $R = \{0\} \cup \langle t \rangle \cup R^*$. Hence $\langle t \rangle$ is a maximal ideal. Claim that all proper non-zero ideals of R are $\langle t^n \rangle$ for $n \geq 1$. Indeed, let $I \subset R$ be a non-zero ideal. Take $rt^n \in I$ for $r \in R^*$ with minimal n. Hence $\langle rt^n \rangle = \langle t^n \rangle \subset I$. Then $I = \langle t^n \rangle$. Hence $\langle t \rangle$ is the unique maximal ideal of R. Thus R is a local ring. All ideals are finitely generated, hence R is Noetherian. Lecture 27 Wednesday 04/12/19

$\impliedby$ Let $t \in R$ be a generator of the unique maximal ideal. Then $R \setminus \langle t \rangle = R^*$. Claim that for every non-zero $a \in R$, there exists a largest $n \geq 0$ such that $a \in \langle t^n \rangle$. If $a \notin \langle t \rangle$, then $a \in R^*$, so $n = 0$. If $a \in \langle t \rangle$, then $a = a_1 t$ for some $a_1 \in R$. Two possibilities can occur. If $a_1 \in R^*$, then $a \notin \langle t^2 \rangle$. If $a_1 \notin R^*$, then $\langle a_1 \rangle$ is a proper ideal of R. We have $\langle a \rangle = \langle a_1 t \rangle \subsetneq \langle a_1 \rangle \subsetneq R$. The inclusion $\langle a \rangle \subsetneq \langle a_1 \rangle$ is strict, because if $\langle a \rangle = \langle a_1 \rangle$, then for some $u \in R^*$ we must have $uta_1 = a_1$, so $t \in R^*$, a contradiction. We continue, since a_1 is not a unit, $a_1 \in \langle t \rangle$ and we write $a_1 = a_2 t$ and we analyse a_2 as we analysed a_1. Either, after finitely many steps, we get $a_n \in R^*$, so that $a = a_n t^n$ and we are done, or we build an ascending chain of ideals $\langle a \rangle \subsetneq \langle a_1 \rangle \subsetneq \langle a_2 \rangle \subsetneq \dots$ that is not stationary. The second possibility cannot occur in a Noetherian ring.

□

Remark. $R = \{0\} \cup \{at^n \mid a \in R^*, \ n \geq 0\}$. Define

$$\begin{array}{cccc} v & : & R \setminus \{0\} & \longrightarrow & \mathbb{Z}_{\geq 0} \\ & & at^n & \longmapsto & n \end{array}.$$

Then $v(at^n \cdot bt^m) = n + m = v(at^n) + v(bt^m)$, and v obviously extends to a surjective homomorphism $K^* \to \mathbb{Z}$, where K is the field of fractions of R. Note that

$$v(at^n + bt^m) \geq \min\{v(at^n), v(bt^m)\}, \qquad a, b \in R^*,$$

since say $n \leq m$, then $at^n + bt^m = t^n(a + bt^{m-n})$, and $a + bt^{m-n} \in R$.

Recall that a **total order** on a set is a binary relation, written as $x < y$, such that for any a and b exactly one of

$$a < b, \qquad a = b, \qquad a > b$$

holds. An **ordered abelian group** is an abelian group G with a total order $<$ compatible with the group structure, so $a < b$ implies that $a + c < b + c$ for all $c \in G$.

Example. $\mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R}$, with the usual order.

Exercise. Any ordered group is torsion-free, so no non-zero elements of finite order.

Definition 15.2. Let K be a field. A **valuation** is a surjective homomorphism $v : K^* \to G$, where G is an ordered group such that

$$v(x \pm y) \geq \min\{v(x), v(y)\}.$$

Exercise. Suppose given $(K, v : K^* \to G)$. Then

$$R = \{x \in K \mid v(x) \geq 0\}$$

is a ring. It is called the **valuation ring** of v. Prove that

$$R^* = \{x \in K \mid v(x) = 0\}.$$

Hence

$$R \setminus R^* = \{x \in K \mid v(x) > 0\}$$

is a unique maximal ideal of R, so R is a local ring.

Exercise. Suppose R is a subring of a field K. When is R a valuation ring? This is so if and only if for any $x \in K^*$ we have $x \in R$ or $x^{-1} \in R$. A hint is $G = K^*/R^*$ so you just need to define a total order on G.

Example.

- $\mathbb{Z}_{\langle p \rangle} = \{a/b \mid p \nmid b,\ b \neq 0,\ a, b \in \mathbb{Z}\}$ is a valuation ring with $G = \mathbb{Z}$.
- Likewise, $k[[x]]$ is a valuation ring with $G = \mathbb{Z}$.
- The field of fractions of $k[[x]] = \left\{\sum_{i \geq 0} a_i x^i \;\middle|\; a_i \in k\right\}$ is the **field of Laurent formal power series**

  $$k((x)) = \left\{\sum_{i \geq m} a_i x^i \;\middle|\; a_i \in k,\ m \in \mathbb{Z}\right\}.$$

  Consider the **field of Puiseux series**

  $$K = \bigcup_{n \geq 1} k\left(\left(x^{\frac{1}{n}}\right)\right) = \left\{\sum_{i \geq m} a_i t^{\frac{i}{N}} \;\middle|\; a_i \in k,\ m \in \mathbb{Z},\ N \text{ fixed}\right\}.$$

  Define v to be the smallest power of t such that the coefficient is non-zero. Then $v : K^* \to \mathbb{Q}$ is a valuation. The valuation ring is

  $$R = \bigcup_{n \geq 1} k\left[\left[t^{\frac{1}{n}}\right]\right].$$

  Then R is not Noetherian. Indeed, $\left\langle t^{1/2^n} \right\rangle$ is an infinite ascending chain of ideals.

Lecture 28
Thursday
05/12/19

Definition 15.3. A **discrete valuation ring (DVR)** is a valuation ring of a discrete valuation, so $G = \mathbb{Z}$.

Theorem 15.4. *Let K be a field. Let $v : K^* \to G$ be a valuation, where G is an ordered group. The valuation ring of K attached to v is Noetherian if and only if $G = \mathbb{Z}$. In other words, a valuation ring is Noetherian if and only if it is a DVR.*

Proof. Let R be the valuation ring attached to (K, v), that is $R = \{x \in K \mid v(x) \geq 0\}$.

$\implies$ Assume R is Noetherian. Let us show that every ideal is principal. Since R is Noetherian, every ideal $I = \langle a_1, \dots, a_n \rangle$ for $a_i \in R$. It is enough to prove that for all $0 \neq x, y \in R$, $\langle x, y \rangle = \langle x \rangle$ or $\langle x, y \rangle = \langle y \rangle$. Since G is totally ordered, one of

$$v(x) < v(y), \qquad v(x) = v(y), \qquad v(x) > v(y)$$

holds. Thus $v(x) \geq v(y)$ or $v(y) \geq v(x)$. Without loss of generality assume $v(y) \geq v(x)$. Then $v(y/x) = v(y) - v(x) \geq 0$, hence $y/x \in R$. Hence $y \in \langle x \rangle$. In particular, as R is a local ring, the maximal ideal is $\langle t \rangle$, for some $t \in R$. Theorem 15.1 implies that R is a UFD and t is a unique irreducible element of R. Then

$$R = \{0\} \cup \{rt^n \mid n \geq 0,\ r \in R^*\}, \qquad K = \{0\} \cup \{rt^n \mid n \in \mathbb{Z},\ r \in R^*\},$$

so R is a valuation ring attached to the valuation that sends rt^n to n.

$\impliedby$ Conversely, assume that $v : K^* \to \mathbb{Z}$. Choose $t \in R$ with $v(t) = 1$. For all $x \in K^*$, if $v(x) \geq 1$ then $x/t \in R$, so $x \in \langle t \rangle$. Then $R^* = \{x \in K \mid v(x) = 0\} = R \setminus \langle t \rangle$. Thus $\langle t \rangle$ is a maximal ideal. Claim that all proper non-zero ideals of R are $\langle t^n \rangle$ for $n \geq 1$. Indeed, let $I \subset R$ be a non-zero proper ideal. Choose $x \in I$ with the least possible $v(x)$. Say, $v(x) = n$. Then $v(t^n) = n$. Then $v(x/t^n) = 0$, so $x/t^n \in R^*$, hence $t^n \in I$. For any $0 \neq y \in I$, $v(y/t^n) = v(y) - n \geq 0$, hence $y \in \langle t^n \rangle$, so $I = \langle t^n \rangle$. Therefore, any ascending chain of ideals $\langle t^n \rangle$ must be stationary, since $\langle t^n \rangle \subsetneq \langle t^m \rangle$ implies that $m < n$. Hence R is Noetherian.

∎

Theorem 15.5 (Main theorem about DVRs)**.** *Let R be an integral domain. The following are equivalent.*

1. *R is a DVR.*
2. *R is a UFD with only one irreducible element, up to a unit.*
3. *R is a Noetherian local ring with principal maximal ideal.*
4. *R is a Noetherian normal local ring of Krull dimension one.*

Proof.

$1 \implies 3$. The second part of the proof of Theorem 15.4.

$3 \implies 2$. Theorem 15.1.

$2 \implies 1$. Easy, since $v(rt^n) = n$.

$1 \implies 4$. Any UFD is Noetherian and normal. All non-zero ideals in a DVR are $\langle t^n \rangle$. Hence zero and $\langle t \rangle$ are the only prime ideals. Since $0 \subsetneq \langle t \rangle$, the Krull dimension is one.

$4 \implies 3$. We must prove that the maximal ideal is principal.

Step 1. Let $I \subset R$ be the maximal ideal. Recall that Nakayama's lemma for a Noetherian ring R implies that if $I^2 = I$, then $I = 0$, by Theorem 9.9. If $I = 0$, then R is a field. But the Krull dimension of a field is zero, so R is not a field. Thus $I \ne 0$. Hence $I^2 \subsetneq I$. Choose $t \in I$ such that $t \notin I^2$. We will prove that $I = \langle t \rangle$.

Step 2. Suppose that $I \ne \langle t \rangle$, so I contains an element y which is not in $\langle t \rangle$. Consider $(\langle t \rangle : \langle y \rangle) = \{r \in R \mid ry \in \langle t \rangle\}$. If $y \notin \langle t \rangle$, then $(\langle t \rangle : \langle y \rangle) \ne R$. Note that $t \in (\langle t \rangle : \langle y \rangle)$, so $(\langle t \rangle : \langle y \rangle) \ne 0$. Since R is Noetherian, this set of ideals contains a maximal element, say $(\langle t \rangle : \langle y \rangle)$ for some y.

Step 3. Claim that $(\langle t \rangle : \langle y \rangle)$ is a non-zero prime ideal. Since the Krull dimension of R is one, it must be the maximal ideal I. Take any $a, b \in R$ such that $ab \in (\langle t \rangle : \langle y \rangle)$, that is $aby \in \langle t \rangle$. Assume that $b \notin (\langle t \rangle : \langle y \rangle)$, that is $by \notin \langle t \rangle$. We have $(\langle t \rangle : \langle y \rangle) \subset (\langle t \rangle : \langle by \rangle)$, but our ideal $(\langle t \rangle : \langle y \rangle)$ is maximal in our set, hence $(\langle t \rangle : \langle y \rangle) = (\langle t \rangle : \langle by \rangle)$. Since $aby \in \langle t \rangle$, $ay \in \langle t \rangle$. This shows that $a \in (\langle t \rangle : \langle y \rangle)$. So $(\langle t \rangle : \langle y \rangle)$ is a prime ideal. The claim is proved. Thus we have $yI \subset \langle t \rangle$.

Lecture 29 Tuesday 10/12/19

Step 4. Let K be the fraction field of R. Then $y/t \in K$, but $y/t \notin R$. However, $(y/t) I \subset R$. We conclude that $(y/t) I$ is an ideal of R. This is a proper ideal, that is $(y/t) I \ne R$, otherwise $t = yx$, for some $x \in I$. But then $t \in I^2$, which is false. Hence $(y/t) I \ne R$. Since R is a local ring, I is the only maximal ideal, thus $(y/t) I \subset I$.

Step 5. Since R is Noetherian, I is a finitely generated ideal, say $I = \langle x_1, \dots, x_n \rangle$. Then $(y/t) x_i$ is a linear combination of the x_i's with coefficients in R. The determinant trick then gives a polynomial $p(x)$ such that $p(y/t) x_i = 0$ for $i = 1, \dots, n$. Since R is an integral domain, we conclude that $p(y/t) = 0$. Recall $p(x)$ is monic, and $p(x) \in R[x]$. Since R is normal, $y/t \in R$, so that $y \in \langle t \rangle$. This contradiction finishes the proof.

□

Corollary 15.6. *Let A be a Noetherian normal integral domain. For each prime ideal $\mathfrak{p} \subset A$ which is minimal among non-zero prime ideals of A, the localisation $A_{\mathfrak{p}}$ is a DVR.*

Proof. Lemma 11.7 implies that $A_{\mathfrak{p}}$ is Noetherian. Proposition 14.5 implies that $A_{\mathfrak{p}}$ is normal. Theorem 6.9 says that

$$\{0, \mathfrak{p}A_{\mathfrak{p}}\} = \{ \text{ prime ideals of } A_{\mathfrak{p}} \} \qquad \leftrightsquigarrow \qquad \{ \text{ prime ideals of } A \text{ contained in } \mathfrak{p} \} = \{0, \mathfrak{p}\}.$$

Hence $\dim A_{\mathfrak{p}} = 1$. Theorem 15.5 then implies that $A_{\mathfrak{p}}$ is a DVR. □

Remark.

$$A = \bigcap_{\text{minimal non-zero prime ideals } \mathfrak{p} \subset A} A_{\mathfrak{p}} \subset K.$$

16 Completion

Let R be a ring and $I \subset R$ be an ideal.

Definition 16.1. Turn R into a topological space with the **I-adic topology** by declaring I^m as open neighbourhoods of zero. In other words, $a_n \to 0$ if for any $m \geq 1$ there exists an $N \geq 1$ such that $a_n \in I^m$ for all $n \geq N$.

For any $x \in R$ the cosets $x + I^m$ are a system of open neighbourhoods of x. Since the complement to a given coset is the union of all the other cosets, it is open, hence the original coset is both open and closed. So every $x + I^m$ is open and closed. Then if we put the discrete topology on R/I^m, then the natural map $R \to R/I^m$ is continuous. Then it is easy to check that addition and subtraction $R \times R \to R$ are continuous, and multiplication $R \to R$ is also continuous. This says that R is a **topological ring**.

Example 16.2. Let $R = \mathbb{Z}$ and $I = \langle p \rangle$. Then $R_I = \mathbb{Z}_{\langle p \rangle} \supset \langle p \rangle$ has completion $\mathbb{Z}_p$, the **ring of p-adic integers**.

Let us construct the completion of R in the I-adic topology, which we just defined. Look at the product ring

$$\prod_{m \geq 1} R/I^m = \{(x_m) \mid x_m \in R/I^m\}.$$

We have surjective maps

$$\begin{array}{cccccc} s_n & : & R/I^{n+1} & \longrightarrow & R/I^n & , \qquad n \geq 1, \\ & & x + I^{n+1} & \longmapsto & x + I^n & \end{array}$$

so

$$\dots \xrightarrow{s_{n+1}} R/I^{n+1} \xrightarrow{s_n} R/I^n \xrightarrow{s_{n-1}} \dots.$$

Definition 16.3. Define

$$\widehat{R} = \varprojlim_m R/I^m,$$

the **I-adic completion** of R, as the subset of $\prod_{m \geq 1} R/I^m$ given by $s_n(x_{n+1}) = x_n$, for all $n \geq 1$.

$\widehat{R}$ is closed under coordinate-wise addition and multiplication. So $\widehat{R}$ is a ring.

Lecture 30 Wednesday 11/12/19

Definition 16.4. Let X_i for $i \in S$ be a collection of topological spaces. A basis of open sets in the **product topology** of $X = \prod_{i \in S} X_i$ consists of

$$\prod_{i \in F} U_i \times \prod_{i \in S \setminus F} X_i,$$

where $U_i \subset X_i$ are open subsets and F is a finite subset of S. An arbitrary open subset is a union of such open sets. Equivalently, the product topology is determined by the condition that $\pi_j : X \to X_j$, for any $j \in S$, is a continuous map.

Theorem 16.5 (Tychonoff's theorem)**.** *If each X_i is compact, such as finite with discrete topology, then $X = \prod_{i \in S} X_i$ is compact.*

Example 16.6. In particular, if R/I^m are finite, then $\prod_{m \geq 1} R/I^m$ is compact. Then $\widehat{R}$ is a closed subset of the compact set $\prod_{m \geq 1} R/I^m$, so $\widehat{R}$ is compact.

Definition 16.7. We equip $\widehat{R}$ with the induced **subspace topology**. A subset of $\widehat{R}$ is open if it is the intersection of an open subset of $\prod_{m \geq 1} R/I^m$ with $\widehat{R}$.

Note the natural map

$$\begin{array}{ccc} R & \longrightarrow & \prod_{m \geq 1} R/I^m \\ x & \longmapsto & (x + I^m) \end{array}$$

has its image in $\widehat{R}$. So there is a natural map $R \to \widehat{R}$. It is continuous.

Definition 16.8. R is **complete** in the I-adic topology if this map is an isomorphism.

Theorem 16.9 (Krull intersection theorem)**.** *If R is Noetherian, then*

$$\bigcap_{m \geq 1} I^m = 0.$$

Then $R \hookrightarrow \widehat{R}$.

Another approach is to define a_n for $n = 1, 2, \dots$ to be a Cauchy sequence if for any $m \geq 1$ there exists an $N \geq 1$ such that for any $n \geq N$, $a_n - a_N \in I^m$. Any Cauchy sequence has a limit in $\widehat{R}$.

Lemma 16.10. *If R is I-adically complete, then I is contained in the Jacobson radical of R.*

Proof. Pick any $a \in I$. Consider $\sum_{n \geq 0} a^n$. Its partial sums is a Cauchy sequence, since

$$(1 + \dots + a^n) - \left(1 + \dots + a^N\right) = a^{N+1} \dots + a^n,$$

and take $N = m$. Thus it converges to some $b \in R$. Then $(1 - a) b = (1 - a) \sum_{n \geq 1} a^n = 1$, since $(1 - a) \sum_{n=1}^N a^n = 1 - a^{N+1} \to 1$. Hence $1 - a \in R^*$, therefore $a \in \mathcal{J}(R)$. ☐

So let us look at local rings, such as discrete valuation rings.

Example 16.11. Start with $R = k[x]$ and $I = \langle x \rangle$. Localise at $\langle x \rangle$. Get

$$R_I = k[x]_{\langle x \rangle} = \left\{ \frac{f(x)}{g(x)} \;\middle|\; f(x), g(x) \in k[x], \; g(0) \neq 0 \right\}.$$

Now consider the completion of $k[x]_{\langle x \rangle}$. I claim that this is $k[[x]]$, since

$$\begin{array}{ccccc} \dots & \xrightarrow{s_2} & k[x] / \langle x^2 \rangle & \xrightarrow{s_1} & k[x] / \langle x \rangle \\ & & \wr\wr & & \wr\wr \\ & & k \oplus kx & & k \end{array},$$

so

$$\begin{array}{ccc} k[[x]] & \longrightarrow & k[x] / \langle x^n \rangle \\ \sum_{i \geq 0} a_i x^i & \longmapsto & \sum_{i=0}^{n-1} a_i x^i \end{array}$$

is an isomorphism.

Example 16.12. Let $R = \mathbb{Z}$ and $I = \langle p \rangle$, so

$$R_I = \mathbb{Z}_{\langle p \rangle} = \left\{ \frac{a}{b} \;\middle|\; (p, b) = 1 \right\}.$$

Let $\mathbb{Z}_p$ be the completion of $\mathbb{Z}_{\langle p \rangle}$ with respect to the topology given by the maximal ideal $p\mathbb{Z}_{\langle p \rangle}$. By Tychonoff's theorem, $\mathbb{Z}_p$ is compact. The elements of $\mathbb{Z}_p$ can be written as

$$a_0 + a_1 p + \dots, \qquad 0 \leq a_i \leq p - 1.$$

Then $\mathbb{Z}_p = \varprojlim_i \mathbb{Z}/p^i$, and the field of fractions of $\mathbb{Z}_p$ is $\mathbb{Q}_p$.

Let R be a complete local ring with maximal ideal I and residue field $k = R/I$.

Definition 16.13. The **reduction** of $x^n + a_{n-1} x^{n-1} + \dots + a_0$ is

$$x^n + \overline{a_{n-1}} x^{n-1} + \dots + \overline{a_0},$$

where $\bar{\cdot}$ means the image under $R \to R/I = k$.

Definition 16.14. A polynomial with coefficients in R is a **lifting** of a polynomial in $k[x]$, if it reduces to it modulo I.

Theorem 16.15 (Hensel's lemma)**.** *If the reduction of a monic polynomial $F(t) \in R[t]$ modulo I is a product of two coprime monic polynomials in $k[t]$, then these can be lifted to polynomials in $R[t]$ whose product is $F(t)$.*

Example 16.16. If $x^2 - a$ for $a \in R$ reduces over k to $x^2 - \overline{a} = (x - \alpha_1)(x - \alpha_2)$ for $\alpha_1, \alpha_2 \in k$ such that $\alpha_1 \neq \alpha_2$, then $x^2 - a = (x - a_1)(x - a_2)$ for $a_1, a_2 \in R$.