M4P55 Commutative Algebra

Lectured by Prof Alexei Skorobogatov
Typeset by David Kurniadi Angdinata

Autumn 2018

Contents

Lecture 1
Friday
05/10/18

0 Introduction

0.1 Outline

Why study commutative algebra? Number theory and algebraic geometry use this language. Structure of the course is

1. rings, ideals, zero divisors, nilpotents, etc,
2. prime and maximal ideals,
3. radicals of ideals, nilradicals and the Jacobson radicals,
4. localisation,
5. modules, Nakayama's lemma,
6. Noetherian and Artinian rings,
7. primary decomposition, and
8. valuation rings and discrete valuation rings.

0.2 References

1. M Reid, Undergraduate commutative algebra, 1995
2. M Atiyah and I G Macdonald, Introduction to commutative algebra, 1969

1 Rings and ideals

Definition 1.1. A commutative **ring** with 1 is a set A with two operations $+$ and $\cdot$, and two elements 0 and 1 such that the following holds.

1. $(A, +)$ is a group with zero 0.
2. Multiplication is
   (a) associative ($(xy)\,z = x\,(yz)$ for all $x, y, z \in A$),
   (b) commutative ($xy = yx$ for all $x, y \in A$), and
   (c) distributive over addition ($x\,(y + z) = xy + xz$ for all $x, y, z \in A$).
3. $x \cdot 1 = 1 \cdot x = x$ for all $x \in A$.

Example. $\mathbb{Z}$ is a ring. The set of even integers $2\mathbb{Z}$ is not a ring because it does not contain 1.

Remark 1.2. Can it happen that $0 = 1$? $x \cdot 0 = x \cdot (0 + 0) = x \cdot 0 + x \cdot 0$ gives $x \cdot 0 = 0$. But $x \cdot 1 = x$. Then $x = 0$ for all $x \in A$, so $A = \{0\}$.

Let A be a commutative ring with 1.

Definition 1.3. A **ring homomorphism** $f : A \to B$ is a homomorphism of abelian groups such that $f\,(xy) = f\,(x)\,f\,(y)$ for any $x, y \in A$ and $f\,(1) = 1$.

Proposition 1.4. A composition of homomorphisms is a homomorphism.

An **isomorphism** is a bijective homomorphism. If $f : A \to B$ is an isomorphism, we write $A \cong B$.

Lecture 2
Monday
08/10/18

Definition 1.5. A subset $I \subset A$ is called an **ideal** if I is a subgroup of $(A, +)$ and $AI = I$. Equivalently, for any $a \in A$ and any $x \in I$ we have $ax \in I$. The **quotient ring** A/I is the quotient group $\{a + I \mid a \in A\}$, which is actually a ring by $(a + I)(b + I) = ab+I$. $1+I$ is the 1 in A/I. $f : A \to A/I$ such that $f(a) = a+I$ is a surjective ring homomorphism. An ideal $I \subset A$ is **principal** if there is $r \in A$ such that $I = rA$.

Proposition 1.6. There is a natural bijection between the ideals of A that contain a fixed ideal I and the ideals of A/I.

Proof. Suppose $J \subset A$ is an ideal containing I. Then associate to J its image $f(J) \subset A/I$. To check this, note that since $f : A \to A/I$ is surjective, for any $x \in A/I$ there is a $y \in A$ such that $f(y) = x$. Hence $xf(J) = f(y) f(J) = f(yJ) \subset f(J)$. Conversely, take an ideal $M \subset A/I$ and associate to it $f^{-1}(M) \subset A$. This is an ideal in A. To check that for all $a \in A$ we have $af^{-1}(M) \subset f^{-1}(M)$, we note that this is equivalent to $f(a) M \subset M$, which is true. These maps are inverses to each other. □

Definition 1.7. Let $g : A \to B$ be a homomorphism of rings. The **image** is the subset $Im(g) = \{x \in B \mid \exists y \in A,\ g(y) = x\}$. The **kernel** is the subset $Ker(g) = \{y \in A \mid g(y) = 0\}$.

The image is a subring of $(B, +)$ but not necessarily an ideal, but the kernel is.

Example. Let $g : \mathbb{Z} \hookrightarrow \mathbb{Q}$. $2\mathbb{Z}$ is an ideal in $\mathbb{Z}$, but not in $\mathbb{Q}$.

An isomorphism theorem states that $A/Ker(g) \cong Im(g) = g(A)$ by $a \mapsto a + Ker(g)$.

2 Polynomial rings

Let R be a ring. Define $R[X]$ as the ring of polynomials $\sum_{i=0}^{n} a_i X^i$ with coefficients $a_i \in R$ and

$$\left(\sum_{i=0}^{k} a_i X^i\right)\left(\sum_{j=0}^{m} b_j X^i\right) = \sum_{k=0}^{n+m}\left(\sum_{k=i+j} a_i b_j\right) X^k.$$

Define $R[X_1, X_2]$ to be the ring $R[X_1][X_2]$. In general, $R[X_1, \dots, X_n] = R[X_1] \dots [X_2]$.

3 Zero-divisors, nilpotents, units

Definition 3.1. A **zero-divisor** in A is an element $x \in A$ such that there exists $y \in A$, $y \neq 0$, with the property that $xy = 0$. A ring with no non-zero zero-divisors is called an **integral domain**. A **nilpotent** is an element $x \in A$ such that $x^n = 0$ for some $n \geq 1$. A **unit** $a \in A$ is an element such that there exists $b \in A$ with the property that $ab = 1$. Such elements are also called **invertible**. b is denoted by a^{-1}. The units form a group under multiplication, denoted by A^*.

Example. In $A = \mathbb{Z}$, $\mathbb{Z}^* = \{1, -1\}$ and $\mathbb{Z}$ is an integral domain. In $A = \mathbb{Z}/4 = \{4\mathbb{Z}, 1 + 4\mathbb{Z}, 2 + 4\mathbb{Z}, 3 + 4\mathbb{Z}\}$, $2 + 4\mathbb{Z}$ is a zero-divisor in $\mathbb{Z}/4$ that is also nilpotent.

Lecture 3
Tuesday
09/10/18

Definition 3.2. A **field** is a ring in which $0 \neq 1$ and every non-zero element is a unit. So if k is a field, then $k \setminus \{0\} = k^*$.

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

1. A is a field.
2. The only ideals in A are $(0) = \{0\}$ and $(1) = A$.
3. Every homomorphism $A \to B$, where $B \neq 0$, is injective.

Proof.

$1 \implies 2$ Let $I \subset A$ be a non-zero ideal. Then there exists $x \in I$, $x \neq 0$. Then x is a unit, i.e. there exists $y \in A$ such that $xy = 1$. For all $a \in A$, $a = a.1 = a.y.x \in (x)$. Thus $I = A$.

$2 \implies 3$ Let $f : A \to B$. $Ker\,(f)$ is an ideal of A. If $Ker\,(f) \neq \{0\}$, then $Ker\,(f) = A$. But then $1 \in Ker\,(f)$ and $f\,(1) = 0$ but $f\,(1) = 1$ so in B we have that $0 = 1$. Then $B = \{0\}$, which is a contradiction.

$3 \implies 1$ Let $x \in A$, $x \neq 0$. If $1 \in (x) = xA$, then x is a unit. If $1 \notin (x)$, then x is not a unit. If $1 \notin (x)$, then consider the map $A \to A/\,(x)$ sending $a \mapsto a + (x)$. Since $1 \notin (x)$, $1 + (x)$ is not zero in $A/\,(x)$. So this is a non-injective homomorphism to a non-zero ring. This contradicts 3.

□

4 Prime ideals and maximal ideals

Definition 4.1. An ideal $P \subset A$ is a **prime ideal** if for any $x, y \in A$, $xy \in P$ implies $x \in P$ or $y \in P$. An ideal $M \subset A$ is called **maximal** if there does not exist an ideal I in A such that $M \subsetneq I \subsetneq A$.

Lemma 4.2. An ideal $P \subset A$ is prime if and only if A/P is an integral domain. An ideal $M \subset A$ is maximal if and only if A/M is a field.

Proof. Let $x, y \in A$ such that $xy \in P$. Then $(x + P)\,(y + P) = xy + P = P$. If $x \notin P$ and $y \notin P$, then $x + P \neq P$ and $y + P \neq P$. These are zero-divisors in A/P. Conversely, if A/P is not an integral domain, then it has zero-divisors. So there exist $x, y \in A$ such that $(x + P)\,(y + P) = P$. This implies $xy \in P$. Since P is prime, $x \in P$ or $y \in P$. So one of $x + P$ and $y + P$ is zero in A/P. Recall that there is a bijection between the ideals in A containing M with the ideals in A/M. Thus $M \subset A$ is maximal if and only if the only ideals in A/M are (0) and (1), if and only if A/M is a field. □

Remark 4.3. Every field is an integral domain, hence every maximal ideal is prime. The converse is false. Take any integral domain which is not a field, such as $\mathbb{Z}$. Then $(0) \in \mathbb{Z}$ is a prime ideal which is not a maximal ideal.

Proposition 4.4. If $f : A \to B$ is a homomorphism of rings, and $P \subset B$ is a prime ideal, then $f^{-1}\,(P)$ is a prime ideal in A.

Proof. Assume that for some $x, y \in A$ we have $xy \in f^{-1}\,(P)$. Then $f\,(xy) = f\,(x)\,f\,(y) \in P$. Then $f\,(x) \in P$ or $f\,(y) \in P$. Then $x \in f^{-1}\,(P)$ or $y \in f^{-1}\,(P)$. □

Remark 4.5. This does not hold for maximal ideals. Let $f : \mathbb{Z} \hookrightarrow \mathbb{Q}$. $f^{-1}\,((0)) = (0)$, but (0) is maximal in $\mathbb{Q}$ and not maximal in $\mathbb{Z}$. But if $f : A \to B$ is a surjective homomorphism of rings, then f^{-1} sends maximal ideals of B to maximal ideals of A. (Exercise)

Theorem 4.6. Every non-zero ring contains at least one maximal ideal.

We need Zorn's lemma, which belongs to set theory. A **partially ordered set** or **poset** is a set S equipped with a **partial order**. By definition it is a reflexive, transitive, antisymmetric binary relation $\leq$,

$$x \leq x, \qquad x \leq y, y \leq z \implies x \leq z, \qquad x \leq y, y \leq x \implies x = y.$$

We don't require that for arbitrary x and y in S, we have either $x \leq y$ or $y \leq x$. A subset $T \subset S$ is called a **chain** if for any $x \in T$, $y \in T$ we have $x \leq y$ or $y \leq x$. An **upper bound** for a subset $T \subset S$ is an element $x \in S$ such that for any $t \in T$ we have $t \leq s$. A **maximal element** in S is an element $x \in S$ such that if $y \in S$ and $y \geq x$, then $y = x$.

Lecture 4
Friday
12/10/18

Theorem 4.7 (Zorn's lemma)**.** If S is a non-empty partially ordered set such that every chain in S has an upper bound in S, then S contains a maximal element.

Proof of Theorem 4.6. Let A be a non-zero ring. To apply Zorn's lemma it is enough to show that every growing chain of ideals $I_1 \subset I_2 \subset \dots$, such that $1 \in I_i$ for all i, has an upper bound which is an ideal not equal to A, so not containing 1. Then Zorn's lemma applied to the set of ideals of A not containing 1 and ordered by inclusion, implies the existence of a maximal ideal. So we have a chain I_j, where j is an element of a set J. Consider $I = \bigcup_{j \in J} I_j$. Claim that I is an ideal in A and $1 \notin I$.

1. $1 \notin I$ is clear. Because otherwise $1 \in I$ gives $1 \in I_j$ for $j \in J$, but it is a contradiction.
2. For any $a \in A$ we have $aI \subset I$, so for all $x \in I$, $ax \in I$. But then $x \in I_j$ for some j. Then $ax \in I_j \subset I$.
3. Suppose $x, y \in I$. Must show $x + y \in I$. There exists $j_1 \in J$ such that $x \in I_{j_1}$. Similarly, there exists $j_2 \in J$ such that $y \in I_{j_2}$. Recall that I_j for $j \in J$ is a chain. Hence either $j_1 \leq j_2$ or $j_2 \leq j_1$. This means that either $I_{j_1} \subset I_{j_2}$ or $I_{j_2} \subset I_{j_1}$. Without loss of generality assume that $I_{j_1} \subset I_{j_2}$. Then $x, y \in I_{j_2}$. Hence $x + y \in I_{j_2}$, hence $x + y \in I$. This proves that I is an ideal not containing 1.

□

Definition 4.8. A ring with a unique maximal ideal is called a **local ring**.

Corollary 4.9. Let I be an ideal of A and $I \neq A$. Then I is contained in a maximal ideal of A.

Proof. There is a bijection between the ideals of A containing I and the ideals in A/I. If $I \subset J \subset A$, then $J \mapsto J/I$. J/I is an ideal in A/I. By Theorem 4.6, A/I contains a maximal ideal, say $M \subset A/I$. Let $f : A \to A/I$ be the map sending $x \mapsto x + I$. Consider $f^{-1}(M) \subset A$. This is an ideal in A. In general, if $I \subset J \subset A$ are ideals, then f induces an isomorphism of rings $A/J \to (A/I)(J/I)$. For additive groups, this is one of the standard isomorphisms theorems, but this respects multiplication, so is an isomorphism of rings. Now, we know that M maximal in A/I implies that (A/I) is a field. This ring is isomorphic to $A/f^{-1}(M)$. Hence $A/f^{-1}(M)$ is also a field. Therefore, $f^{-1}(M)$ is maximal in A. □

Corollary 4.10. Every non-unit is contained in a maximal ideal.

Proof. If $x \in A$ is a non-unit, consider (x). $1 \notin (x)$, otherwise x is a unit. By Corollary 4.9 (x) is contained in a maximal ideal of A. □

Example.

1. Every field is a local ring. In this case (0) is a maximal ideal.
2. Let k be a field. Consider the ring of formal power series $k[[t]] = \{a_0 + a_1 t + \cdots \mid a_i \in k\}$, such that

$$\left(\sum_{i=0}^{\infty} a_i t^i\right)\left(\sum_{j=0}^{\infty} b_j t^j\right) = a_0 b_0 + (a_0 b_1 + a_1 b_0) t + \dots.$$

   Then the principal ideal (t) is a maximal ideal. Indeed, $k[[t]]/(t) \cong k$ is a field. (Exercise: $k[[t]] \setminus (t) = k[[t]]^*$)

3. $\mathbb{Z}_{(p)} = \{a/b \mid a, b \in \mathbb{Z},\ b \neq 0,\ p \nmid b\}$. (Exercise: (p) is a maximal ideal and there are no other maximal ideals)

If A is a local ring with maximal ideal M, then A/M is called the **residue field** of A.

Lemma 4.11 (Prime avoidance)**.** Let A be a ring and $P \subset A$ be a prime ideal. Suppose that $I_1, \dots, I_n$ are ideals in A such that $\bigcap_{i=1}^n I_i \subset P$. Then there exists j, $1 \leq j \leq n$, such that $I_j \subset P$. If $\bigcap_{i=1}^n I_i = P$, then there exists j, $1 \leq j \leq n$, such that $I_j = P$.

Proof. Suppose our claim is false. Then there exists $a_j \in I_j$ such that $a_j \notin P$ for $j = 1, \dots, n$. Then $a_1 \dots a_n \in \bigcap_{j=1}^n I_i \subset P$. $(a_1 \dots a_{n-1}) a_n \in P$ gives $a_1 \dots a_{n-1} \in P$ or $a_n \in P$. But $a_n \notin P$, so $a_1 \dots a_{n-2} \in P$, a contradiction. The second statement follows. We know that $I_k \subset P$ for some k, $1 \leq k \leq n$, but $P = \bigcap_{j=1}^n I_j \subset I_k$. Hence $P = I_k$. □

Lecture 5
Monday
15/10/18

5 Nilradical and the Jacobson radical

Proposition 5.1. Let A be a ring. The set $N(A)$ of all nilpotent elements of A is an ideal in A. It is called the **nilradical** of A. The quotient ring $A/N(A)$ has no non-zero nilpotents.

Proof. Clearly, if $x^n = 0$ and $y^n = 0$, then $(xy)^n = 0$, if $n \geq m$. $(x+y)^{n+m}$ is the sum with coefficients of of monomials in which either the power of x is $\geq n$ or the power of y is $\geq m$. So this is zero. Let $a \in A$. Then $(ax)^n = 0$. Therefore, $N(A)$ is an ideal. Now let $t + N(A)$ for $t \in A$ be a nilpotent element in $A/N(A)$. For some k we have $t^k + N(A)$ is the trivial coset, that is $t^k \in N(A)$. Thus $\left(t^k\right)^l = 0$ for some $l > 0$. Hence $t \in N(A)$, so $t + N(A)$ is the zero element of $A/N(A)$. □

Proposition 5.2. The nilradical $N(A)$ is the intersection of all prime ideals of A.

Proof.

- $\subset$ $N(A) \subset \bigcap_{P \subset A} P$, where P is a prime ideal of A. Take $x \in A$, $x^n = 0$. Take a prime ideal $P \subset A$. We have that $P \ni x^n = x \dots x$ gives $x \in P$.

- $\supset$ Now let $f \in A$ be a non-nilpotent element, that is $0 \notin \left\{f^i \mid i \geq 1\right\}$. Let Σ be the set of ideals of A that do not intersect $\left\{f^i \mid i \geq 1\right\}$. Σ contains the zero ideal (0), so $\Sigma \neq \emptyset$. Order the elements of Σ by inclusion. Every chain in Σ has an upper bound. If I_j for $j \in J$ is a chain, then $\bigcup_{j \in J} I_j$ is an ideal of A. Moreover, if $f^k \in \bigcup_{j \in J} I_j$, then $f^k \in I_{j_0}$ for some $j_0 \in J$, but this is impossible. By Zorn's Lemma, we know that Σ has a maximal element. Call it P. Claim that P is a prime ideal. To prove this, assume that $x, y \in A$ such that $x, y \notin P$. We must show that $xy \notin P$. Consider $P + (x)$, all elements of the form $\alpha + rx$, where $\alpha \in P$ and $r \in A$. $x \notin P$ gives $P \neq P + (x)$. By construction, P is maximal in Σ, hence $P + \sigma$ is not in Σ, that is there exists $n \geq 1$ such that $f^n \in P + (x)$. Similarly, there exists m such that $f^m \in P + (y)$. Therefore, f^{n+m} belongs to $P + (xy)$. If $xy \in P$, then $P + (xy) = P$ but then $f^{n+m} \in P$, which is absurd because $P \in \Sigma$. Thus $xy \notin P$. This shows that P is a prime ideal and $f \notin P$.

□

What happens if we consider the intersection of all maximal ideals of A. This intersection is called the **Jacobson radical** of A. It is denoted by $J(A)$.

Proposition 5.3. $x \in J(A)$ if and only if $1 - xy$ is a unit in A for all $y \in A$.

Proof. Suppose that $x \in J(A)$, that is x is contained in every maximal ideal of A, but $1 - xy$ is not a unit for some $y \in A$. By Corollary 4.10 every non-unit is contained in some maximal ideal, so there exists a maximal ideal $M \subset A$ such that $1 - xy \in M$. Since $x \in M$ we conclude that $1 \in M$, which is impossible. Conversely, suppose $x \notin J(A)$, that is $x \notin M$ for some maximal ideal $M \subset A$. Consider the sum of two ideals $M + (x)$. This is an ideal in A, such that $M \subsetneq M + (x)$. Since M is maximal, we have $M + (x) = A$. Therefore $1 = m + xy$, where $m \in A$ and $y \in A$. Now $1 - xy = m \in M$ cannot be a unit. □

Let $I \subset A$ be an ideal. The **radical** $rad(I)$ or $r(I)$ or $\sqrt{I}$ is defined as $\{x \in A \mid \exists n \geq 1,\ x^n \in I\}$.

Proposition 5.4. $r(I)$ is the intersection of all prime ideals of A that contain I.

Proof. Use the bijection between ideals containing I and the ideals in A/I. □

Lecture 6
Tuesday
16/10/18

Definition 5.5. Let J be an index set. Suppose we have a ring R_j for $j \in J$. $\prod_{j \in J} R_j$ has a natural structure of a ring. 0 in $\prod_{j \in J} R_j$ is $(0, \dots, 0)$ and 1 in $\prod_{j \in J}$ is defined as $(1, \dots, 1)$, and

$$\left(r_j\right)_{j \in J} + \left(r'_j\right)_{j \in J} = \left(r_j + r'_j\right)_{j \in J}, \qquad \left(r_j\right)_{j \in J} \cdot \left(r'_j\right)_{j \in J} = \left(r_j \cdot r'_j\right)_{j \in J}.$$

$\prod_{j \in J} R_j$ is called the **product of rings** R_j for $j \in J$. If R is a ring equipped with homomorphisms $f_j : R \to R_j$ for each $j \in J$, then $(f_j) : R \to \prod_{j \in J} R_j$ is a homomorphism of rings.

Recall that $N(R) = \bigcap_{P \subset R} P$, where P are prime ideals of R. Consider the product ring $\prod_{P \subset R} R/P$. Putting together the canonical surjective maps $R \to R/P$ by $x \mapsto x + P$ for all $P \subset R$ we obtain a homomorphism $f : R \to \prod_{P \subset R} R/P$. $Ker(f) = \bigcup_{P \subset R} Ker[R \to R/P] = \bigcap_{P \subset R} = N(R)$. Hence we get an injective homomorphism $R/N(R) \to \prod_{P \subset R} R/P$. Similarly, we get an injective homomorphism $R/J(R) \to \prod_{M \subset R} R/M$, where M are maximal ideals of R and $J(R)$ is the Jacobson radical of R.

6 Localisation of rings

Localisation refers to introducing denominators.

Example. From $R = \mathbb{Z}$ to $\mathbb{Q} = \{a/b \mid a, b \in \mathbb{Z},\ b \neq 0\}$.

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

Example.

1. Take any $a \in A$ which is not nilpotent, that is $a^n = 0$ for $n \geq 1$. Then $\left\{1, a, a^2, \dots\right\}$ is a multiplicative set.
2. Let $P \subset A$ be a prime ideal. Then $A \setminus P$ is a multiplicative set. Indeed, $x, y \notin P$ gives $xy \notin P$.
3. Let $P_j \subset A$, for $j \in J$, be a family of prime ideals of A. Then $A \setminus \bigcup_{j \in J} P_j = \bigcap_{j \in J} (A \setminus P_j)$ is a multiplicative set.
4. A^* is a multiplicative set in A.
5. The set of all non-zero-divisors of A is a multiplicative set.
6. Let $I \subset A$ be an ideal. Then $1 + I = \{1 + x \mid x \in I\}$ is a multiplicative set.

Definition 6.2. Let A be a ring with a multiplicative set S. Consider $A \times S$, that is the set of pairs of elements (a, s), where $a \in A$ and $s \in S$. Define an equivalence relation $\sim$ as follows. $(a, s) \sim (b, t)$ if and only if there exists $u \in S$ such that $u(at - bs) = 0$. Define $S^{-1}A$ to be the set of equivalence classes of $\sim$. Write the equivalence class of (a, s) as a/s. Define multiplication on $S^{-1}A$ as

$$\frac{a}{s} \cdot \frac{b}{t} = \frac{ab}{st}.$$

Define addition on $S^{-1}A$ as

$$\frac{a}{s} + \frac{b}{t} = \frac{at + bs}{st}.$$

Define 0 in $S^{-1}A$ as $0/1$ and we define 1 in $S^{-1}A$ as $1/1$.

(Exercise: check that if $(a, s) \sim (a', s')$ and $(b, t) \sim (b', t')$, then $(ab, st) \sim (a'b', s't')$)
(Exercise: check that if $(a, s) \sim (a', s')$ and $(b, t) \sim (b', t')$, then $(at + bs, st) \sim (a't' + b's', s't')$)
(Exercise: with this definition $S^{-1}A$ is a ring)

Remark 6.3. $\sim$ is indeed an equivalence relation. $(a, s) \sim (a, s)$, $(a, s) \sim (b, t)$ gives $(b, t) \sim (a, s)$. Let us check that if $(a, s) \sim (b, t)$ and $(b, t) \sim (c, r)$, then $(a, s) \sim (c, r)$. There exist $u, v \in S$ such that $u(at - bs) = 0$ and $v(br - ct) = 0$. Then $uv(atr - bsr) = 0$ and $uv(brs - cts) = 0$, so $uvt(ar - bs) = 0$.

Lemma 6.4. Let A be a ring with a multiplicative set S. Then $f : A \to S^{-1}A$ defined by $f(x) = x/1$ is a homomorphism of rings. $Ker(f) = 0$ if and only if S contains no zero-divisors.

Proof.

$$f(x + y) = \frac{x + y}{1} = \frac{x}{1} + \frac{y}{1}, \qquad f(xy) = \frac{xy}{1} = \frac{x}{1} \cdot \frac{y}{1}.$$

$Ker(f) = \{x \mid \exists u \in S,\ ux = 0\}$ since $x/1 = 0/1$ if and only if there exists $u \in S$ such that $u(x \cdot 1 - 0 \cdot 1) = 0$. □

Example. Let k be a field. Explore what happens when $A = k\left[x, y\right] / \left(xy\right)$ and $S = \{1, x, \dots\}$. Determine $S^{-1}A$ and $Ker\left(f\right)$.

Lecture 7 Friday 19/10/18

Lecture 7 is a problem class.

Lecture 8 Monday 22/10/18

Lemma 6.5 (Universal property of localisation)**.** Let A be a ring with a multiplicative set $S \subset A$. Suppose $g : A \to B$ is a homomorphism such that $g\left(S\right) \subset B^*$, that is for all $s \in S$, $g\left(s\right)$ is a unit in B. Then there exists a unique homomorphism $h : S^{-1}A \to B$ such that $g = h \circ f$, where $f : A \to S^{-1}A$ is the canonical map.

Proof. Define $h\left(a/s\right) = g\left(a\right)g\left(s\right)^{-1}$ since g invertible. Check that h is well-defined, that is if $a/s = a'/s'$, then $u\left(as' - a's\right) = 0$ for $u \in S$. Apply g and get $g\left(u\right)\left(g\left(a\right)g\left(s'\right) - g\left(a'\right)g\left(s\right)\right) = 0$. $g\left(u\right) \in B^*$ and $g\left(a\right)g\left(s'\right) = g\left(a'\right)g\left(s\right)$. Hence $g\left(a\right)g\left(s\right)^{-1} = g\left(a'\right)g\left(s'\right)^{-1}$. Take any $a \in A$. Then $f\left(a\right) = a/1$, hence $\left(h \circ f\right)\left(a\right) = g\left(a\right)$. Finally, let us show there is only one homomorphism $h : S^{-1}A \to B$ such that $g = h \circ f$. Suppose $h' : S^{-1}A \to B$ is such that $g = h' \circ f$, so that for any $a \in A$ we have $g\left(a\right) = h'\left(a\right)$. For any $s \in S$, s^{-1} is an element of $S^{-1}A$, and so is s. $1 = s^{-1}s$ gives $1 = h'\left(1\right) = h'\left(s^{-1}\right)h'\left(s\right)$. Thus $h'\left(s^{-1}\right) = h'\left(s\right)^{-1} = g\left(s\right)^{-1}$ because h' on the image of A in $S^{-1}A$ is the same as g. Comparing this with the definition of h we see that $h' = h$. □

Let $I \subset A$ be an ideal. Define $S^{-1}I = \{x/s \mid x \in I,\ s \in S\}$. This is an ideal in $S^{-1}I$. It is the ideal generated by $f\left(I\right) \subset S^{-1}A$.

Proposition 6.6. Let A be a ring with a multiplicative set S. Let $I_1, \dots, I_n$ be ideals in A. Then

1. $S^{-1}\left(I_1 + \dots + I_n\right) = S^{-1}I_1 + \dots + S^{-1}I_n$,
2. $S^{-1}\left(I_1 \dots I_n\right) = S^{-1}I_1 \dots S^{-1}I_n$,
3. $S^{-1}\left(\bigcap_{j=1}^n I_j\right) = \bigcap_{j=1}^n S^{-1}I_j$, and
4. $r\left(S^{-1}I\right) = S^{-1}r\left(I\right)$, where $r\left(I\right)$ is the radical of I.

Proposition 6.7. Every ideal of $S^{-1}A$ is of the form $S^{-1}I$ for some ideal $I \subset A$.

Proof. Start with an ideal $J \subset S^{-1}A$. Consider $f^{-1}\left(J\right) \subset A$. This is an ideal. Call it I. Claim that $J = S^{-1}I$. Pick any element $a/s \in J$. Then $a \in J$. Since $f\left(a\right) = a/1 \in J$ we have that $a \in I$. Therefore, $a/s \in S^{-1}I$. This proves $J \subset S^{-1}I$. But it is clear that $S^{-1}I \subset J$. Indeed, $x \in I$ then $x/1 \in J$. But J is an ideal, hence $x/s \in J$. □

Theorem 6.8. The prime ideals in $S^{-1}A$ are the ideals $S^{-1}P$, where P is a prime ideal of A such that $P \cap S \neq \emptyset$. Thus we have a bijection between the set of prime ideals in $S^{-1}A$ and the set of prime ideals in A that do not intersect S.

Proof. Suppose that P is a prime ideal in A, $P \cap S \neq \emptyset$. Claim that $S^{-1}P$ is a prime ideal in $S^{-1}A$. If $\left(a/s\right)\left(b/t\right) \in S^{-1}P$, then $\left(a/s\right)\left(b/t\right) = c/u$, where $c \in P$, $u \in S$. This is equivalent to $v\left(abu - cst\right) = 0$ for some $v \in S$. $\left(ab\right)\left(vu\right) = c \in P$ such that $v \in P$. $vu \in S$ and $S \cap P = \emptyset$, so $vu \notin P$. But $P \subset A$ is a prime ideal, hence $ab \in P$. Thus $a \in P$ gives $a/s \in S^{-1}P$ or $b \in P$ gives $b/t \in S^{-1}P$. This proves $S^{-1}P \subset S^{-1}A$ is prime. For any ideal $J \subset S^{-1}A$, we know that $f^{-1}J$ is an ideal in S. Moreover, if J is prime, then $f^{-1}J \subset A$ is prime. Let us show that $f^{-1}J \cap S = \emptyset$. Otherwise, take $s \in S \cap f^{-1}J$, so $s/1 \in J$. But $1/s \in J^{-1}A$, hence $1 = \left(1/s\right)s \in J$, so $J = S^{-1}A$. But J is a prime ideal, so $J \neq S^{-1}A$. To show that $P \mapsto S^{-1}P$ and $J \mapsto f^{-1}J$ are the identity maps, we need to check that $P = f^{-1}\left(S^{-1}P\right)$ and $J = S^{-1}f^{-1}\left(J\right)$. $S^{-1}P = \{x/s \mid x \in P,\ s \in S\}$. If $y \in f^{-1}\left(S^{-1}P\right) \subset A$ is such that $f\left(y\right) = x/s$, then $y/1 = x/s$. Hence $ys = x \in P$. Since $P \cap S = \emptyset$, $s \notin P$. Therefore, $y \in P$. Hence $P = f^{-1}\left(S^{-1}A\right)$. Now let us prove that $J = S^{-1}f^{-1}\left(J\right)$. But in Proposition 6.7 we showed that there is an ideal $I \subset A$ such that $J = S^{-1}I$. In the proof of Proposition 6.7 we have taken $I = f^{-1}\left(J\right)$. So we are done. □

Lecture 9 Tuesday 23/10/18

7 Determinants

Lemma 7.1. Let $f(x_1, \dots, x_n) \in \mathbb{Z}[x_1, \dots, x_n]$. If f as a function $\mathbb{Z}^n \to \mathbb{Z}$ is zero, that is f only takes zero values on arbitrary elements of $\mathbb{Z}^n$, then f is the zero polynomial.

Proof. Induction in n. If $n = 1$, then $f(x)$ is a polynomial with infinitely many roots. So $f(x)$ is the zero polynomial, so cannot have more than $\deg(f)$ roots. Assume we know the lemma for $n - 1$ variables. Write $f(x_1, \dots, x_n) = \sum_{i=0}^{N} f_i(x_1, \dots, x_{n-1}) x_n^i$ for $f_j(x_1, \dots, x_{n-1}) \in \mathbb{Z}[x_1, \dots, x_{n-1}]$. Fix $x_1, \dots, x_{n-1}$. We get a polynomial in one variable x_n, so this polynomial has zero coefficients. This implies that each $f_i(x_1, \dots, x_n)$ takes only zero values. By the induction assumption, each f_i is the zero polynomial. □

Remark 7.2. This means that if a polynomial formula with coefficients in $\mathbb{Z}$ is true in $\mathbb{Z}$, this is true in an arbitrary commutative ring.

Example. $(x+y)^n = \sum_{i=0}^{n} \binom{n}{i} x^i y^{n-i}$ is true in any ring.

The underlying fact is the existence of a canonical map $\mathbb{Z} \to R$ by $1 \mapsto 1$.

Definition 7.3. Let R be a commutative ring. Let $A = (a_{ij})$ be a square matrix for $1 \le i \le n$ and $1 \le j \le n$, with entries in R. Then $\det(A)$ is defined as $(-1)^{i+1} a_{i1} M_{i1} + \dots (-1)^{i+n} a_{in} M_{in}$ for i fixed. Here M_{ij} is the determinant of the $(n-1) \times (n-1)$ submatrix of A obtained by removing the i-th row and the j-th column.

Proposition 7.4. $\det(A) = (-1)^{i+1} a_{i1} M_{i1} + \dots (-1)^{i+n} a_{in} M_{in}$.

Proof. This is known for matrices with entries in $\mathbb{C}$, so by Remark 7.2 this holds in any commutative ring. □

Remark 7.5. The official definition is

$$\det(A) = \sum_{\pi \in S_n} sgn(\pi) a_{1\pi(1)} \dots a_{n\pi(n)},$$

where $sgn : S_n \to \{\pm 1\}$.

Proposition 7.6. For $i \neq j$,

$$(-1)^{j+1} a_{i1} M_{j1} + \dots + (-1)^{j+n} a_{in} M_{jn} = 0,$$

$$(-1)^{j+1} a_{1i} M_{1j} + \dots + (-1)^{j+n} a_{ni} M_{nj} = 0.$$

Define the **adjacent** matrix as an $n \times n$ matrix $A_{ij}^v = (-1)^{i+j} M_{ji}$. Putting together all the previous identities we get the following.

Theorem 7.7. $A \cdot A^v = A^v \cdot A = \det(A) I_n$.

Lecture 10
Friday
26/10/18

8 Modules

Definition 8.1. Let A be a ring. A **module** M over A is an abelian group $(M, 0, +)$ with an action $\cdot$ of A on M, that is $A \times M \to M$ by $a \cdot m = am$, such that the following axioms hold.

1. $1 \cdot m = m$ for all $m \in M$ and $a \in A$.
2. $\mu \cdot (\lambda \cdot m) = (\mu\lambda) \cdot m$ $\lambda, \mu \in A$.
3. $\lambda(x+y) = \lambda x + \lambda y$ for all $\lambda \in A$ and $x, y \in M$.
4. $(\mu + \lambda) x = \mu x + \lambda x$ for all $\mu, \lambda \in A$ and $x \in M$.

Example.

1. $M = A$. More generally, consider an ideal $I \subset A$. A acts on I by $A \times I \to I$ by $a \cdot x = ax$.
2. If A is a field, then an A-module is the same as a vector space over this field.
3. Take M to be any abelian group. Take $A = \mathbb{Z}$. Define an action of $\mathbb{Z}$ as follows. $1 \cdot m = m$ and $n \cdot m = (1 + \cdots + 1) \cdot m = m + \cdots + m = nm$. $0 = n + (-n) \in \mathbb{Z}$, then $0 = (n + (-n)) \cdot m = nm + (-n)\, m$. Hence $(-n) \cdot m = -(n \cdot m) = -(m + \cdots + m)$. So, there is exactly one way to equip any abelian group with the structure of a $\mathbb{Z}$-module.
4. Let k be a field and let $A = k[x]$. A $k[x]$-module is a vector space over k with extra structure $x \times M \to M$. This is a linear transformation of M. It can be arbitrary. Thus a $k[x]$-module is a pair (M, f), where M is a k-vector space and $f : M \to M$ is linear transformation of M.

Definition 8.2. Let M and N be A-modules. A map $f : M \to N$ is called a **homomorphism of A-modules** if f is a homomorphism of abelian groups and $f(a, m) = af(m)$ for any $a \in A$ and $m \in M$. If $f : M \to N$ and $g : M \to N$ are homomorphisms of A-modules, then so is $f + g$, so we get $Hom_A(M, N)$, a group of such homomorphisms. This is also an A-module via the action $(a, f(a)) \mapsto a \cdot f(a)$.

Definition 8.3. A **submodule** $N \subset M$ is a subgroup, stable under the action of A. Then M/N is naturally an A-module with A-action inherited from M. Define $(N : M) = \{a \in A \mid raM \subset rN \subset N\}$. This is an ideal in A. In particular, can do this when $N = 0$. Note $Ann(M) = (0 : M) = \{a \in A \mid aM = 0\}$. This is called the **annihilator** of M.

Definition 8.4. If $f : M \to N$ is a homomorphism of A-modules, then $Ker(f)$ is an A-module and $Im(f) \cong M/Ker(f)$ is as isomorphism of A-modules.

Definition 8.5. An A-module M is **finitely generated** if there exist $m_1, \dots, m_n$ in M such that $M = \{a_1 m_1 + \cdots + a_n m_n \mid a_i \in A\}$.

Example. A **free** A-module of rank n is the set $A^n = \{(a_1, \dots, a_n) \mid a_i \in A\}$ with coordinate-wise addition. $a \in A$ acts on $(a_1, \dots, a_n)$ by sending it to $(aa_1, \dots, aa_n)$. If $f(1, 0, \dots, 0) = m_1$, $f : A^m \to M$ is an example of an A-module homomorphism.

Lemma 8.6. Let A be a ring. Let M be a finitely generated A-module and let $A \subset A$ be an ideal such that $JM = M$, that is sums of xm, where $x \in J$ and $m \in M$, give all of M. Then there exists $a \in J$ such that $(1 - a)\, M = 0$.

Proof. Let $m_1, \dots, m_n$ be a set of generators of M. $m_i \in M = JM$, so $m_i = x_{i1} m_1 + \cdots + x_{in} m_n$, where $x_{ij} \in J$. Let $X = (x_{ij})_{1 \le i,j \le n}$, so

$$(I_n - X) \begin{pmatrix} m_1 \\ \vdots \\ m_n \end{pmatrix} = 0.$$

Let $(I_n - X)^v$ be the adjunct matrix of $I_n - X$. Then $(I_n - X)^v (I_n - X) = \det(I_n - X)\, I_n$. Hence

$$\det(I_n - X) \begin{pmatrix} m_1 \\ \vdots \\ m_n \end{pmatrix} = \begin{pmatrix} 0 \\ \vdots \\ 0 \end{pmatrix}.$$

$\det(I_n - X) = \prod_{i=1}^n (1 - x_{ii}) + J \equiv 1 \mod J$. So $\det(I_n - X) = 1 - a$, where $a \in J$. $(1 - a)\, m_i = 0$ for all i gives $(1 - a)\, M = 0$. □

Lecture 11
Monday
29/10/18

Corollary 8.7 (Nakayama's lemma)**.** Let A be a ring and let M be an A-module, which is finitely generated. Let $I \subset A$ be an ideal contained in the Jacobson radical $J(A)$. Then $IM = M$ implies $M = 0$.

Proof. Lemma 8.6 gives an $a \in I$ such that $(1 - a)\, M$. But $a \in J(A)$. By Proposition 5.3 $1 - a \in A^*$ so that there exists $u \in A^*$ such that $u(1 - a) = 1$, so $M = 1 \cdot M = u(1 - a) \cdot M = 0$. □

Another proof considers $M = (m_1, \dots, m_n)$. Let us call a generating set minimal, if no proper set is a generating set. Assume that $m_1, \dots, m_n$ is a minimal generating set. $IM = M$ implies that $m_1 = a_1 m_1 + \dots + a_n m_n$, where $a_i \in I$. $(1 - a_1) m_1 = a_2 m_2 + \dots + a_n m_n$. Proposition 5.3 says that $1 - a_1 \in A^*$. Hence $m_1 = (1 - a_1)^{-1} a_2 m_2 + \dots + (1 - a_1)^{-1} a_n m_n$. This is a contradiction, because $m_2, \dots, m_n$ is a generating set.

9 Localisation of modules

Definition 9.1. Let A be a ring with a multiplicative set S, and let M be an A-module. Define $\sim$ on $M \times S$ by $(m, s) \sim (n, t)$ if and only if there exists $u \in S$ such that $u (tm - sn) = 0$. This is an equivalence relation. Denote the equivalence class of (m, s) by m/s. Then the set of these equivalence classes form a module denoted by $S^{-1}M$ over $S^{-1}A$. The action of $S^{-1}A$ on $S^{-1}M$ is $(a/s)(m/t) = (am/st)$. $m/s + n/t = (mt + ns)/st$. The zero in $S^{-1}M$ is $0/1$.

Definition 9.2. Let A be a ring and let $P \subset A$ be a prime ideal. Then $S = A \setminus P$ is a multiplicative set. The ring $S^{-1}A$ is denoted A_P. It is called the localisation of A at P. Recall that by Theorem 6.8 the prime ideals of A_P are of the form $S^{-1}I$, where $I \subset A$ is a prime ideal such that $I \cap (A \setminus P) = \emptyset$, if and only if $I \subset P$.

Theorem 9.3. Let A be a ring with a prime ideal P. Then $a \in A_P$ is a unit if and only if $a \notin PA_P = S^{-1}P = (A \setminus P)^{-1} P$. The ideal PA_P is the unique maximal ideal of A_P. So A_P is a local ring.

Proof. Suppose $a/s \in A_P$ is a unit. Then for some $b/t \in A_P$ we have $(a/s)(b/t) = 1$. $ab/st - 1/1 = 0$ if and only if there exists $u \in S$ such that $u (ab - st) = 0$. $uab = ust \in S = A \setminus P$. Hence $a \notin P$, so that $a/s \notin PA_P$. Conversely, if $a/s \notin PA_P$, then $a \notin P$ and $s \in S$ gives $a \in S = A \setminus P$. So a/s is a unit whose inverse is s/a. PA_P is a maximal ideal, because joining any new element will be the whole ring, as this element must be a unit. □

Example. $\mathbb{Z}_{(p)} = \{a/b \mid a, b \in \mathbb{Z},\ (p, b) = 1\}$ and

$$p\mathbb{Z}_{(p)} = \left\{ \frac{a}{b} \;\middle|\; a, b \in \mathbb{Z},\ p \mid a,\ (p, b) = 1 \right\}, \qquad \mathbb{Z}_{(p)}^* = \left\{ \frac{a}{b} \;\middle|\; a, b \in \mathbb{Z},\ p \nmid a,\ (p, b) = 1 \right\}.$$

Do the same for $A = k[x]$ and $P = (f(x))$, where $f(x)$ is irreducible.

Proposition 9.4. Let M be an A-module. Then $M = 0$ if and only if $M_P = 0$ for all maximal ideals $P \subset A$.

Proof. Suppose $M \neq 0$. Choose $x \in M$, $x \neq 0$. Define $I = Ann(x) = \{a \in A \mid ax = 0\}$. This is an ideal in A, and $I \neq A$ because $1 \cdot x = x$, so $1 \notin I$. Let P be a maximal ideal such that $I \subset P$. Claim that $M_P \neq 0$. Consider $x/1 \in M_P$. If $M_P = 0$, then $x/0 = 0/1$, so $ux = 0$ for some $u \in A \setminus P$. $u \in I = Ann(x)$ but $u \notin P$. This is a contradiction because $I \subset P$. □

Lecture 12
Tuesday
30/10/18

10 Chain conditions: Noetherian and Artinian rings

Lemma 10.1. Let Σ be a partially ordered set. Then the following properties are equivalent.

1. Every non-empty subset of Σ has a maximal element.
2. Every ascending chain $x_1 \leq x_2 \leq \dots$ is stationary, that is there exists n such that for any $m \geq 0$ we have $x_{n+m} = x_n$.

Proof.

$1 \implies 2$ Any ascending chain has a maximal element, say x_n. Hence $x_{m+n} = x_n$, for all $m \geq 0$.

$2 \implies 1$ Suppose $S \subset \Sigma$ does not have a maximal element. Choose $x_1 \in S$. There exists $x_2 \in S$ such that $x_2 > x_1$. If $x_1 < \cdots < x_2$ are chosen, then since x_n is not a maximal element, we can choose $x_{n+1} > x_n$. This constructs an ascending chain that is not stationary.

□

Definition 10.2. A ring A is called **Noetherian** if every ascending chain of ideals in A is stationary. An A-module M is Noetherian if every chain of submodules of M is stationary. In particular, a ring A is Noetherian if it is a Noetherian module over A. A ring A is called **Artinian** if every descending chain of ideals is stationary. An A-module M is Artinian if every descending chain of submodules is stationary.

Example. Let $\mathbb{Z} \supset (n)$ is Noetherian. $(a) \subset (b)$ if and only if b divides a. $(15) \subsetneq (5) \subsetneq (1) = \mathbb{Z}$. But $(2) \supsetneq (4) \supsetneq \cdots \supsetneq (2^n) \supsetneq \dots$ is an infinite descending chain of ideals so $\mathbb{Z}$ is not Artinian. If A is a finite ring, then it is trivially both Noetherian and Artinian.

Proposition 10.3. Let A be a ring and let M be an A-module. Then M is Noetherian if and only if every submodule of M is finitely generated.

Proof. Suppose M is Noetherian, but $N \subset M$ is a submodule that is not finitely generated. Then take $x_1 \in N$. Since $N \neq (x_1)$, the submodule generated by x_1, we can find $x_2 \in N \backslash (x_1)$. This gives $(x_1) \subsetneq (x_1, x_2)$ and so on. This produces an ascending chain which is not stationary, a contradiction. Now suppose that every submodule of M is $f \cdot g$. Consider any ascending chain $M_1 \subset M_2 \subset \dots$. Let $N = \bigcup_{i \geq 1} M_i$. This is a submodule of M. By assumption $N = (x_1, \dots, x_n)$ for some $x_i \in N$. For each x_i there is an M_j in our chain such that $x_i \in M_j$. So there will be some M_l that contains $x_1, \dots, x_n$. Then $N = M_l$. And clearly for any $m \geq 0$ we have $M_l \subset M_{l+m} \subset N = M_l$, so $M_{l+m} = M_l$. So M is Noetherian. □

Remark 10.4. Applying this to the A-module A we see that A is Noetherian if and only if every ideal is finitely generated. Hence every principal ideal domain is Noetherian.

Example. $\mathbb{Z}$, $k[x]$, $k[x_1, \dots, x_n]$. Hilbert's basis theorem says that if R is Noetherian, then $R[x]$ is also Noetherian.

Proposition 10.5. Let A be a ring. Let M be an A-module and $N \subset M$ a submodule. Then M is Noetherian if and only if N and M/N are both Noetherian A-modules.

Proof. Suppose M is Noetherian. Then clearly N is Noetherian. M/N is Noetherian too. Indeed, let L be a submodule of M/N. Let T be the inverse image of L in M. Then we have a surjective homomorphism of A-modules $T \to L$. Since T is finitely generated, so that $T = (x_1, \dots, x_n)$ for some $x_i \in T$. Then the images of $x_1, \dots, x_n$ generate L. Now assume N and M/N are Noetherian. This can also be proved using ascending chains. Take any ascending chain $M_1 \subset M_2 \subset \dots$. Then $N \cap M_1 \subset N \cap M_2 \subset \dots$ is an ascending chain of submodules of N. Let $n_1 \in \mathbb{N}$ be such that for all $i \geq 0$, $N \cap M_{n+i} = N \cap M_{n_1}$. Consider $(M_i + N)/N \subset M/N$. This is just the set of cosets $x + N$, where $x \in M_i$. In fact $(M_i + N)/N \cong M_i / M \cap N$. We obtain an ascending chain $(M_1 + N)/N \subset (M_2 + N)/N \subset \cdots \subset (M_{n_2} + N)/N = (M_{n_1} + N)/N = \dots$. Take $n = \max\{n_1, n_2\}$. It works, that is $M_n = M_{n+1} = \dots$. Indeed, take any $x \in M_{n+i}$ for $i \geq 0$. Then there exists $y \in M_n$ such that $x + N = y + N$. Thus $x - y \in N \cap M_{n+i}$. But this is $N \cap M_n$. So there exists $z \in N \cap M_n$ such that $x - y = z$. Hence $x = y + z \in M_n$. □

Lecture 13
Friday
02/11/18

Lecture 13 is a problem class.
(Exercise: do the same in the Artinian case)

Lecture 14
Monday
05/11/18

Corollary 10.6. Let A be a Noetherian or Artinian ring. Let M be a finitely generated A-module. Then M is Noetherian or Artinian.

Proof. Let $M = (m_1, \dots, m_n)$ for $m_i \in M$, so

$$M = \{a_1 m_1 + \cdots + a_n m_n \mid a_i \in A\}.$$

Let $A^{\oplus n} = \{(a_1, \dots, a_n) \mid a_i \in A\}$ be a free A-module of rank n. There is a homomorphism of A-modules $A^{\oplus n} \to M$ sending $(a_1, \dots, a_n)$ to $a_1 m_1 + \cdots + a_n m_n$. It is surjective. By Proposition 10.5 it is enough to show that $A^{\oplus n}$ is Noetherian. Prove by induction in n. Clearly, A is Noetherian. $A^{\oplus(n-1)} \subset A^{\oplus n}$. The quotient $A^{\oplus n}/A^{\oplus(n-1)} \cong A$ by $(a_1, \dots, a_n) \mapsto a_n$. By Proposition 10.5 $A^{\oplus(n-1)}$ and A Noetherian implies that $A^{\oplus n}$ is Noetherian too. □

Corollary 10.7. Let A be a ring and let M be an A-module. Suppose that we have $0 = M_0 \subset \dots M_n = M$ are A-submodules of M. Then M is Noetherian or Artinian if and only if each quotient M_{i+1}/M_i is Noetherian or Artinian.

Proof. Use Proposition 10.5. □

Lemma 10.8. Let A be a Noetherian ring. Let $S \subset A$ be a multiplicative set. Then $S^{-1}A$ is Noetherian.

Proof. Consider a non-empty set Σ of ideals of $S^{-1}A$. There is a canonical homomorphism of rings $f : A \to S^{-1}A$ by $f(a) = a/1$. If I is an ideal of $S^{-1}A$, then $f^{-1}(I)$ is an ideal in A. Then $I = S^{-1}f^{-1}(I)$. Now Σ gives a non-empty set of ideals of A under $I \to f^{-1}(I)$. Let J be a maximal element of this set. Then $S^{-1}J$ is a maximal element of Σ. Hence $S^{-1}A$ is Noetherian. □

11 Primary decomposition

Definition 11.1. An ideal Q in a ring R not equal to R, that is a proper ideal, is called **primary** if all $x, y \in R$ such that $xy \in Q$ we have $x \in Q$ or $y^n \in Q$ for some n. Equivalently, $I \subsetneq R$ is called primary if every zero-divisor in R/I is nilpotent.

Example. Let p be a prime number. Then (p^m) for $m \geq 1$ is a primary ideal in $\mathbb{Z}$. $ab \in (p^m)$ if and only if $p^m \mid ab$. Consider a. If $p \nmid a$, then $p^m \mid b$, hence $b \in (p^m)$. Otherwise $p \mid a$, then $p^m \mid a^m$, so $a^m \in (p^m)$.

Lecture 15 is a test.

Lecture 15 Tuesday 06/11/18

Example. $(f(x)^n) \subset k[x]$ for $f(x)$ irreducible is primary.

Lecture 16 Friday 09/11/18

Example. Let $R = k[x, y]$ and $I = \left(x^3, y^5, xy\right)$. Claim that I is primary. Take any $f(x, y) = f_0 + xg(x, y) + yh(x, y)$. If $f_0 = 0$, since x and y are nilpotent, when considered as elements of R/I, $f(x, y)$ is nilpotent. If $f_0 \neq 0$, $f(x, y)$ is a sum of a unit and a nilpotent, hence a unit. In particular, any zero-divisor in R/I is nilpotent.

Example. Let $R = k[x, y]$ and $I = (xy)$. $xy \in I$, but $x^n \notin I$ for all $n \geq 0$. Hence I is not a primary ideal.

Example. Even simpler, $(6) \subset \mathbb{Z}$ is not a primary ideal.

Proposition 11.2. Let $I \subset R$ be an ideal. If the radical $r(I)$ is a maximal ideal, then I is primary. In particular, any power of a maximal ideal is primary.

Proof. Consider R/I. $r(I)/I$ is the nilradical of the ring R/I, which is the intersection of all prime ideals of R/I. We are given that $r(I)$ is a maximal ideal, so $r(I)/I$ is a maximal ideal of R/I. Hence $r(I)/I$ is the unique prime ideal of R/I. If $x \notin r(I)/I$, then $x \in (R/I)^*$. Indeed, every non-unit is contained in a maximal ideal by Corollary 4.10, but there is only one maximal ideal and x is not in it. If $x \in r(I)/I$, then x is nilpotent. So all zero-divisor of R/I are nilpotent, hence I is a primary ideal of R. Now let $M \subset R$ be a maximal ideal. Then M^n is primary, since $r(M^n) = M$. Indeed, for any $x \in M$ $x^n \in M^n$, so $M \subset r(M^n)$. Since M is maximal we must have $M = r(M^n)$. □

Example. In the example $I = \left(x^3, xy, y^5\right) \supset (x, y)^5$.

Proposition 11.3. Let $I \subset R$ be a primary ideal. Then the radical $r(I)$ is a prime ideal of R. It is the smallest prime ideal of R containing I.

Proof. Let $x, y \in R$ for $xy \in r(I)$. Then there exists n such that $x^n y^n \in I$. If $x^n \in I$, then $x \in r(I)$. Suppose $x^n \notin I$. Since I is primary, there exists m such that $(y^n)^m \in I$. Then $y \in r(I)$. This proves that $r(I)$ is prime. Note that $r(I)$ is the intersection of all prime ideals containing I. Hence if $r(I)$ is a prime ideal, it is the smallest prime ideal containing I. □

Definition 11.4. Let $P \subset R$ be a prime ideal. An ideal $I \subset R$ is called P**-primary**, if I is a primary ideal such that $r(I) = P$.

Lemma 11.5. Let $I_1, \dots, I_n$ be P-primary ideals in R, where P is a prime ideal. Then $\bigcap_{j=1}^n I_j$ is also a P-primary ideal.

Proof. Assume $n = 2$. The general case by induction. $r(I_1) = r(I_2) = P$ and $r(I_1 \cap I_2) = r(I_1) \cap r(I_2)$. Hence $r(I_1 \cap I_2) = P$. Let us show that $I_1 \cap I_2$ is primary. Take $x, y \in R$ such that $xy \in I_1 \cap I_2 \subset I_1$. If $x \notin I_1 \cap I_2$, then, say, $x \in I_1$. We know that $y^n \in I_1$ for some $n \geq 0$. Hence $y \in r(I_1) = P = r(I_1 \cap I_2)$, so that $y^m \in I_1 \cap I_2$. □

Warning that it is not true in general that if $r(I)$ is prime, then I is primary. True if $r(I)$ is maximal though.

Lecture 17
Monday
12/11/18

Definition 11.6. Let R be a ring, and let $I \subsetneq R$ be an ideal. Call I **irreducible** if for any two ideals J and K in R such that $I = J \cap K$ we have either $J = I$ or $K = I$. I is **reducible**, that is not irreducible, if $I = J_1 \cap J_2$, where $I \subsetneq J_i$ for $i = 1, 2$.

Note. $x \in R$, which is not a unit, is irreducible if x is not a product of two non-units.

Proposition 11.7.

1. Any prime ideal is irreducible.
2. If R is Noetherian, then any irreducible ideal is primary.

Proof.

1. Let P be a prime ideal. Suppose $P = I \cap J$. Note that $IJ \subset I \cap J$. By the prime avoidance lemma 4.11 $I \cap J \subset P$ implies that $I \subset P$ or $J \subset P$. Say, $I \subset P = I \cap J \subset I$. Thus $I = P$.
2. Let $I \subset R$ be an irreducible ideal. Go over to R/I. An equivalent statement is given that the zero ideal in a ring is irreducible, that is (0) is not the intersection of two non-zero ideals, show that $xy = 0$, $x \neq 0$ implies $y^n = 0$ for some n. So let $A = R/I$. We work in A, so $x, y \in A$. R Noetherian gives A is Noetherian. Consider $\{\alpha \in A \mid \alpha y = 0\} = Ann(y) \subset Ann(y^2) \subset \dots$. These are ideals in A. There is an $n > 0$ such that $Ann(y^n) = Ann(y^{n+1})$. We want to show that some $y^k = 0$, that is $(y^k) = (0)$. Claim that can take $k = n$. Let us prove that $0 = (x) \cap (y^n) \neq (0) \cap (y^n)$. By the irreducibility of the zero ideal, this imply $(y^n) = 0$. Suppose that there exists $a \neq 0$, $(a) \in (x) \cap (y^n)$. Then $a = rx$ for some $r \in A$. Then $ay = rxy = 0$. But $a \in (y^n)$, so $a = by^n$ for some $b \in A$. We obtain $by^{n+1} = 0$. In other words, $b \in Ann(y^{n+1}) = Ann(y^n)$ so that $by^n = 0$ so $a = 0$. We proved that $y^n = 0$. Therefore, $I \subset R$ is a primary ideal.

□

Let R be a ring and let $I \subsetneq R$ be an ideal. A **primary decomposition** of I is an expression of I as an intersection of finitely many primary ideals.

Theorem 11.8 (Noether)**.** Any proper ideal in a Noetherian ring has a primary decomposition.

Proof. Let $I \subsetneq R$ be an ideal. We want to prove that I is an intersection of finitely many irreducible ideals using Proposition 11.7. Suppose that this is not true. Look at all the ideals of R that cannot be written as intersections of finitely many irreducible ideals. Since R is Noetherian, this set has a maximal element, say J. By construction, J is not an irreducible ideal of R. Hence J is reducible, so $J = J_1 \cap J_2$, where $J \subsetneq J_1$ and $J \subsetneq J_2$. As J is a maximal element of our set of ideals, J_1 and J_2 are not in this set. Therefore, J_1 and J_2 each can be written as an intersection of finitely many irreducible ideals. Then $J = J_1 \cap J_2$ is also an intersection of finitely many irreducible ideals. This is a contradiction. Thus our set is empty, and so theorem is proved. □

Recall that if I and J are ideals, then $(I : J) = \{r \in R \mid rJ \subset I\}$.

Lemma 11.9. Let R be a ring with a prime ideal P. Let $I \subset R$ be a P-primary ideal, that is $P = r(I)$. Let $x \in R$. Then

1. $x \in I$, then $(I : (x)) = R$.
2. $x \notin I$, then $(I : (x))$ is a P-primary ideal.
3. $x \notin P$, then $(I : (x)) = I$.

Lecture 18
Tuesday
13/11/18

Proof.

1. Obvious. $x \in I$ gives $1 \cdot x \in I$ so $1 \in (I : (x))$.
2. We want to prove the following.
   (a) $r((I : (x))) = P$. Take $y \in (I : (x))$. Then $yx \in I$. We know that I is primary and $x \notin I$. Hence $y^n \in I$ for some $n \geq 1$. Therefore, $y \in r(I) = P$. We proved that $I \subset (I : (x)) \subset P$. This implies $P = r(I) \subset r((I : (x))) \subset r(P) = P$. This shows that $r((I : (x))) = P$. So 1 is proved.

   (b) $(I : (x))$ is primary. We need to show that if $yz \in (I : (x))$, so $y(xz) = xyz \in I$, and $y \notin r((I : (x)))$, so $y^n \notin (I : (x))$ for all n gives $y^n x \notin I$, then we must show $z \in (I : (x))$. But I is primary and $y^n \not I$ for all n, by definition of primary ideals we must have $xz \in I$. Hence $z \in (I : (x))$. So 2 is proved.

   Hence 2 is proved.
3. Let $y \in (I : (x))$. Then $xy \in I$. $x \notin P = r(I)$ hence no power of x is in I. Hence y must be in I.

□

We know that any ideal of a Noetherian ring has a primary decomposition $I = I_1 \cap \dots \cap I_n$, where each $I_i \subset R$ is primary. Let us call this decomposition **minimal** if $r(I_i)$ are distinct prime ideals for $i = 1, \dots, n$. Indeed, this can be arranged with Lemma 11.5 because $\bigcap_{s=1}^{n}$, where each J_s is a P-primary ideal, is again a P-primary ideal and we have $I_j \not\supset \bigcap_{l \neq j} I_l$, which can clearly be arranged by removing redundant ideals.

Theorem 11.10 (First uniqueness theorem)**.** Let $I = \bigcap_{j=i}^{m} I_j$ be a minimal primary decomposition. Then the prime ideals $r(I_1), \dots, r(I_n)$ are uniquely determined by I, so they do not depend on the choice of a primary decomposition.

Proof. Consider $(I : (x))$ for $x \in R$. Look at $r((I : (x)))$ and consider the prime ideals of R that can be written as $r((I : (x)))$. Claim that such prime ideals are precisely $r(I_1), \dots, r(I_n)$. $(I : (x)) = \left(\bigcap_{j=1}^{n} I_j : (x)\right) = \bigcap_{j=1}^{n} (I_j : (x))$. Hence $r((I : (x))) = \bigcap_{j=1}^{n} r((I : (x)))$. Lemma 11.9 gives

1. $x \in I_j$ gives $(I_j : (x)) = R$, so $r((I_j : (x))) = R$, and
2. $x \notin I_j$ gives $(I_j : (x))$ is P_j-primary, so $r((I_j : (x))) = P_j$.

Therefore, $r((I : (x))) = \bigcap_{x \notin I_j} P_j$. If $r((I : (x)))$ is prime, we know by the prime avoidance lemma 4.11 that $r((I : (x))) = P_j$ for some P_j. Conversely, for each j, by minimality of our primary decomposition, there exists $x_j \notin I_j$, but $x_j \in \bigcap_{l \neq j} I_l$. Then $r((I_l : (x_j))) = R$ for $l \neq j$, so $r((I_j : (x_j))) = P_j$. Hence $r((I : (x_j))) = P_j$. □

Lecture 19
Friday
16/11/18

Lecture 19 is a problem class.

Lecture 20
Monday
19/11/18

12 Artinian rings and modules

Definition 12.1. Let A be a ring and let M be a non-zero A-module. M is **simple** if and only if the only submodules of M are 0 and M. Any A-module M has a **composition series** if it contains submodules $M = M_0 \supset \cdots \supset M_n = 0$ such that the quotients M_i/M_{i+1} are simple A-modules for $i = 0, \dots, n-1$. Any such collection of submodules is called a composition series.

Proposition 12.2. For any A-module M the following are equivalent.

1. M is both Noetherian and Artinian.
2. M has a composition series.

Proof.

$1 \implies 2$ Since M is Noetherian, M contains a maximal submodule. Any set of submodules of M has a maximal element. Call it M_1. Call $M = M_0$. Then M_1/M_0 is simple by the choice of M_1. Continue, and find $M_2 \subset M_1$ maximal submodule. We construct a decreasing chain of submodules $M = M_0 \supsetneq \cdots \supsetneq M_0 = 0$ because M is Artinian. So we obtain a composition series.

$2 \implies 1$ Assume M has a composition series $M = M_0 \supsetneq M_n = 0$. Any simple module is Noetherian and Artinian. Corollary 10.7 says that if $L \subset N$ are A-modules such that L and N/L are Artinian, then N is also Artinian. The same for Noetherian. Apply this to M_{n-2}/M_{n-1}, where M_{n-1} is simple. We know that M_{n-2}/M_{n-1} is also simple. Hence M_{n-2} is Noetherian and Artinian. Then apply this to $M_{n-3} \supset M_{n-2}$.

□

Proposition 12.3. If M has a composition series of length n, then any other composition series of M will have length n.

Proof. Let $l(M)$ denote the smallest length of a composition series of M. If M has no composition series, set $l(M) = \infty$.

1. Let $N \subsetneq M$ be a proper submodule. Then $l(N) < l(M)$. Let $n = l(M)$ and suppose that $M = M_0 \supsetneq \cdots \supsetneq M_n = 0$ is a composition series. Consider $N_i = N \cap M_i$. $N = N_0 \supset \cdots \supset N_n = 0$. $N_{i+1} = N_i \cap M_{i+1}$. $N_i/N_{i+1} = N_i/(N_i \cap M_{i+1}) = (N_i + M_{i+1})/M_{i+1} \subset M_i/M_{i+1}$, which is a simple module. Hence $N_i/N_{i+1} = 0$ or $N_i/N_{i+1} = M_i/M_{i+1}$. So remove repeated terms in $N = N_0 \supset \dots N_n = 0$. We obtain a composition series for N. This proves that $l(N) \leq n = l(M)$. Assume that $N \neq M$. Let us show that $l(N) \neq l(M)$. Let us prove that if $l(N) = l(M)$, then $N = M$. We started with a composition series of length $n = l(M)$. If $l(N) = l(M)$, then there were no repetitions in $N = N_0 \supsetneq \cdots \supsetneq N_n = 0$. All inclusions here are strict. $N_n = M_n = 0$. $N_{n-1} = N \cap M_{n-1} \neq 0$ is a submodule of M_{n-1}, which is simple. Thus $N_{n-1} = M_{n-1}$. Then $N_{n-2} = N \cap M_{n-2} \neq N_{n-1} = N \cap M_{n-1}$. Therefore, $0 \neq N_{n-2}/N_{n-1} \subset M_{n-2}/M_{n-1}$ is an equality. Hence $N_{n-2} = M_{n-2}$. Continue like this. The final shows that $N_0 = M_0$, that is $N = M$.
2. Let $M = M_0 \supsetneq \cdots \supsetneq M_k = 0$ be a composition series. We have $k \geq l(M)$. 1 gives that $l(M) = l(M_0) > \cdots > l(M_k) = 0$. Hence $l(M_{k-1}) \geq 1, \dots, l(M) \geq k$. Hence $k = f(M)$.

□

Definition 12.4. If $l(M) < \infty$, then $l(M)$ is called the **length** of M.

Proposition 12.5. Let M be an A-module and let N be a submodule of M. Then N and M/N have finite length, then M has finite length and $l(M) = l(N) + l(M/N)$.

Proof. Take a composition series of M/N and pull it back to M via the map $M \to M/N$. $M = M_0 \supsetneq \cdots \supsetneq N \supsetneq \dots$. Now take a composition series in N and combine it with the M_i's. □

Lecture 21
Tuesday
20/11/18

Example.

1. Any field is an Artinian ring.
2. A finite dimensional vector space over a field k is an Artinian k-module.
3. Finite rings and finite modules are Artinian.
4. An example of a non-Artinian ring is $k[t]$.

Lemma 12.6. An Artinian integral domain is a field.

Proof. Let $x \in A$, $x \neq 0$. Consider $(x) \supset \left(x^2\right) \supset \dots$. This is a descending chain of ideals, hence is stationary, that is there exists n such that $(x^n) = \left(x^{n+k}\right)$ for all $k \geq 0$. In particular, $(x^n) = \left(x^{n+1}\right)$, hence $x^n = x^{n+1}y$ for some $y \in A$. A is an integral domain, hence $x\left(x^{n-1} - x^n y\right) = 0$ for $x \neq 0$ implies $x^{n-1} = x^n y$. Continue and obtain $1 = xy$. Hence $x \in A^*$, so A is a field. □

Corollary 12.7. In an Artinian ring any prime ideal is maximal.

Proof. Let $P \subset A$ be a prime ideal. Then A/P is also an Artinian ring. A/P is an integral domain, hence a field by Lemma 12.6. So P is maximal. □

Corollary 12.8. In an Artinian ring the nilradical coincides with the Jacobson radical.

Lemma 12.9. Let A be an Artinian ring. Then A has only finitely many maximal ideals.

Proof. For contradiction suppose we have countably many maximal ideals $I_1, I_2, \dots$. $I_1 \supset \dots \supset I_1 \cap \dots \cap I_n = I_1 \cap \dots \cap I_{n+1} = \dots$. This implies that $I_1 \cap \dots \cap I_n \subset I_{n+1}$. Since I_{n+1} is a prime ideal, there is a $j \in \{1, \dots, n\}$ such that $I_j \subset I_{n+1}$ by the prime avoidance lemma. But I_j is a maximal ideal, hence $I_j = I_{n+1}$, but we assumed that all the I_k's are pairwise different. Contradiction. □

Lemma 12.10. The nilradical of an Artinian ring is nilpotent. In other words, there exist $n \in \mathbb{Z}_{\geq 1}$ such that $N(A)^n = 0$.

Proof. $N(A) \supset \dots \supset N(A)^n = N(A)^{n+1} = \dots$. Such an n exists, because A is Artinian. We want to show that $N(A)^n = 0$. Let C be the set of all ideals $I \subset A$ such that $I \cdot N(A)^n \neq 0$. For contradiction we assume $N(A)^n \neq 0$. Then C is not empty, because C contains $N(A)$. Since A is Artinian, any non-empty set of ideals of A has a minimal element, say I. So we have $I \cdot N(A)^n \neq 0$. So there is an $x \in I$ such that $x \cdot N(A)^n \neq 0$. But then $(x) \cdot N(A)^n \neq 0$, so (x) is in C. Since I is minimal and $(x) \subset I$, we must have $(x) = I$. Let us observe that $0 \neq (x) \cdot N(A)^n = (x) \cdot N(A)^n \cdot N(A)^n$. This shows that the ideal $(x) \cdot N(A)^n$ is in C, but $(x) \cdot N(A)^n \subset (x) = I$, which is minimal in C. Therefore, $(x) \cdot N(A)^n = (x) \ni x$. This implies that $x = xy$, where $y \in N(A)^n \subset N(A)$. In particular, y is nilpotent, that is $y^m = 0$ for some m. $x = \dots = xy^m = 0$, so $x = 0$. Hence $I = 0$. This is a contradiction as $I \cdot N(A)^n \neq 0$. Thus $N(A)^n = 0$. □

Lecture 22
Friday
23/11/18

Lemma 12.11. Let k be a field and let V be a vector space over k. The following are equivalent.

1. V is finite dimensional.
2. V is a Noetherian k-module.
3. V is an Artinian k-module.

Proof.

$1 \implies 2$ Trivial.

$2 \implies 3$ Use the fact that V has a finite generating set.

$3 \implies 1$ Trivial.

□

Lemma 12.12. Let A be a ring. Suppose we have maximal ideals $I_1, \dots, I_n$, possibly with repetitions. If $I_1 \dots I_n = 0$, then A is Artinian if and only if A is Noetherian.

Proof. Let $M_1 = I_1 \supset \dots \supset M_n = I_1 \dots I_n = 0$ and A be Noetherian, hence all the M_i's are Noetherian too. Hence M_i/M_{i+1} are Noetherian A-modules for all i. Note that $M_i \cdot I_{i+1} = M_{i+1}$, hence $I_{i+1} \subset A$ acts as zero on M_i/M_{i+1}. Therefore, M_i/M_{i+1} is naturally a module for the quotient ring A/I_{i+1}. Since I_{i+1} is a maximal ideal, the ring A/I_{i+1} is a field, and M_i/M_{i+1} is a vector space over A/I_{i+1}. Since M_i/M_{i+1} is a Noetherian A-module, this is a finite dimensional vector space over A/I_{i+1}. By Lemma 12.11, M_i/M_{i+1} is also an Artinian A/I_{i+1}-module. Hence, M_i/M_{i+1} is an Artinian A-module. In particular, $M_{n-1}/M_n = M_{n-1}$ is Artinian, but M_{n-2}/M_{n-1} is also Artinian. Hence M_{n-2} is Artinian. Continue like this. Finally, prove that A is Artinian. (Exercise: converse) □

Definition 12.13. Let A be a ring. The **Krull dimension** of A is the supremum of all $n \in \mathbb{Z}_{>0}$ such that A has a chain of proper prime ideals $I_0 \subsetneq \dots \subsetneq I_n$. $\dim(A)$ is a positive integer or infinity.

Example.

1. Any field has dimension zero.

2. Any principal ideal domain which is not a field has dimension one, such as $\mathbb{Z}$ or $k[x]$, where k is a field. $(0) \subsetneq P$ for P a prime ideal. In a PID all non-zero prime ideals are maximal. An integral domain but not a field has $\dim(A) = 1$ if and only if all prime ideals are maximal.

3. $k[x_1, \dots, x_n]$ has this chain $(0) \subsetneq \dots \subsetneq (x_1, \dots, x_n)$. $\dim(k[x_1, \dots, x_n]) \geq n$. In fact dimension is n.

Theorem 12.14. A ring is Artinian if and only if it is Noetherian and has dimension zero.

Proof. Let us show that A Artinian gives A Noetherian and $\dim(A) = 0$. Corollary 12.7 says that every prime ideal is maximal, hence $\dim(A) = 0$. Lemma 12.9 says that A has only finitely many maximal ideals, call them $I_1, \dots, I_n$. $I_1 \dots I_n \subset I_1 \cap \dots \cap I_n = J(A) = N(A)$ by Corollary 12.8. But Lemma 12.10 says $N(A)^m = 0$ for some $m \geq 1$. We conclude that $I_1^m \dots I_n^m = 0$. We can apply Lemma 12.12 and so prove that A is Noetherian. For the other implication, let us first prove that if A is Noetherian, then $N(A)^m = 0$, for some $m \geq 1$. Indeed, $N(A)$ is finitely generated, so $N(A) = (m_1, \dots, m_n)$. For each $i = 1, \dots, m$, there is a $a_i \geq 1$ such that $m_i^{a_i} = 0$. Take $a = a_1 + \dots + a_n$. Then $(m_1, \dots, m_n)^a = 0$. So $N(A)$ is a nilpotent ideal. As a consequence, we obtain that any ideal in a Noetherian ring contains some power of its radical $I \subset A$. There exists n such that $r(I)^n \subset I$ by applying the fact that the nilradical is nilpotent to A/I and $N(A/I) = r(I)/I$, so $N(A/I)^n = 0$ gives $r(I)^n \subset I$. Now (0) in A has a primary decomposition, since A is Noetherian. Write $(0) = J_1 \cap \dots \cap J_n$, where J_i are primary ideals. We know that $P = r(J_i)$ is a prime ideal of A by Proposition 11.3. Since $\dim(A) = 0$, each P_i is actually a maximal ideal. For each $i = 1, \dots, n$ there is a $k_i \geq 1$ such that $P_i^{k_i} \subset J_i$, since $P_i = r(J_i)$. Hence $(0) = J_1 \cap \dots \cap J_n \supset J_1 \cdot \dots \cdot J_n \supset P_1^{k_1} \dots P_n^{k_n}$, hence $P_1^{k_1} \dots P_n^{k_n} = 0$. By Lemma 12.12 we conclude that A is Artinian. □

Lecture 23
Monday
26/11/18

Theorem 12.15 (Structure theorem)**.** Any Artinian ring is isomorphic to a product of local Artinian rings.

Recall that a ring is local if it has only one maximal ideal.

Example. Let $R = k[x]$. Let $f(x)$ be a non-zero polynomial and $A = R/(f)$. $\dim_k(A) < \infty$ so A is Artinian. $f(x) = \prod_{i=1}^n f_i(x)^{m_i}$, where $f_i(x)$ are pairwise different irreducible polynomials. The ideals of A correspond to factors of $f(x)$. Maximal ideals correspond to $f_i(x)$. Chinese remainder theorem gives $A = R/(f) \cong \prod_{i=1}^n R/(f_i(x)^{m_i})$.

Definition 12.16. The ideal $I, J \subset R$ are **coprime** if $I + J = R$.

Suppose $I_1, \dots, I_n$ are ideals of R. Consider the natural homomorphism $\phi : R \to \prod_{i=1}^n R/I_i$ by $\phi(r) = (r + I_1, \dots, r + I_n)$.

Lemma 12.17.

1. If $I_j + I_k = R$ for any $j \neq k$, then $\prod_{j=1}^n = \bigcap_{j=1}^n I_j$.

2. ϕ is surjective if and only if $I_j + I_k = R$ for any pair $j \neq k$.

3. ϕ is injective if and only if $\bigcap_{j=1}^{n} I_j = 0$.

Proof. See problem sheet 4. □

Proof of Theorem 12.15. Recall that A is an Artinian ring. By Lemma 12.9 A has only finitely many maximal ideals, say $I_1, \dots, I_n$, all pairwise different. $I_1 \dots I_n \subset I_1 \cap \dots \cap I_n = J(A) = N(A)$ by Corollary 12.8. By Lemma 12.10 $N(A)^m = 0$. Hence $(I_1 \dots I_n)^m = 0$. $I_j \subsetneq I_j + I_k = R$ for $j \neq k$, where I_j is maximal. By Lemma 12.17 $\cap_{j=1}^{n} I_j = \prod_{j=1}^{n} I_j$. Claim that if $j \neq k$, then $I_j^a + I_k^a = R$ for any $a \geq 1$. Indeed, $I_j + I_k = R$ so there exist $x \in I_j$, $y \in I_K$ such that $1 = x + y$. Hence $1^{2a} = (x+y)^{2a}$, which is a sum of a multiple of x^a and a multiple of y^a, which is in $I_j^a + I_k^a$. By Lemma 12.17 we have $\cap_{j=1}^{n} I_j^a = \prod_{j=1}^{n} I_k^a$. So ϕ gives an isomorphism $A / \prod_{j=1}^{n} I_j^a \cong \prod_{j=1}^{n} A / I_j^a$. It is enough to show that each A / I_j^a is a local ring. Take a large enough, say $a = m$. Then $\prod_{j=1}^{n} I_j^a = 0$. Note that $N\left(A / I_j^a\right) = I_j / I_j^a$. Indeed, for all $x \in I_j$ we have $x^a \in I_j^a$. Since I_j / I_j^a is a maximal ideal of A / I_j^a, this is $N\left(A / I_j^a\right)$. This is the intersection of all prime ideals of A_j^a. Thus all of them coincide with I_j / I_j^a, so are maximal. Hence, I_j / I_j^a is a unique maximal ideal of A / I_j^a. □

Lecture 24 is a test.
Lecture 25 is a problem class.

Lecture 24
Tuesday
27/11/18

Lecture 25
Friday
30/11/18

Lecture 26
Monday
03/12/18

13 Integral closure

Theorem 13.1. Let R be a ring. Let $A \subset R$ be a subring. Let $x \in R$. The following are equivalent.

1. There are $a_0, \dots, a_{n-1} \in A$ such that $x^n + \dots + a_n = 0$

2. The A-module $A[x]$ is finitely generated. Here $A[x] \subset R$ are all polynomial expressions in x with coefficients in A.

3. There is a subring $B \subset R$ containing A and x such that B is a finitely generated A-module.

Proof.

$1 \implies 2$ $x^n = -\left(a_{n-1} x^{n-1} + \dots + a_0\right)$ so x^n belongs to the A-module generated by $1, \dots, x^{n-1}$. $x^{n+1} = -x\left(a_{n-1} x^{n-1} + \dots + a_0\right) = -a_{n-1} x^n + \dots$. Clearly, $x^k \in A \cdot 1 + \dots + A \cdot x^{n-1}$. So $A[x]$ is a finitely generated A-module.

$2 \implies 3$ Trivial. Indeed, take $B = A[x]$.

$3 \implies 1$ Assume such a B exists. There exists $y_1, \dots, y_n$ in B which generate B as an A-module. Now $x \in B$ and B is a ring, so $x y_1, \dots, x y_n \in B$. Hence $x y_i = \sum_{j=1}^{n} a_{ij} y_j$ for $i = 1, \dots, n$, where $a_{ij} \in A$. Let M be the matrix (a_{ij}), and let $d = \det(x \cdot I - M) \in B$. By the determinant trick, we have $d y_i = 0$ for $i = 1, \dots, n$. Therefore, since $B = (y_1, \dots, y_n)$, we have $dB = 0$. But B contains one. Hence $d = 0$. If $p(t)$ is the characteristic polynomial of M, that is $p(t) = \det(t \cdot I - M) \in A[t]$ with leading coefficient one, then $p(x) = 0$. This proves 1.

□

Definition 13.2. Let $A \subset R$ be rings. An element $x \in B$ is **integral** over A if the equivalent conditions of Theorem 13.1 hold. A monic polynomial $p(t) \in A[t]$ such that $p(x) = 0$ is called the **equation of integral dependence** of x over A. R is called integral over A if every element in R is integral over A.

Example.

1. Let $R = k[x] \supset k\left[x^2\right] = A$. $k[x]$ is integral over $k\left[x^2\right]$. $t^2 - x^2 = 0$, hence x is integral. (Exercise: check that all elements are integral, without using Theorem 13.1)

2. Let $\mathbb{Z}\left[\left(-1+\sqrt{-3}\right)/2\right]$ and $\zeta = \left(-1+\sqrt{-3}\right)/2$. $\zeta^2 + \zeta + 1 = 0$. $\mathbb{Z}\left[\left(-1+\sqrt{-3}\right)/2\right]$ is integral over $\mathbb{Z}$.

3. But $\mathbb{Z}[1/5]$ is not an integral extension of $\mathbb{Z}$. $1/5$ is not integral over $\mathbb{Z}$.

Lemma 13.3.

1. If $A \subset B \subset C$ are rings such that 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 of B integral over A is a subring B, called the **integral closure** of A in B and denoted by $\widetilde{A}$. Then $\widetilde{A}$ is integrally closed in B, that is every element of B which is integrally closed over $\widetilde{A}$ already belongs to $\widetilde{A}$.

Proof.

1. Assume that $c_1, \dots, c_n \in C$ generate C as a B-module. Assume that $b_1, \dots, b_m \in B$ generate B as an A-module. Then $b_i c_j$ for all i and j generate C as an A-module.

2. By Theorem 13.1 $A[x_1]$ is a finitely generated A-module. But 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. By 1 $A[x_1, x_2]$ is a finitely generated A-module. Then continue by repeating this $n-1$ times.

3. We must show that any $c \in C$ is integral over A. Since c is integral over B, there are $b_0, \dots, b_{n-1} \in B$ such that $c^n + \dots + b_0 = 0$. But B is integral over A, hence each b_i is integral over A. Then by 2 $A[b_0, \dots, b_{n-1}]$ is a finitely generated A-module. This implies that $A[b_0, \dots, b_{n-1}, c]$ is a finitely generated A-module, using 1. Theorem 13.1 says that x is integral over A.

4. Must show that if x, y are integral elements of B, then so is $xy, x+y, -x$. Consider $A[x,y]$. By 2 this is a finitely generated A-module. This is a ring which is a finitely generated A-module, hence by Theorem 13.1 every element of this ring is integral over A. In particular, $x+y, -x, xy$ are integral. Let us show that $\widetilde{A}$ is integrally closed in B, that is for all $x \in B$ that is integral over $\widetilde{A}$ belongs to $\widetilde{A}$. Indeed, $A \subset \widetilde{A} \subset \widetilde{\widetilde{A}}$ are rings, and $\widetilde{A}$ is integral over A, $\widetilde{\widetilde{A}}$ is integral over $\widetilde{A}$. Hence, by 3 $\widetilde{\widetilde{A}}$ is also integral over A. Therefore, $\widetilde{\widetilde{A}} = \widetilde{A}$.

□

Lecture 27
Tuesday
04/12/18

Definition 13.4. Let A be an integral domain, and let B be the field of fractions of A. In this case $\widetilde{A}$ is called the **normalisation** of A. If $\widetilde{A} = A$, then A is called a **normal** ring.

Example.

1. Any UFD is normal (Exercise), for example $\mathbb{Z}$ is normal. $k[x_1, \dots, x_n]$ is a UFD, hence a normal ring.

2. Number theory examples. Let $\zeta = e^{2\pi i/n}$ for $n \geq 2$. $\mathbb{Q}(\zeta)$ is a cyclotomic field. $\mathbb{Z} \subset \mathbb{Q}(\zeta)$ and $\zeta^n - 1 = 0$, hence ζ is integral over $\mathbb{Z}$. Assume F is a field extension of $\mathbb{Q}$. Define the ring of integers of F as the integral closure of $\mathbb{Z}$ in F. A fact is that the ring of integers of $\mathbb{Q}(\zeta)$ is $\mathbb{Z}[\zeta]$. Another class of interesting number fields is $\mathbb{Q}(\sqrt{a})$ for $a \in \mathbb{Z}$ square-free. What is the integral closure of $\mathbb{Z}$ in $\mathbb{Q}(\sqrt{a})$? Is it $\mathbb{Z}[\sqrt{a}]$? $\sqrt{a}^2 - a = 0$. Yes, if $a \equiv 2 \mod 4$ or $a \equiv 3 \mod 4$. No, if $a \equiv 1 \mod 4$. It is bigger than $\mathbb{Z}[\sqrt{a}]$. $\mathbb{Q}\left(\sqrt{-3}\right) = \mathbb{Q}\left(\left(-1+\sqrt{3}\right)/2\right) = \mathbb{Q}(\zeta_3) \supset \mathbb{Z}[\zeta_3]$, the normalisation of $\mathbb{Z}[\sqrt{a}]$.

3. Normalisation in algebraic geometry. $y^2 = x^3$ has a cusp at $(0,0)$, since $f(x,y) = x^3 - y^2$ and $((\partial f/\partial x)(0,0), (\partial f/\partial x)(0,0)) = (0,0)$, a singular point. Let $A = k[x,y]/\left(y - x^3\right)$. A is the ring of functions on this curve. Is A normal? No. Let $t = y/x$. $t^2 = y^2/x^2$, so $t^2 - x = 0$ hence t is an element of the field of fractions of A, which is not in A, but is integral over A. So $A \subset k[t]$ is in the field of fractions of A. But $k[t]$ is a UFD, hence normal. Thus $k[t]$ is the normalisation of A. The map $t \mapsto \left(t^2, t^3\right)$ is a map from the affine line to our curve. It is a desingularisation of our singular curve.

Lecture 28
Friday
07/12/18

14 Discrete valuation rings

Theorem 14.1. Let R be an integral domain. The following are equivalent.

1. R is a UFD with only one irreducible element, up to multiplication by units.
2. R is a Noetherian local ring whose maximal ideal is principal.

Theorem 14.2. UFD with one irreducible element if and only if a Noetherian local ring whose maximal ideal is principal.

A ring R as in 1 is a ring where every non-unit is at^n for $a \in R^*$ and $n \geq 1$.

Proof.

$1 \implies 2$ Let t be an irreducible element of R. Every non-unit belongs to (t). So $R \setminus (t) \subset R^*$. In fact, the elements of R not divisible by t are units. So $R^* = R \setminus (t)$. Hence (t) is a maximal ideal. Claim that all ideals of R are (t^n) for $n \geq 1$. Let I be an ideal in R. Let n be the smallest integer such that I contains at^n for $a \in R^*$. Then $(t^n) = (at^n) \subset I$. I does not contain bt^m for $b \in R^*$ and $m < n$, hence $I = (t^n)$. Hence R is a PID, so is Noetherian. It is clear that if $n \geq 2$, then $(t^n) \subsetneq (t)$. So (t) is a unique maximal ideal.

$2 \implies 1$ Let t be a generator of the maximal ideal. Then $R \setminus (t) = R^*$. Claim that $\bigcap_{n \geq 1} (t^n) = 0$, where $(t) \supset \left(t^2\right) \supset \dots$. Equivalently, for each non-zero $a \in R$ there is a largest n such that $a \in (t^n)$. If $a \in (t)$, then $a \in R^*$ and $n = 0$ so we are done. Now assume $a \in (t)$. Then $a = a_1 t$, for some $a_1 \in R$. If $a_1 \neq (t)$, that is $a_1 \in R^*$, then $a \notin \left(t^2\right)$. Indeed, otherwise $a = bt^2$, where $b \in R$. $bt^2 = a_1 t$. R is an integral domain, hence $bt = a_1$, which is a contradiction. But if $a_1 \in (t)$, then $(a) \subsetneq (a_1)$. The inclusion is strict, because otherwise there is a unit $u \in R^*$ such that $a_1 = ua = a_1 ut$, hence $ut = 1$ which is absurd, because $t \notin R^*$. This shows that if n does not exist, then there is an infinite strictly increasing chain of ideals in R. This is a contradiction because R is Noetherian.

□

Recall that a set has a total order $x < y$ if for every two elements exactly one of these holds.

$$x < y, \qquad x = y, \qquad x > y.$$

An abelian group G is an **ordered group** if G has a total order compatible with the group structure, that is if $x < y$ then $x + z < y + z$ for any $z \in G$.

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

Definition 14.3. Let K be a field. A **valuation** in K is a surjective homomorphism $v : K^* \to G$, where G is an ordered group, such that $v(x \pm y) \geq \min\{v(x), v(y)\}$. One defines $v(0) = \infty$.

(Exercise: $R = \{x \in K \mid v(x) \geq 0\}$ is a ring, called the valuation ring of v)

(Exercise: if $R^* = \{x \in K \mid v(x) = 0\}$, $R \setminus R^* = \{x \in K \mid v(x) > 0\}$ is the unique maximal ideal of R, thus every valuation ring is a local integral domain)

Definition 14.4. A ring is called a **valuation ring** if its field of fractions K has a valuation $v : K^* \to G$, for some ordered group G, such that $R = \{x \in K \mid v(x) \geq 0\}$. A valuation ring is a **discrete valuation ring** if the ordered group is $\mathbb{Z}$, with the usual order.

Example.

1. $\mathbb{Z}_{(p)} = \{a/b \mid a, b \in \mathbb{Z},\ (p, b) = 1\}$ is a DVR, where $K = \mathbb{Q}$. $v(p^n \cdot (c/d)) = n \in \mathbb{Z}$, where $c, d \in \mathbb{Z}$ and $p \nmid c, d$.
2. The ring of formal power series $k[[t]]$ is a DVR. $v(a_0 + a_1 t + \dots) = n$ such that $a_0 = \dots = a_{n-1} = 0$ and $a_n \neq 0$ for $a_i \in k$. $k((t)) = \left\{\sum_{i \geq m} a_i t^i \mid a_i \in k,\ m \in \mathbb{Z}\right\}$.

3. An example of a valuation ring which is not a DVR. Fix n. Puiseux series is

$$k\left[\left[t^{1/n}\right]\right]=\left\{\sum_{i\geq n}a_it^i \;\middle|\; a_i\in k\right\}.$$

   Let $R=\bigcup_{n\geq 1}k\left[\left[t^{1/n}\right]\right]$. Define v as the highest power of t dividing our element. $v : K^* \to \mathbb{Q}$ by $v\left(at^{c/d}+\dots\right)=c/d$ is not a discrete valuation. Note that the power series with zero constant term form a maximal ideal of R. $t\subsetneq t^{1/2}\subsetneq\dots$. So R is not a Noetherian ring.

Theorem 14.5. A valuation ring is Noetherian if and only if it is a DVR.

Proof. Let R be a Noetherian valuation ring. Then I claim that the maximal ideal I is principal. Any ideal in R is finitely generated, say $I=(x_1,\dots,x_n)$. By induction, it is enough to show that any ideal with two generators, say (x,y), is generated by x or y. Consider $v(x)$ and $v(y)$. $v(x)<v(y)$, $v(x)=v(y)$, or $v(x)>v(y)$. Without loss of generality assume that $v(x)<v(y)$. Then $y\in(x)$ because $R=\{z\in K\mid v(z)\geq 0\}$. In particular, $v(y/x)=v(y)-v(y)\geq 0$ gives $y/x\in R$. □

Lecture 29 Monday 10/12/18

Theorem 14.6.

1. R is a DVR.
2. R is a UFD with only irreducible elements.
3. R is a Noetherian local ring with principal maximal ideal.
4. R is a Noetherian normal local ring of dimension one.

Proof. For contradiction, assume there exist $y\in I\setminus(t)$. It is possible that y has the additional property $Iy\subset(t)$. K is the field of fractions of R. $y/t\in K\setminus R$ and $(y/t)I\subset R$. We have $(y/t)I$ is an ideal in R.

1. $(y/t)I=R$. $1=xy/t$ so $t=xy\in I^2$, a contradiction.
2. $(y/t)I\subset I$. Goal is try to show that $y/t\in R$. Then $y\in(t)$ will be a contradiction. R is Noetherian, hence $I=(x_1,\dots,x_n)$ for some $x_i\in R$.

$$\frac{y}{t}x_1=a_{11}x_1+\dots+a_{1n}+x_n,\dots,\frac{y}{t}x_n=a_{n1}x_1+\dots+a_{nn}+x_n,$$

   for $a_{ij}\in R$. $A^v\cdot A=\det(A)\cdot I$. Let

$$M=\begin{pmatrix}\frac{y}{t}-a_{11} & \dots & -a_{1n}\\ \vdots & \ddots & \vdots\\ -a_{n1} & \dots & \frac{y}{t}-a_{nn}\end{pmatrix}\begin{pmatrix}x_1\\ \vdots\\ x_n\end{pmatrix}=0.$$

   $\det(M)\cdot x_i=0$ for $i=1,\dots,n$. Without loss of generality $x_i\neq 0$. R is an integral domain. We see that $\det(M)=0$. $\det(M)=(y/t)^n+\dots+r_0$, where $r_i\in R$. Therefore, y/t is an element of K which is integral over R. By assumption R is normal, and since $y/t\in K$ is integral over R, we must have $y/t\in R$. Then $y\in(t)$ is a contradiction.

□

Lecture 30 Tuesday 11/12/18

Lecture 30 is a problem class.