Commutative Algebra

B Totaro

Michaelmas 2011

Contents

Notes typed by Zach Norwood. Send any comments/corrections to zn217 at cam.

Lectures

Commutative algebra is about commutative rings: $\mathbb{Z}$, $k[x_1,\dots,x_n]$, etc.

The philosophy of the subject is to try to think of a commutative ring as a ring of functions on some space. 7/10

1 Basics

1.1 Rings & homomorphisms

Definition. A ring R is a set with two binary operations, $+$ and $\cdot$, such that:

(1) $(R,+)$ is an abelian group (with identity 0);

(2) $(R,\cdot)$ is a monoid (with identity (1);

(3) Addition distributes over multiplication [sic?]:

$$x(y+z) = xy + xz \quad \text{and} \quad (y+z)x = yx + zx$$

for all $x, y, z \in R$.

Examples. Though we won't deal with them in this course, here are some examples of noncommutative rings:

(1) For a field k, the ring $M_n k$ of $n \times n$ matrices over k; and

(2) For a field k and a group G, the group ring kG.

In this course, a *ring* means *commutative ring* unless otherwise stated.

Examples. The following are examples of rings:

(1) fields, such as $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, $\mathbb{F}_p = \mathbb{Z}/p$ for p a prime;

(2) the ring $\mathbb{Z}$ of integers;

(3) the ring $k[x_1, x_2, \dots, x_n]$ of polynomials with coefficients in a field k;

(4) for a topological space X the ring $C(X)$ of continuous functions $X \to \mathbb{R}$;

(5) for a smooth manifold X the set $C^\infty(X)$ of smooth functions $X \to R$ forms a ring.

Remark. We don't require $0 \neq 1$ in a ring. If $0 = 1$ in a ring R, then (Exercise!) $R = \{0\} = \{1\}$, and we call this ring the *zero ring*, $R = 0$.

Exercise. $0 \cdot x = 0$ and $(-1) \cdot x = -x$ for every $x \in R$.

Definition. Let R be a ring. Say $x \in R$ is a *unit* (or *is invertible*) if there is an element y in R such that $xy = 1$. If so, then y is unique (Exercise!) and so write $y = x^{-1}$ or $y = \frac{1}{x}$.

An element $x \in R$ is a *zerodivisor* if there is a nonzero element $y \in R$ such that $xy = 0$. An element $x \in R$ is *nilpotent* if there is a $n > 0$ such that $x^n = 0$.

Definition. A ring R is a *field* if $1 \neq 0$ in R and every nonzero element of R is invertible. We say R is an *integral domain* (or just a *domain*) if $1 \neq 0$ in R and the product of any two nonzero elements of R is nonzero. A ring R is *reduced* if the only nilpotent element of R is 0.

Examples.

(1) The zero ring is reduced but is not a domain (or a field).

(2) For a positive integer n, the ring $\mathbb{Z}/n$ is a field iff it's a domain, iff n is prime. Also, $\mathbb{Z}/n$ is reduced iff n is a product of distinct primes. In $\mathbb{Z}/12$, for instance, 6 is nilpotent and nonzero, the elements 2 & 3 are zerodivisors but not nilpotent, and 5 is a unit.

(3) $\mathbb{Z}$ and $k[x_1, \ldots, x_n]$ are domains and not fields if $n \geq 1$. (See Example(s) Sheet 1.)

Definition. A *homomorphism* from a ring A to a ring B is a function $f\colon A \to B$ that preserves $+, \cdot$, and 1; that is,

- $f(x+y) = f(x) + f(y)$ for all $x, y \in R$;
- $f(xy) = f(x)f(y)$ for all $x, y \in R$;
- $f(1_A) = 1_B$.

Can check that a homomorphism f satisfies $f(0) = 0$ and $f(-x) = -f(x)$. (Exercise!)

Example. If A is a subring of B then the inclusion map $A \hookrightarrow B$ is a ring homomorphism. Also, if $f\colon A \to B$ and $g\colon B \to C$ are ring homomorphisms, then so is the composite $g \circ f$. Rings and homomorphisms form a category.

Definition. An *ideal* I in a ring R is an additive subgroup such that for any $x \in I$ and $y \in R$, $xy \in I$.

Remark. The kernel of any ring homomorphism is an ideal.

Examples.

(1) The only ideals in a field k are 0 and k.

(2) Any ideal $I \subseteq R$ that contains 1 must be all of R. So an ideal is not usually a subring.

(3) $\mathbb{Z}$ is a PID: i.e., every ideal in $\mathbb{Z}$ is of the form $(n) = \{nx : x \in \mathbb{Z}\}$ for some $n \in \mathbb{Z}$.

(4) If A is a ring of functions on a space X and $Y \subseteq X$ is a subspace, then
$$I = \{f \in A : f(y) = 0 \,\forall\, y \in Y\}$$
is an ideal.

10/10

Definition. For ideals I and J in a ring R we define $I + J$ to be the ideal (Check: Exercise!) $I + J := \{x + y : x \in I,\, y \in J\}$.

For an ideal I in a ring R, the *quotient ring* R/I is the quotient abelian group with product structure defined by $f(x)f(y) := f(xy)$ (where f is the quotient map $f\colon R \twoheadrightarrow R/I$).

This is well defined since I is an ideal, and $f\colon R \twoheadrightarrow R/I$ is a ring homomorphism. Usually we use the same name x for an element of R and its image in R/I.

Example. In $\mathbb{Q}[x]$ the elements x^3 and $5x^2$ aren't equal, but in the quotient ring $\mathbb{Q}[x]/(x^2-5)$, we do have $x^3 = 5x$.

For a ring homomorphism $f\colon A \to B$ the image $f(A) = \operatorname{im} f$ is a subring of B, and $\ker f = \{a \in A : f(a) = 0\}$ is an ideal of A. Moreover, $A/\ker f$ and $\operatorname{im} f$ are isomorphic as rings: $A/\ker f \cong \operatorname{im} f$.

Note: for a positive integer n, the quotient ring $\mathbb{Z}/(n)$ is usually called $\mathbb{Z}/n$ for short.

Exercise. For a nonzero ring R, the following are equivalent:

(1) R is a field;

(2) the only ideals in R are 0 and R;

(3) any ring homomorphism from R to a nonzero ring is injective.

Exercise. Show that in any ring R the set of nilpotent elements forms an ideal, called the *nilradical* of R, $\mathcal{N} = \operatorname{rad}(0) \subseteq R$. Show the quotient $R/\mathcal{N}$ is reduced.

1.2 Modules

Definition. A *module* M over a ring R is an abelian group with a function $R \times M \to M$, written $(r, m) \mapsto rm$, satisfying

(1) $(r+s)m = rm + sm$ for all $r, s \in R$, $m \in M$;

(2) $r(m_1 + m_2) = rm_1 + rm_2$ for all $r \in R$, $m_1, m_2 \in M$;

(3) $(rs)m = r(sm)$ for all $r, s \in R$, $m \in M$;

(4) $1 \cdot m = m$ for every $m \in M$.

Remark. This definition makes sense for noncommutative rings and defines a *left* R-module.

Examples.

(1) For a field k, a k-module is just a k-vector space.

(2) A $\mathbb{Z}$-module is just an abelian group.

(3) For a field k, a $k[x]$-module M is equivalent to a k-vector space with a k-linear map $x\colon M \to M$.

(4) An ideal I in a ring R determines two R-modules. First, an ideal is exactly an R-submodule of R. But also the quotient ring R/I is an R-module.

Definition. An *R-module homomorphism* (or *R-linear map*) $M_1 \to M_2$ is a homomorphism $f\colon M_1 \to M_2$ of abelian groups such that $f(rm_1) = rf(m_1)$ for every $r \in R$, $m_1 \in M_1$.

This definition makes the collection of R-modules (for a fixed R) into a category.

For R-modules M and N the set $\operatorname{Hom}_R(M, N)$ of R-linear maps $M \to N$ is an abelian group under pointwise addition: $(f+g)(m) = f(m)+g(m)$ for $m \in M$. Since R is commutative, $\operatorname{Hom}_R(M, N)$ is an R-module:

$$(a \cdot f)(m) = a \cdot f(m) \text{ for } a \in R,\ f \in \operatorname{Hom}_R(M, N),\ m \in M.$$

Definition. An *R-submodule* of an R-module M is an abelian subgroup $N \subseteq M$ such that $r \cdot n \in N$ for all $r \in R$, $n \in N$.

For an R-submodule N of M, the *quotient R-module* M/N is the quotient abelian group with the obvious R-module structure: $r(f(m)) = f(rm)$, if $f\colon M \twoheadrightarrow M/N$ is the quotient map.

For any homomorphism $f\colon M \to N$ of R-modules, the *kernel* is the set $\ker f = \{m \in M : f(m) = 0\}$, the *image* is $\operatorname{im} f = f(M) \subseteq N$, and the *cokernel* is the set $\operatorname{coker}(f) = N/f(M)$ are R-modules. Here f induces an isomorphism

$$M/\ker f \xrightarrow{\cong} \operatorname{im} f.$$

1.3 Prime & maximal ideals

Definition. An ideal I in a ring R is:

- *maximal* if R/I is a field;
- *prime* if R/I is a domain;
- *radical* if R/I is reduced.

In particular maximal ⇒ prime ⇒ reduced.

Exercise. (1) An ideal I in R is maximal iff $I \neq R$ and there is no ideal J with $I \subsetneq J \subsetneq R$.

(2) An ideal I is prime iff $I \neq R$ and the product xy belongs to I only if $x \in I$ or $y \in I$.

(3) Write out what it means for I to be radical without mentioning R/I.

Examples.

(1) The maximal ideals in $\mathbb{Z}$ are (2), (3), (5), (7),.... The prime ideals are 0 and (2), (3), (5), (7),.... Radical ideals in $\mathbb{Z}$ are 0 and the ideals $(p_1, \ldots, p_r)$ with $r \geq 0$ and the p_i distinct primes. (Note in any ring $(1) = R$.)

(2) Let k be a field. Then $k[x]$ is a PID and therefore a UFD (see Lang). So every ideal in $k[x]$ has the form (f) for some $f \in k[x]$. Therefore an ideal in $k[x]$ is either (0) or $k[x] = (1)$, or $(f_1^{e_1}, \ldots, f_r^{e_r})$, where $f_1, \ldots, f_r \in k[x]$ are irreducible polynomials, distinct modulo units (note $k[x]* = k*$), and $e_1, \ldots, e_r$ are each ≥ 1. So the nonzero prime ideals in $k[x]$ are (f) with f irreducible over k.

Example. If k is algebraically closed, the only irreducible polynomials (up to units) are $x - a$ for $a \in k$.

Example. Some examples of prime ideals in $\mathbb{Z}[x]$ are (0), (7), (x), and $(7, x)$. Of these, only $(7, x)$ is maximal.

Definition. For a homomorphism $f\colon A \to B$ of rings and an ideal $J \subseteq B$, the *contraction* of J in A is the preimage $f^{-1}(J)$, which is an ideal of A.

For a ring homomorphism $f\colon A \to B$ and an ideal $I \subseteq A$, the *extended ideal* $I^e = IB \subseteq B$ is the ideal generated by $f(I) \subseteq B$.

In particular, for f the inclusion of a subring A of B, the contracted ideal of $J \subseteq B$ is just the intersection $J \cap A \subseteq A$, and the extended ideal is $IB \subseteq B$.

Lemma 1.1. For any ring homomorphism $f\colon A \to B$ and any prime ideal $\mathfrak{p} \subseteq B$, the contraction $f^{-1}(\mathfrak{p}) \subseteq A$ is prime.

Proof. Notice that the contraction $f^{-1}(\mathfrak{p})$ is the kernel of the composite

$$A \xrightarrow{f} B \longrightarrow B/\mathfrak{p}.$$

Since $\mathfrak{p}$ is prime in B, the quotient $B/\mathfrak{p}$ is a domain, and the image $\operatorname{im}(A \to B/\mathfrak{p})$, which is a subring of $B/\mathfrak{p}$, must also be a domain. Observing that $\operatorname{im}(A \to B/\mathfrak{p}) \cong A/\ker(A \to B/\mathfrak{p}) = A/f^{-1}(\mathfrak{p})$, we conclude that $f^{-1}(\mathfrak{p})$ is prime in A. ∎

Note that, unlike prime ideals, maximal ideals don't always pull back under ring homomorphisms: under the inclusion $\mathbb{Z} \hookrightarrow \mathbb{Q}$, the inverse image of the maximal ideal $0 \subseteq \mathbb{Q}$ is the prime ideal $0 \subseteq \mathbb{Z}$, which is not maximal. 12/10

We'll show that every nonzero ring contains a maximal ideal, hence a prime ideal. (For the zero ring, the only ideal is not maximal.)

The proof relies on Zorn's Lemma, which is equivalent to the Axiom of Choice.

Lemma 1.2 (Zorn's Lemma)**.** Let S be a poset. Suppose every chain (totally ordered subset) of S has an upper bound in S. Then S has a maximal element.

Theorem 1.3. Every nonzero ring R contains a maximal ideal.

Proof. Let S be the poset of proper ideals of R (ordered by $\subseteq$). We have to show that every totally ordered subset C of ideals in R has an upper bound; i.e., that there exists a proper ideal $J \subseteq R$ such that $I \subseteq J$ for every $I \in C$.

If $C = \varnothing$ then the ideal $0 \subseteq R$ suffices. If $C \neq \varnothing$, then let $J = \bigcup C \subseteq R$. Because C is totally ordered, J is an ideal in R. It remains to show that $J \neq R$. If $J = R$ then 1 belongs to J, but then 1 belongs to some $I \in C$; then $I = R$, a contradiction. So J is an upper bound for C, and we're done by Zorn's Lemma. ∎

Corollary 1.4. Every proper ideal I in a ring R is contained in some maximal ideal.

Proof. We use the theorem applied to R/I. Because $I \neq R$, the quotient R/I is nonzero, so R/I has a maximal ideal $\mathfrak{m}$. Then the composite

$$R \twoheadrightarrow R/I \twoheadrightarrow (R/I)/\mathfrak{m}$$

has kernel a maximal ideal of R, since $(R/I)/\mathfrak{m}$ is a field. ∎

Definition. For a ring R the *prime spectrum* $\mathrm{Spec}(R)$ is the set of prime ideals in R.

We define a topology on the set $\mathrm{Spec}(R)$, the Zariski topology: For an ideal $I \subseteq R$, define $V(I) := \{\mathfrak{p} \in \mathrm{Spec}(R) : \mathfrak{p} \supseteq I\}$. We define the closed subsets of $\mathrm{Spec}(R)$ to be the subsets $V(I)$ for an ideal $I \subseteq R$. (A subset $S \subseteq \mathrm{Spec}(R)$ is open iff $\mathrm{Spec}(R) \smallsetminus S$ is closed.)

Why do we do this? Say R is the ring of functions on a set X with values in a field k containing the constant k. Then a point $p \in X$ gives a maximal ideal in R, namely the kernel $\ker(R \twoheadrightarrow k)$ of the evaluation map $f \mapsto f(p)$. For an arbitrary commutative ring R consider the homomorphisms from R to *any* field. The kernel of a ring homomorphism from R to a field is a prime ideal. Conversely, a prime ideal $\mathfrak{p}$ is the kernel of the composite $R \twoheadrightarrow R/\mathfrak{p} \hookrightarrow \mathrm{Frac}(R/\mathfrak{p})$. (The ring $\mathrm{Frac}(R/\mathfrak{p})$ is the field of fractions of the domain $R/\mathfrak{p}$.) Then we have

$$V(I) = \{\mathfrak{p} \in \mathrm{Spec}(R) : \forall f \in I,\ f \text{ maps to 0 in the ring } R/\mathfrak{p}\}.$$

If $I = (f_1, \ldots, f_r) \subseteq R$, then we write $V(I) = \{f_1 = 0, \ldots, f_r = 0\}$.

Theorem 1.5. For any ring R, the set $\mathrm{Spec}(R)$ is a topological space.

Proof. We have to show:

(1) Both $\varnothing$ and $\mathrm{Spec}(R)$ are closed subsets of $\mathrm{Spec}(R)$;

(2) the intersection of any collection of closed subsets is closed; and

(3) the union of two closed subsets is closed.

(1) The closed set $V(0) \subseteq R$ is exactly the set $\{\mathfrak{p} \in \mathrm{Spec}(R) : \mathfrak{p} \supseteq 0\} = \mathrm{Spec}(R)$. So $\mathrm{Spec}(R)$ is closed. Also $V(R) = \{\mathfrak{p} \in \mathrm{Spec}(R) : \mathfrak{p} \supseteq R\} = \varnothing$, so $\varnothing$ is closed.

(2) We're given a collection $(I_\alpha)_{\alpha \in S}$ of ideals, and we want to find a J such that $V(J) = \bigcap_{\alpha \in S} V(I_\alpha)$. Let $J = \sum_{\alpha \in S} I_\alpha$, the ideal of finite sums of elements of $\bigcup_{\alpha \in S} I_\alpha$. Then it is obvious that a prime ideal $\mathfrak{p} \subseteq R$ contains J iff $\mathfrak{p}$ contains every I_α. So $\bigcap_{\alpha \in S} V(I_\alpha)$ is closed.

(3) Given ideals I and J in R, we want to find an ideal $K \subseteq R$ such that $V(K) = V(I) \cup V(J)$. Let $K = I \cap J$, which is an ideal. We need to show that the prime $\mathfrak{p}$ contains $I \cap J = K$ if and only if $\mathfrak{p} \supseteq I$ or $\mathfrak{p} \supseteq J$. It is easy to see that if $\mathfrak{p} \supseteq I$ or $\mathfrak{p} \supseteq J$, then $I \cap J = K$; so suppose the prime $\mathfrak{p}$ contains $I \cap J$ and suppose that $\mathfrak{p}$ contains neither I nor J. Then there are elements $x \in I$ and $y \in J$ that are not in $\mathfrak{p}$. We have $xy \notin \mathfrak{p}$ because $\mathfrak{p}$ is prime, but $xy \in I \cap J$, a contradiction. Therefore we have proved the other implication. ∎

Examples.

- The spectrum $\mathrm{Spec}(\mathbb{Q})$ of $\mathbb{Q}$, or of any field, is just a point.
- $\mathrm{Spec}(\mathbb{Z})$ is a set $\{(2), (3), (5), \ldots\}$ of discrete points along with a blob 0. The points (p) for p prime are closed in $\mathrm{Spec}(\mathbb{Z})$, but the closure of the point 0 is $\mathrm{Spec}(\mathbb{Z})$. In this case 0 is called the *generic point*.
- $\mathrm{Spec}(\mathbb{C})$ is just $\mathbb{C}$ with a generic point. A subset of $\mathrm{Spec}(\mathbb{C}[x])$ is closed (?) if and only if it is either the whole space or it is a finite subset of $\mathbb{C} \smallsetminus \{0\} \subseteq \mathrm{Spec}(\mathbb{C}[x])$.

Different ideals in a ring R can give the same closed set $V(I) \subseteq \mathrm{Spec}(R)$. We'll now analyze when this occurs. The first step is the following theorem.

Theorem 1.6. For every ring R, the nilradical of R is the intersection of all prime ideals in R.

Proof. One direction is easy: if $x \in R$ is nilpotent, i.e. $x^n = 0$ for some $n \geq 1$, then $x \in \mathfrak{p}$ for every ideal $\mathfrak{p}$ in R. Indeed, $R/\mathfrak{p}$ is a domain, so the image of x in the quotient $R/\mathfrak{p}$ is nilpotent; so $x = 0$ in $R/\mathfrak{p}$, i.e., $x \in \mathfrak{p}$.

Conversely, suppose that $x \in R$ belongs to every prime ideal and that x is not nilpotent. Let S be the set of ideals I in R such that $x^n \notin I$ for all $n > 0$. First we'll show that S has a maximal element using Zorn's Lemma.

Clearly $S \neq \varnothing$ since the ideal 0 is an element of S. Suppose that $\{I_\alpha\}$ is a totally ordered nonempty subset of S; we have to find an upper bound J in S for $\{I_\alpha\}$. Let $J = \bigcup I_\alpha$, which is an ideal since $\{I_\alpha\}$ is totally ordered. We have to show that $J \in S$, i.e. that $x^n \notin J$ for all $n > 0$. If x^n were in J, we would have $x^n \in I_\alpha$ for some α, a contradiction. So by Zorn's Lemma S contains a maximal element J. I claim J is prime. (Clearly $x \notin J$, so that will finish the proof.) If not, there are $a \in R \smallsetminus J$ and $b \in R \smallsetminus J$ such that $ab \in J$. Then the ideals $J + (a)$ and $J + (b)$ do not belong to S by the maximality of J, so there exist positive integers m and n such that $x^m \in J + (a)$ and $x^n \in J + (b)$. But then $x^{m+n} \in J + (ab) = J$, a contradiction. We conclude that J is prime. ∎

14/10 The theorem about the nilradical implies the following: for an ideal I in a ring R, the set closed set $V(I)$ associated to I is equal to $\operatorname{Spec}(R)$ if and only if $I \subseteq \operatorname{rad}(0) \subseteq R$.

Definition. For an ideal I in a ring R, the *radical* $\operatorname{rad}(I)$ of I is the ideal

$$\operatorname{rad}(I) = \left\{x \in R : (\exists\, n > 0)\ x^n \in I\right\}.$$

Clearly $I \subseteq \operatorname{rad}(I)$; it's easy to check that $\operatorname{rad}(I)$ is radical and is the smallest radical ideal that contains I. (Exercise!) Also, $\operatorname{rad}(I)$ is the inverse image in R of the nilradical in R/I.

Lemma 1.7. For any ideal I in a ring R, the radical $\operatorname{rad}(I)$ of I is the intersection of all prime ideals that contain I.

Proof. Look at the quotient ring R/I. We know that the nilradical of R/I is the intersection of the primes in R/I. The primes in R/I are exactly those whose preimages in R are prime and contain I. ∎

Corollary 1.8. For any ideals I and J in a ring R, their associated closed sets are equal if and only if their radicals are equal: $V(I) = V(J)$ if and only if $\operatorname{rad}(I) = \operatorname{rad}(J)$.

Proof. By definition, $V(I) = V(J)$ if and only if the set of primes containing I is the set of primes containing J. This is true if and only if $\operatorname{rad}(I) = \operatorname{rad}(J)$ by the Lemma (1.7). ∎

So we have a one-to-one correspondence between radical ideals in R and closed subsets of $\operatorname{Spec}(R)$. Given a closed subset $S \subseteq \operatorname{Spec}(R)$, the corresponding radical ideal is $\bigcap S \subseteq R$.

Example. For an integer $n \neq 0$, the closed subset $V((n)) = \{n = 0\}$ of $\operatorname{Spec}(\mathbb{Z})$ is exactly the set of prime ideals (p) for prime numbers p dividing n. So the subset $\{12 = 0\} \subseteq \operatorname{Spec}(\mathbb{Z})$ is the pair of points $\{(2), (3)\}$. This is the same as the closed subset $\{6 = 0\} \subseteq \operatorname{Spec}(\mathbb{Z})$, since $\operatorname{rad}((12)) = (6)$.

Definition. The product IJ of ideals $I, J \subseteq R$ is the ideal containing all finite products ab with $a \in I$ and $b \in J$.

Clearly $IJ \subseteq I \cap J$. In some examples $IJ = I \cap J$, but that isn't always true.

Example. In the ring $\mathbb{Z}$, the intersection of the ideals (2) and (3) is the same as their product: $(2) \cap (3) = (6) = (2)(3)$. But this isn't always the case: for example, $(2) \cap (2) = (2)$, whereas $(2)(2) = (4)$.

Exercise. Show that IJ has the same radical as $I \cap J$.

With this in mind, observe that $V(I) \cup V(J) = V(I \cap J) = V(IJ)$. (Recall we proved the first equality in showing that the Zariski topology formed a topology.)

Since the topology on $\operatorname{Spec}(R)$ can't distinguish between the intersection $I \cap J$ and the product IJ, we will often use the product, which is the simpler of the two. Indeed, if $I = (f_1, \ldots, f_a)$ and $J = (g_1, \ldots, g_b)$, then IJ is generated by all products $f_i g_j$, whereas it's not clear how to write down generators for $I \cap J$.

In particular, for an ideal I and a positive integer n, we define I^n to be the product ideal

$$I^n = \underbrace{II \cdots I}_{n}.$$

By convention $I^0 = R$.

Theorem 1.9. Let $f : A \to B$ be a homomorphism of commutative rings. Define the associated map $g : \operatorname{Spec}(B) \to \operatorname{Spec}(A)$ by $g(\mathfrak{p}) = f^{-1}(\mathfrak{p})$. Then:

(1) g is continuous;

(2) for a homomorphism $A \to A/I$ for an ideal $I \subseteq A$, the map g is a homeomorphism $\mathrm{Spec}(A/I)$ onto the closed subset $V(I)$ of $\mathrm{Spec}(A)$.

Proof.

(1) It suffices to prove that the preimage under g of every closed set in $\mathrm{Spec}(A)$ is closed in $\mathrm{Spec}(B)$. Let $V(I)$ be a closed set in $\mathrm{Spec}(A)$; we want to show that $g^{-1}(V(I)) = V(J)$, some ideal J in B. Let J be the extended ideal $J = f(I) \cdot B \subseteq B$. We want to show that a prime ideal $\mathfrak{p}$ in B contains the extended ideal $f(I)B$ if and only if $f^{-1}(\mathfrak{p})$ contains I. But this is obvious: $\mathfrak{p} \supseteq f(I)B$ iff $\mathfrak{p} \supseteq f(I)$ since $\mathfrak{p}$ is an ideal, and $\mathfrak{p} \supseteq f(I)$ iff $f^{-1}(\mathfrak{p}) \supseteq I$. This completes the proof that $g^{-1}(V(I)) = V(J)$.

(2) I'll show that $g\colon \mathrm{Spec}(A/I) \to \mathrm{Spec}(A)$ is injective. Because f is surjective, we the equality $f^{-1}(\mathfrak{p}) = f^{-1}(\mathfrak{q})$ implies $\mathfrak{p} = \mathfrak{q}$. That is, the map g is injective. The proof that g has a continuous inverse is an exercise. ∎

Now for some language without much content:

2 Affine schemes

An *affine scheme* is a topological space X and a commutative ring R together with a homeomorphism $X \xrightarrow{\cong} \mathrm{Spec}(R)$. In this case we call R the *ring $\mathcal{O}(X)$ of regular functions* on the affine scheme X.

Example. For any field k the spectrum $\mathrm{Spec}(k)$ is just a point as a topological space, but as a scheme this scheme determines the field k.

Definition. For a ring R and $n \geq 0$, we define *affine n-space over R* to be the affine scheme $\mathrm{Spec}(R[x_1, \ldots, x_n])$. A *morphism of affine schemes* is a map $\mathrm{Spec}(B) \to \mathrm{Spec}(A)$ given by a ring homomorphism $A \to B$.

So a morphism $X \to Y$ of affine schemes determines a ring homomorphism $\mathcal{O}(Y) \to \mathcal{O}(X)$. This is like the setting when $f\colon X \to Y$ is a continuous map of topological spaces, and f induces a ring homomorphism $C(Y) \to C(X)$ (given by precomposition by f).

3 Irreducible closed subsets of $\mathrm{Spec}(R)$

Lemma 3.1. Let R be a domain. The closure in $\mathrm{Spec}(R)$ of the point corresponding to the prime ideal $0 \subseteq R$ is all of $\mathrm{Spec}(R)$. We call that point the *generic point* of $\mathrm{Spec}(R)$.

Proof. Suppose we have an ideal I such that $V(I)$ contains the point p corresponding to the prime (since R is a domain) ideal $0 \subseteq R$. Then 0 contains I, which means $I = 0$. So $V(I) = \mathrm{Spec}(R)$. ∎

Corollary 3.2. For any ring R and any point $p \in \mathrm{Spec}(R)$ let $\mathfrak{p}$ be the corresponding prime ideal in R. Then the closure of the point p is the closed subset $V(\mathfrak{p})$.

Proof. We know $\mathrm{Spec}(R/\mathfrak{p})$ is homeomorphic to the closed subset $V(\mathfrak{p}) \subseteq \mathrm{Spec}(R)$ (Theorem 1.9). This homeomorphism sends the prime ideal 0 in $R/\mathfrak{p}$ to its inverse image in R, which is $\mathfrak{p}$. So the closure of the point p in $\mathrm{Spec}(R)$ is $V(\mathfrak{p})$, by the lemma. ∎

Definition. A topological space X is *connected* if X is nonempty and is not the union of two disjoint nonempty closed subsets. We say X is *irreducible* if X is nonempty and cannot be written as $A \cup B$, for A, B proper closed subsets of X.

Example. The unit interval $[0,1] \subseteq \mathbb{R}$ is connected but not irreducible: $[0,1] = [0,1/2] \cup [1/2,1]$.

Lemma 3.3. For a ring R there is a one-to-one correspondence among the following:

(1) prime ideals in R;

(2) points in $\mathrm{Spec}(R)$;

(3) irreducible closed subsets of $\mathrm{Spec}(R)$.

Proof. The equivalence (1) $\leftrightarrow$ (2) follows from the definition of $\mathrm{Spec}(R)$. For every point $\mathfrak{p} \in \mathrm{Spec}(R)$, the closure $\{\mathfrak{p}\} = V(\mathfrak{p})$ is irreducible. Indeed, suppose $V(\mathfrak{p}) = A \cup B$ for A, B closed in $\mathrm{Spec}(R)$, and $A \neq V(\mathfrak{p})$ and $B \neq$

$V(\mathfrak{p})$. Clearly $\mathfrak{p} \in A$ or $\mathfrak{p} \in B$; say $\mathfrak{p} \in A$. But then, since A is closed, it must be that $A \supseteq \overline{\{\mathfrak{p}\}} = V(\mathfrak{p})$, a contradiction. So $V(\mathfrak{p})$ is irreducible.

Conversely, I claim any irreducible closed subset of $\mathrm{Spec}(R)$ is the closure of a point. The subset can be written as $V(I) \subseteq \mathrm{Spec}(R)$; we may assume I is a radical ideal. I claim that, if $V(I)$ is irreducible, then I must be prime. (The proof of this completes the proof, since $V(\mathfrak{p})$ for a prime $\mathfrak{p}$ is the closure of a point $\{\mathfrak{p}\}$.) Clearly $I \neq R$, since $V(R) = \varnothing$. It remains to show that if $a, b \in R$ satisfy $ab \in I$, then $a \in I$ or $b \in I$. Suppose for a contradiction that neither a nor b belongs to I. Then $V(I+(a)) \subsetneq V(I)$ and $V(I+(b)) \subsetneq V(I)$. We get a contradiction by proving that $V(I) = V(I+(a)) \cup V(I+(b))$: Clearly the inclusion $\supseteq$ holds; we have

$$V(I+(a)) \cup V(I+(b)) = V((I+(a))(I+(b))),$$

but $(I+(a))(I+(b)) \subseteq I+(ab) \subseteq I$ since $ab \in I$. Therefore $V(I) \subseteq V((I+(a))(I+(b)))$. ∎

17/10

Exercise. Show that closed points in $\mathrm{Spec}(R)$ are in one-to-one correspondence with maximal ideals in R.

So we have one-to-one correspondences

$$\begin{aligned} \{\text{closed points in } \mathrm{Spec}(R)\} &\longleftrightarrow \{\text{maximal ideals in } R\}, \\ \{\text{irreducible closed subsets of } \mathrm{Spec}(R)\} &\longleftrightarrow \{\text{prime ideals in } R\}, \\ \{\text{closed subsets of } \mathrm{Spec}(R)\} &\longleftrightarrow \{\text{radical ideals in } R\}. \end{aligned}$$

Example. The subset $\{xy = 0\}$ of $\mathbb{A}^2_k$ is not irreducible: it's the union of two irreducible subsets $\{x = 0\} \cup \{y = 0\}$.

4 Operations on modules

Definition. Let M be a module over a ring R. We define the *annihilator* ideal to be

$$\mathrm{Ann}_R(M) := \{a \in R : am = 0 \ \forall m \in M\}.$$

Also the *annihilator* of an element $m \in M$ is defined to be

$$\mathrm{Ann}_R(m) = \{a \in R : am = 0\}.$$

The *direct sum* of the R-modules M and N is the product set $M \oplus N := M \times N$ with the module structure

$$(m_1, n_1) + (m_2, n_2) = (m_1 + m_2, n_1 + n_2),$$

$$a(m, n) = (am, an).$$

The *direct product* of a collection $\{M_\alpha\}_{\alpha \in S}$ of R-modules is $\prod_{\alpha \in S} M_\alpha$ with obvious module structure.

The *direct sum* of $\{M_\alpha\}_{\alpha \in S}$ is the submodule of the direct product consisting of elements $(m_\alpha : \alpha \in S)$ such that $m_\alpha = 0$ for all but finitely many α.

A *free R-module* is the direct sum of some collection of copies of R, written $R^{\oplus S}$ for a set S. (e.g., $(r_1, \ldots, r_m, 0, \ldots, 0, \ldots)$ is a typical element of $R^{\oplus R}$.)

This free module contains one copy of R for each element of S. Every element of $R^{\oplus S}$ is a finite R-linear combination of the basis elements $(0, \ldots, 0, 1, 0, \ldots)$. Using that, one proves a 'universal property' of free modules: R-linear maps $R^{\oplus S} \to M$ (for any R-module M) are in one-to-one correspondence with functions $S \to M$.

Definition. A sequence of R-linear maps

$$\cdots \longrightarrow M_{i+1} \xrightarrow{d_{i+1}} M_i \xrightarrow{d_i} M_{i-1} \longrightarrow \cdots$$

is called *exact* if $\mathrm{im}(d_{i+1}) = \ker d_i$ for every i.

Examples.

(1) A sequence $0 \longrightarrow M \xrightarrow{f} N$ is exact iff f is injective.

(2) A sequence $M \xrightarrow{f} N \longrightarrow 0$ is exact iff f is surjective.

(3) You can check (Exercise!) that the sequence $0 \longrightarrow M \xrightarrow{f} N \longrightarrow 0$ is exact iff $M \xrightarrow{f} N$ is an isomorphism.

(4) Finally, can check (Exercise!) that the 'short' sequence

$$0 \longrightarrow A \longrightarrow B \longrightarrow C \longrightarrow 0$$

is exact iff A is isomorphic to a submodule of B and $C \cong B/A$.

An R-module M is *generated* by a subset $S \subseteq M$ if M is the smallest submodule of M containing S.

Definition. An R-module M is *finitely generated* (as an R-module) if M is generated by a finite set S.

If a module M is generated by a set S, then we get a surjection

$$R^{\oplus S} \longrightarrow M \longrightarrow 0. \qquad \text{exact}$$

Given a set S of generators for an R-module M, let $K = \ker(R^{\oplus S} \twoheadrightarrow M)$. Let T be a set of generators for the R-module K. Then we have an exact sequence

$$R^{\oplus T} \xrightarrow{\phi} R^{\oplus S} \longrightarrow M \longrightarrow 0.$$

Such a diagram is called a *presentation* of M as an R-module. In this way, we see that M is completely determined by a set S and a set $T \subseteq R^{\oplus S}$.

Example. Consider the $\mathbb{Z}$-module $\mathbb{Z}\langle e_1, e_2 \mid 2e_1 = 2e_2\rangle$, ie $\mathbb{Z}^{\oplus 2}/(2,-2)$. Can check that this is isomorphic to $\mathbb{Z} \oplus \mathbb{Z}/2$.

Definition. A module M over R is *projective* iff there is an R-module N such that $M \oplus N$ is free.

For example, a free R-module is projective.

Lemma 4.1. Let M be an R-module. The following are equivalent:

(1) M is projective as an R-module;

(2) For any short exact sequence

$$0 \longrightarrow A \longrightarrow B \longrightarrow M \longrightarrow 0,$$

the sequence *splits*, i.e. there is an R-linear map $M \to B$ such that the composition $M \to B \to M$ is the identity. (This implies $B \cong A \oplus M$.)

(3) For any short exact sequence

$$0 \longrightarrow A \longrightarrow B \longrightarrow C \longrightarrow 0,$$

of R-modules and any R-linear map $M \to C$, this map *lifts* to B; that is, there is an R-linear map $M \to B$ such that the composites $M \to B \to C$ and $M \to C$ are equal.

Proof. (3) $\Rightarrow$ (2): Apply (3) to the sequence in (2) and the identity map $M \to M$.

(2) $\Rightarrow$ (1): Let S be a set of generators for M: so we have the exact sequence

$$0 \longrightarrow K \longrightarrow R^{\oplus S} \longrightarrow M \longrightarrow 0.$$

Given (2) this sequence splits, so $R^{\oplus S} \cong M \oplus K$. Therefore M is projective.

Suppose M is a projective R-module and $B \to C$ is a surjective R-linear map. We want to show that any R-linear map $M \to C$ lifts to a map $M \to B$. There is an R-module N such that $M \oplus N \cong R^{\oplus S}$ for some set S. Consider the projection $R^{\oplus S} \twoheadrightarrow M$. Such a map ($M \to C$??) is equivalent to a function $S \to C$. For every $s \in S$ pick an element of B that maps to the image of s in C. This gives an R-linear map $R^{\oplus S} \to B$ (because the map $B \to C$ is surjective). Restrict this to the submodule $M \subseteq R^{\oplus S}$ to get a map $M \to B$. Check that this map composed with the given map $B \to C$ is the given map $M \to C$. ∎ 19/10

Example. The $\mathbb{Z}$-module $\mathbb{Z}/2$ is not projective, since the exact sequence

$$0 \longrightarrow \mathbb{Z} \xrightarrow{2} \mathbb{Z} \longrightarrow \mathbb{Z}/2 \longrightarrow 0$$

does not split: the only map $\mathbb{Z}/2 \to \mathbb{Z}$ is the zero map. (Generalise this. Exercise!)

Remark. A finitely generated projective R-module is equivalent to a vector bundle on $\operatorname{Spec} R$ for a noetherian ring R.

Exercise. Show that a finitely generated projective module over a ring R is the summand of a finitely generated free module, $R^{\oplus n}$ for some $n \in \mathbb{N}$. (Use the Lemma.)

5 Direct limits

A *directed set* S is a poset S such that for any $a, b \in S$ there is a $c \in S$ such that $a \le c$ and $b \le c$. A *directed system of sets* A is a functor from a directed set to the category **Set** of sets.[1] That is, every $s \in S$ is assigned a set A_s, and every pair of elements $s \le t$ is assigned a map $A_s \xrightarrow{f_{st}} A_t$ such that

(1) f_{ss} is the identity on A_s; and

(2) if $s \le t \le u$ in S, then $f_{su} = f_{tu} \circ f_{st}$ as maps $A_s \to A_u$.

Definition. Define the *direct limit* $\varinjlim A_s$ of a directed system $(A_s : s \in S)$ of sets to be the quotient of the disjoint union $\coprod_{s \in S} A_s$ by the following relation: $a \in A_s$ is equivalent to $b \in A_t$ if there is an element $u \in S$ such that $u \ge s$, $u \ge t$, and $f_{su}(a) = f_{tu}(b)$ in A_u.

Think of the greater elements of S as things coming later in time; so the relation identifies things that are eventually equal.

The same definition defines the direct limit of a directed system of groups, rings, R-modules, etc.

If $(A_s : s \in S)$ is a directed system of R-modules, then the direct limit $\varinjlim A_s$ is an R-module: the sum of the elements $a \in A_s$ and $b \in A_t$ is given by an element $u \in S$ such that $s \le u$ and $t \le u$; define $a + b$ by mapping a and b into the R-module A_u and adding them there. One checks that this is well defined on $\varinjlim A_s$. Multiplication by an element of R is defined similarly.

[1] See Lang's *Algebra* if you're unfamiliar with functors.

Exercise. Prove the universal property of direct limits of R-modules: for any directed system $(A_s : s \in S)$ of R-modules there is a one-to-one correspondence between R-linear maps $\varinjlim A_s \to N$ and families of R-linear maps $(A_s \to \varinjlim_{t \in S} A_t)_{s \in S}$ such that for every pair $s \le t$ in S the composite $A_s \longrightarrow A_t \xrightarrow{g_t} N$ is the map $g_s \colon A_s \to N$.

Example. The direct limit of the $\mathbb{Z}$-modules

$$\mathbb{Z} \xrightarrow{2} \mathbb{Z} \xrightarrow{2} \mathbb{Z} \xrightarrow{2} \cdots$$

is isomorphic to $\mathbb{Z}[\frac{1}{2}]$, the subgroup of $\mathbb{Q}$ of elements $\frac{a}{2^b}$. Indeed, the limit is isomorphic to the direct limit

$$\varinjlim(\mathbb{Z} \hookrightarrow \tfrac{1}{2}\mathbb{Z} \hookrightarrow \tfrac{1}{4}\mathbb{Z} \hookrightarrow \cdots) = \bigcup_{s \ge 0} \tfrac{1}{2^s}\mathbb{Z} = \mathbb{Z}[\tfrac{1}{2}].$$

Also, the direct limit of the $\mathbb{Z}$-modules

$$\mathbb{Z} \xrightarrow{0} \mathbb{Z} \xrightarrow{0} \mathbb{Z} \xrightarrow{0} \cdots$$

is the group 0.

6 Tensor products

Let R be a (commutative) ring and M, N R-modules. Then an *R-bilinear map* $f \colon M \times N \to P$ is a function $M \times N \to P$ that is linear in each variable; that is, $f(m, -) \colon N \to P$ is an R-linear map for every $m \in M$ and $f(-, n) \colon M \to P$ is an R-linear map for every $n \in N$.

Theorem 6.1. For any two R-modules M and N there is an R-module $M \otimes_R N$, called the *tensor product* of M and N, with a bilinear map $M \times N \to M \otimes_R N$, such that for any R-bilinear map $f \colon M \times N \to P$ there is a unique R-linear map

$$g \colon M \otimes_R N \to P$$

such that the composite $M \times N \longrightarrow M \otimes_R N \xrightarrow{g} P$ is equal to f.

Proof. Consider the free R-module $R^{\oplus(M\times N)}$. Write $a\otimes b$ for the basis element corresponding to $a\in M$, $b\in N$. So every element of $R^{\oplus(M\times N)}$ is uniquely a finite sum $\sum_{i=1}^{N} r_i(m_i\otimes n_i)$ for some $r_i\in R$, $m_i\in M$, $n_i\in N$. Define $M\otimes_R N$ as the quotient of $R^{\oplus(M\times N)}$ by the following relations:

$$\begin{aligned}(m_1+m_2)\otimes n &= m_1\otimes n + m_2\otimes n,\\ m\otimes(n_1+n_2) &= m\otimes n_1 + m\otimes n_2,\\ (rm)\otimes n &= r(m\otimes n),\\ m\otimes(rm) &= r(m\otimes n)\end{aligned}$$

(for every $r\in R$, $m_i, m\in M$, $n_i, n\in N$). (That is, take the quotient by the submodule generated by all elements $(m_1+m_2)\otimes n-(m_1\otimes n+m_2\otimes n)$, etc.)

Clearly, by these relations, the obvious map $M\times N\to M\otimes_R N$ is R-bilinear. (We've forced it to be!) And for any R-module P with an R-bilinear map $f\colon M\times N\to P$, there is a corresponding R-linear map $R^{\oplus(M\times N)}\to P$. Because f is bilinear, the submodule of $R^{\oplus(M\times N)}$ that we killed maps to 0 in P. So f factors through the quotient to give a map $g\colon M\otimes_R N\to P$. Uniqueness of this map g is left as an exercise. ∎

Tensor products allow us to describe bilinear maps in terms of linear maps, which are simpler.

Remark. (1) By construction, every element of $M\otimes_R N$ can be written as a finite sum $\sum r_i(m_i\otimes n_i)=\sum(r_i m_i)\otimes n_i$. But it isn't obvious how to tell whether two such sums define the same element of $M\otimes_R N$. The elements of $M\otimes_R N$ of the form $m\otimes n$ are called *decomposable*. Every element of $M\otimes_R N$ is a finite sum of decomposable elements but might not be decomposable itself.

(2) It can be hard to tell whether two elements of $M\otimes_R N$ are equal. For instance, in the $\mathbb{Z}$-module $\mathbb{Q}\otimes_{\mathbb{Z}}\mathbb{Z}/2$, we have

$$1\otimes 1 = 2(\tfrac{1}{2})\otimes 1 = \tfrac{1}{2}\otimes 2 = \tfrac{1}{2}\otimes 0 = 0.$$

In fact $\mathbb{Q}\otimes_{\mathbb{Z}}\mathbb{Z}/2=0$, as we will see.

(3) For a noncommutative ring R, the tensor product $M\otimes_R N$ is defined whenever M is a right R-module and N is a left R-module. In this case, we have the equality

$$(mr)\otimes n = m\otimes(rn).$$

In general (for R noncommutative), the tensor product $M\otimes_R N$ is an abelian group, but not necessarily an R-module. If there is a commutative ring R and a homomorphism from A into the centre of R, then $M\otimes_R N$ is at least an A-module, though.

Exercise. Show that (for R commutative) the tensor product is a functor in each variable. In particular, if $M_1\to M_2$ is an R-linear map, then the tensor product gives an R-linear map $M_1\otimes_R N\to M_2\otimes_R N$. (Hint: use the universal property of tensor products.)

21/10

Theorem 6.2. For all R-modules A, B, and C, there exist isomorphisms:

(1) $A\otimes_R B\xrightarrow{\cong} B\otimes_R A$;

(2) $(A\otimes_R B)\otimes_R C\xrightarrow{\cong} A\otimes_R(B\otimes_R C)$;

(3) $(A\oplus B)\otimes_R C\xrightarrow{\cong}(A\otimes_R C)\oplus(B\otimes_R C)$;

(4) $R\otimes_R A\xrightarrow{\cong} A$.

Proof sketch. The main point is to construct maps in both directions using the universal property of $\otimes$: For (1), for example, we want to try to map $a\otimes b$ to $b\otimes a$, $a\in A$, $b\in B$. By the universal property of $A\otimes_R B$ it suffices to construct an R-bilinear map $A\times B\to B\otimes_R A$; the obvious choice is $(a,b)\mapsto b\otimes a$. But this *is* bilinear, so we get the map we want. Composing this map with the map we obtain in the other direction is the identity on decomposable elements, hence the identity on all elements. ∎

This theorem implies, for instance, that $(R^{\oplus a})\otimes_R(R^{\oplus b})\xrightarrow{\cong} R^{\oplus ab}$ for $a,b\in\mathbb{N}$. Set $M=R^{\oplus a}$ and $N=R^{\oplus b}$. If M is a free R-module with basis $e_1,\dots,e_a$ and N is free with basis $f_1,\dots,f_b$, then $M\otimes_R N$ is a free

R-module with basis elements $e_i \otimes f_j$ for $1 \le i \le a$, $1 \le j \le b$. So every element of $M \otimes_R N$ can be *uniquely* written as a sum

$$\sum_{\substack{1\le i\le a\\ 1\le j\le b}} c_{ij} e_i \otimes f_j.$$

Contrast this with the direct-sum situation: $R^{\oplus a} \oplus R^{\oplus b} \xrightarrow{\cong} R^{\oplus a+b}$.

Lemma 6.3. Let $A \to B \to C \to 0$ be an exact sequence of R-modules. Then for every R-module M, the maps

$$A \otimes_R M \longrightarrow B \otimes_R M \longrightarrow C \otimes_R M \longrightarrow 0$$

form an exact sequence.

(Note that this lemma does not generalise to exact sequences of arbitrary shape!)

Proof sketch. The image $\mathrm{im}(B \otimes_R M \to C \otimes_R M)$ contains all decomposable elements of $C \otimes_R M$ (since the given map $B \to C$ is surjective), so it contains all elements of $C \otimes_R M$.

Clearly the composite map $A \otimes_R M \to B \otimes_R M \to C \otimes_R M$ is 0, because the given map $A \to 0$ is 0. That is, we have the inclusion

$$\mathrm{im}(A \otimes_R M \to B \otimes_R M) \subseteq \ker(B \otimes_R M \to C \otimes_R M).$$

To prove exactness use the universal property of $B \otimes_R M$. ∎

Example. For an element $f \in R$ consider the exact sequence

$$R \xrightarrow{f} R \twoheadrightarrow R/(f) \longrightarrow 0$$

(where the map $R \xrightarrow{f} R$ is 'multiplication by f'). The lemma gives that for any R-module M, we have an isomorphism

$$M \otimes_R R/(f) \cong M/fM.$$

Using that, we can write out what the tensor product of any two finitely generated R-modules over a PID R is. (For this we assume the classification of finitely generated modules over a PID; see Lang's *Algebra* if this is unfamiliar.)

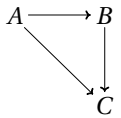
More generally, the lemma implies that for any ring R, if M is an R-module with generators $e_1, \dots, e_a$ and relations $r_i \in R^{\oplus a}$ and N is an R-module with generators $f_1, \dots, f_b$ and relations $s_j \in R^{\oplus b}$, then the tensor product $M \otimes_R N$ is the R-module with generators $e_i \otimes f_j$ ($1 \le i \le a$, $1 \le j \le b$) modulo relations given by $e_i \otimes s_j = 0$ and $r_i \otimes f_j = 0$ (for all i, j that make sense).

6.1 Algebras and tensor products

Definition. For a commutative ring A, an *A-algebra* is a ring B with a given ring homomorphism $A \to B$.

Example. The polynomial ring $k[x_1, \dots, x_n]$ is a k-algebra (and the given homomorphism is the obvious one).

Definition. An *A-algebra homomorphism* $B \to C$ is a ring homomorphism $B \to C$ such that the diagram



commutes.

This definition of morphism makes A-algebras (for a fixed ring A) into a category. It is often more natural to work in the category of k-algebras for a field k, rather than all commutative rings.

Remark. Among noncommutative rings an A-algebra B means A is a commutative ring, B is perhaps noncommutative, and there is a given homomorphism $A \to Z(B)$, the centre of B.

For example, the ring $M_n(k)$ of $n \times n$ matrices over a field k is a k-algebra: the given homomorphism sends an element $a \in k$ to the diagonal matrix aI_n (I_n is the identity matrix). Likewise, for a group G, the group ring kG is a k-algebra.

Back to commutative rings:

For a ring A, the polynomial ring $A[x_1, \ldots, x_n]$ has the following universal property: For every A-algebra B, A-algebra homomorphisms $A[x_1, \ldots, x_n] \to B$ are equivalent to functions $\{1, 2, \ldots, n\} \to B$. We say an A-algebra B is *of finite type* of it is finitely generated as an A-algebra. Equivalently, $B \cong A[x_1, \ldots, x_n]/I$ for some $n \in \mathbb{N}$ and ideal $I \subseteq A[x_1, \ldots, x_n]$.

We say a morphism $X \to Y$ of affine schemes is *of finite type* if the ring $\mathcal{O}(X)$ of regular functions is an algebra of finite type over $\mathcal{O}(Y)$. Equivalently, X is of finite type over Y if X is isomorphic to a closed subspace of $\mathbb{A}^n_Y$ for some $n \in \mathbb{N}$. (*Affine space* $\mathbb{A}^n_Y$ is defined to be $\operatorname{Spec} k[x_1, \ldots, x_n]$ endowed with the Zariski topology.)

Definition. A *closed subscheme* of $\operatorname{Spec}(R)$ is an affine scheme of the form $\operatorname{Spec}(R/I)$.

Example. Suppose k is a field and we have a map $X = \operatorname{Spec}(\mathcal{O}(X)) \to \operatorname{Spec}(k)$. Then the map $X \to \operatorname{Spec} k$ is of finite type if and only if $\mathcal{O}(X)$ is a finitely generated k-algebra, if and only if there is an isomorphism $\mathcal{O}(X) \xrightarrow{\cong} k[x_1, \ldots, x_n]/I$, $n \in \mathbb{N}$, for some ideal I.

Definition. An *affine variety* over a field k is an affine scheme of the form $\operatorname{Spec}(R)$, such that R is a k-algebra of finite type and R is a domain. In particular, an affine variety is irreducible as a topological space.

Example. A^n_k is an affine variety over k for $n \geq 0$. Also, $\{f = 0\} \subseteq A^n_k$ for f an irreducible polynomial in $k[x_1, \ldots, x_n]$ is an affine variety.

If B is an algebra over a ring A, then there is a natural functor from the category B-**Mod** of B-modules to A-**Mod**. Given a ring homomorphism $f\colon A \to B$ and a B-module M, we can view M as an A-module by defining $a \cdot m := f(a)m \in M$ for $a \in A$, $m \in M$.

There is also a less obvious functor, *extension of scalars*, from A-**Mod** to B-**Mod**. For an A-module M, I claim $M \otimes_A B$ is a B-module in a natural way. We define $b_1(m \otimes b_2) = m \otimes b_1 b_2$. Using the universal property of $\otimes$, show this is well defined.

Example. If M if a free A-module of rank n, then $M \otimes_A B$ is a free B-module of rank n (by the basic properties of $\otimes$). More generally, if M has a presentation $M = A\langle e_1, \ldots, e_a \mid r_i \in A^{\oplus a}\rangle$, then $M \otimes_A B = B\langle e_1, \ldots, e_a \mid r_i \in B^{\oplus}\rangle$.

Example. Let M be the $\mathbb{Z}$-module $M = \mathbb{Z}\langle e_1, e_2 \mid 2e_1 = 2e_2\rangle$ ($\cong \mathbb{Z} \oplus \mathbb{Z}/2$). Then we see that

$$M \otimes_{\mathbb{Z}} \mathbb{Q} \cong \mathbb{Z}\langle e_1, e_2 \mid 2e_1 = 2e_2\rangle \cong \mathbb{Q}^2/\mathbb{Q}(2, -2) \cong \mathbb{Q}.$$

And

$$\begin{aligned} M \otimes_{\mathbb{Z}} (\mathbb{Z}/2) &\cong \mathbb{Z}/2\langle e_1, e_2 \mid 2e_1 = 2e_2\rangle \\ &= (\mathbb{Z}/2)^{\oplus 2}/(\mathbb{Z}/2)(2, -2) \cong (\mathbb{Z}/2)^{\oplus 2}. \end{aligned}$$

If B and C are A-algebras, then the tensor product $B \otimes_A C$ is an A-algebra with multiplication defined on decomposable elements: $(b_1 \otimes c_1)(b_2 \otimes c_2) = b_1 b_2 \otimes c_1 c_2$. One checks this is well-defined.

24/10

Examples.

(1) $\mathbb{Q} \otimes_{\mathbb{Z}} (\mathbb{Z}/2) \cong \mathbb{Q}/2\mathbb{Q} = 0$. (For the first isomorphism, recall Lemma 6.3 and the following example.)

(2) For a field k, we have an isomorphism of polynomial rings: $k[x] \otimes_k k[y] \cong k[x, y]$. The obvious map $k[x] \otimes_k k[y] \to k[x, y]$ is an isomorphism since a basis for $k[x] \otimes_k k[y]$ given by the elements $x^i \otimes y^j$, $i \geq 0$, $j \geq 0$, maps to a basis of elements $x^i y^j$ for $k[x, y]$. (Notice that every module over a field is free; i.e., every vector space has a basis.)

Remark. In the Part III Algebraic Geometry course, $\mathbb{A}^n_k$ means k^n with the Zariski topology. Here, $\mathbb{A}^n_k = \operatorname{Spec} k[x_1,\dots,x_n]$ with the Zariski topology. One can actually view k^n as a subset of $\operatorname{Spec} k[x_1,\dots,x_n]$ by the following inclusion:

$$(a_1,\dots,a_n) \mapsto \ker(k[x_1,\dots,x_n] \to k),$$

where the map $k[x_1,\dots,x_n] \to k$ is given by evaluation at $(a_1,\dots,a_n)$. This discrepancy is nothing to worry about, though, because the categories of affine k-varieties for each definition of $\mathbb{A}^n_k$ (for k algebraically closed) are equivalent. For example, in both categories the collection of maps $\mathbb{A}^m_k \to \mathbb{A}^n_k$ consists of k-algebra homomorphisms $k[x_1,\dots,x_n] \to k[x_1,\dots,x_m]$, which are just polynomials $(f_1(x_1,\dots,x_m),\dots,f_n(x_1,\dots,x_m))$ over k.

6.2 Exactness properties of tensor products

We showed (Lemma 6.3) that tensoring an exact sequence

$$A \longrightarrow B \longrightarrow C \longrightarrow 0$$

of R-modules with any R-module M gives an exact sequence. But it's not true that tensoring an exact sequence, e.g.,

$$A \longrightarrow B \longrightarrow C,$$

with M gives an exact sequence in general.

Example. Indeed, consider the product $(0 \longrightarrow \mathbb{Z} \xrightarrow{2} \mathbb{Z}) \otimes_Z (\mathbb{Z}/2)$. The result is a sequence

$$0 \longrightarrow \mathbb{Z}/2 \xrightarrow{2} \mathbb{Z}/2, \qquad (*)$$

but the map $2\colon \mathbb{Z}/2 \to \mathbb{Z}/2$, $x \mapsto 2x$, is just the zero map; so the sequence $(*)$ is not exact since the map $0\colon \mathbb{Z}/2 \to \mathbb{Z}/2$ is not injective.

It turns out to be fruitful to analyse those modules M for which tensoring by M *does* preserve exactness:

Definition. For a ring R, an R-module is *flat* if and only if the functor $N \mapsto M \otimes_R N$ is *exact* (i.e., for an exact sequence $N_1 \to N_2 \to N_3$, the sequence $M \otimes_R N_1 \to M \otimes_R N_2 \to M \otimes_R N_3$ is exact).

Examples. (1) $\mathbb{Z}/2$ is not flat as a $\mathbb{Z}$-module, as we've seen.

(2) Clearly R is flat as an R-module.

(3) Also, the direct sum of any collection of flat modules is flat, since the tensor product $\otimes_R$ is distributive over the direct sum (of even infinitely many modules). So every free R-module is flat.

It sounds like checking flatness will turn out to be quite difficult, as it requires considering many sequences. The following theorem allows us to check only some of those sequences.

Theorem 6.4. If R is a ring and M is an R-module, then the following are equivalent:

(1) M is a flat R-module;

(2) Tensoring with M preserves injections of R-modules;

(3) For any ideal $I \subseteq R$ the R-linear map $M \otimes_R I \to M \otimes_R R \cong M$ is injective.

Proof. That (1) implies (2) is clear from the definition of a flat R-module and the expression of an injection as an exact sequence. That (2) implies (3) is also clear. We will prove that (2) implies (1) and delay the proof that (3) implies (2). (Though there is an elementary proof, it will be easier to prove this after we have introduced the Tor functor: Lemma 10.9.)

Let $N_1 \xrightarrow{f_1} N_2 \xrightarrow{f_2} N_3$ be an exact sequence of R-modules. Then we have an exact sequence

$$N_1 \xrightarrow{f_1} N_2 \xrightarrow{f_2} f_2(N_2) \longrightarrow 0,$$

since f_2 is a surjection onto its image. So we have an exact sequence

$$M \otimes_R N_1 \longrightarrow M \otimes_R N_2 \longrightarrow M \otimes_R f_2(N_2) \longrightarrow 0.$$

Since M satisfies (2), the map $M \otimes_R f_2(N_2) \to M \otimes_R N_3$ is injective. Therefore the sequence

$$M \otimes_R N_1 \longrightarrow M \otimes_R N_2 \longrightarrow M \otimes_R N_3$$

is exact, as the map $M \otimes_R N_2 \longrightarrow M \otimes_R N_3$ factors through $M \otimes_R f_2(N_2)$. ■

Exercise. Using Theorem 6.4, prove the following:

(1) For a domain R, any flat R-module is torsion-free. (By definition, an R-module is *torsion-free* if, for all $r \in R$, $m \in M$, the equation $rm = 0$ implies $r = 0_R$ or $m = 0_M$.)

(2) If R is a PID, then an R-module is flat if and only if it's torsion-free. (e.g., $R = \mathbb{Z}$, $R = k[x]$, ...)

We say an R-algebra A is *flat* if and only if A is flat as an R-module.

7 Localisation

Localising a ring means 'inverting some elements of the ring', and it's related to concentrating attention near a point in a space. The process also generalises passing from a domain R to Frac R, its field of fractions (e.g., $\mathbb{Z} \rightsquigarrow \mathbb{Q}$).

Example. We can think of $\mathbb{C}[x]$ as a ring of functions $\mathbb{C} \to \mathbb{C}$. Its fraction field is called $\mathbb{C}(x)$, the field of rational functions $\frac{f(x)}{g(x)}$, $f, g \in \mathbb{C}[x]$, $g \neq 0$. An element of $\mathbb{C}(x)$ can be viewed as a function $\mathbb{C} \smallsetminus S \to C$ (where S is the finite set of points a where $g(a) = 0$). A typical localisation of $\mathbb{C}[x]$ is the ring of rational functions defined near 0 in $\mathbb{C}$, that is, the set $\left\{\frac{f(x)}{g(x)} : g(0) \neq 0\right\}$.

Definition. A subset S of a ring R is *multiplicatively closed* if it is a submonoid of $(R, \cdot)$; that is, $1 \in S$ and the product of any two elements of S is in S.

Theorem 7.1. Let R be a ring and S a multiplicatively closed subset of R. Then there is a ring $R[S^{-1}]$ with a ring homomorphism $f : R \to R[S^{-1}]$ such that

(1) for every $s \in S$ the image $f(s)$ is invertible in $R[S^{-1}]$;

(2) $R[S^{-1}]$ is universal with respect to property (1): That is, for any ring B and ring homomorphism $g : R \to B$ with the property that all elements of R map to invertible elements of B, there is a unique ring homomorphism $h : R[S^{-1}] \to B$ such that $g = hf$.

Before proving the theorem, we prove that the universal property (2) characterises $R[S^{-1}]$ up to unique isomorphism:

Suppose the rings C_1 and C_2 have properties (1) and (2). Thus we have ring homomorphisms $f_1 : R \to C_1$ and $f_2 : R \to C_2$ such that (1) and (2) hold for both (C_1, f_1) and (C_2, f_2). Then by property (2) there are ring homomorphisms $g_1 : C_1 \to C_2$ and $g_2 : C_2 \to C_1$ such that $f_2 = g_1 f_1$ and $f_1 = g_2 f_2$. You can check that $g_1 g_2$ and $g_2 g_1$ are both identity maps (by the uniqueness part of (2)). (Exercise!) So $g_1 : C_1 \to C_2$ is an isomorphism of rings. It isn't difficult to see that such an isomorphism must be unique.

Sketch of proof of 7.1. Define elements of $R[S^{-1}]$ as 'fractions' $\frac{a}{s}$, $a \in R$, $s \in S$. That is, $R[S^{-1}]$ is the set of equivalence classes for an equivalence relation on $R \times S$.

> (One's first idea for such an equivalence relation might be to say $\frac{a}{s} = \frac{b}{t}$ iff $at = bs$ in R. But this does not define an equivalence relation in general. Indeed, if $(at - bs)u = 0$ in R for some $a, b \in R$, $s, t, u \in S$, then — as u becomes invertible in $R[S^{-1}]$ — we would also have $\frac{a}{s} = \frac{b}{t}$ in $R[S^{-1}]$.)

In general we say that $(a, s) \sim (b, t)$ and write $\frac{a}{s} = \frac{b}{t}$ if $(at - bs)u = 0$ for some $u \in S$. I claim this is an equivalence relation. That it is reflexive and symmetric is obvious. Suppose $\frac{a}{s} = \frac{b}{t}$ and $\frac{b}{t} = \frac{c}{u}$. Then we have $v, w \in S$ such that $(at - bs)v = 0$ and $(bu - ct)w = 0$. Multiplying each side of the first equation by uw and each side of the second by sv, we see that

$$atuvw = bsuvw = cstvw,$$

so $(au - cs)tvw = 0$ in R. But tvw belongs to S, since S is multiplicatively closed. Therefore $\frac{a}{s} = \frac{c}{u}$, which proves the relation is transitive.

So we have a set $R[S^{-1}]$ of equivalence classes of fractions $\frac{a}{s}$, $a \in R$, $s \in S$. One defines addition and multiplication in $R[S^{-1}]$ by the usual rules for fractions:

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

(Note that $st \in S$ since S is multiplicatively closed.) The homomorphism $R \to R[S^{-1}]$ is given by $a \mapsto \frac{a}{1}$. The following exercise completes the proof:

Exercise. Check that these operations are well defined and that they make $R[S^{-1}]$ into a ring. Prove the universal property (2) of this ring $R[S^{-1}]$. ■

26/10

Lemma 7.2. The kernel of the ring homomorphism $R \to R[S^{-1}]$, $a \mapsto \frac{a}{1}$, is the set

$$\{a \in R : as = 0 \text{ for some } s \in S\}.$$

Proof. The equality $\frac{a}{1} = \frac{0}{1}$ in $R[S^{-1}]$ holds if and only if there is some $s \in S$ such that $as = (a \cdot 1 - 0 \cdot 1)s = 0$ in R. ■

Example. Suppose R is a domain and S is a multiplicatively closed subset of $R \smallsetminus \{0\}$. Define the ring $R[S^{-1}]$ to be the *fraction field* $\mathrm{Frac}(R)$. In this case $R \subset \mathrm{Frac}(R)$ by the lemma.

For example, $\mathrm{Frac}(\mathbb{Z}) = \mathbb{Q}$, and $\mathrm{Frac}(k[x_1, \ldots, x_n])$ is called the *field $k(x_1, \ldots, x_n)$ of rational functions over the field k in n variables*. The elements of the field $k(x_1, \ldots, x_n)$ of rational functions are of the form $\frac{f(x_1,\ldots,x_n)}{g(x_1,\ldots,x_n)}$ for $f, g \in k[x_1, \ldots, x_n]$, $g \neq 0$.

More generally, for R a domain and S a multiplicatively closed subset of $R \smallsetminus \{0\}$, we have inclusions $R \subseteq R[S^{-1}] \subseteq \mathrm{Frac}(R)$. So in this case we could define $R[S^{-1}]$ as the subring of $\mathrm{Frac}(R)$ generated by R and the inverses of elements $s \in S$.

But if $0 \in S$ then $R[S^{-1}] = 0$, which is *not* a subring of $\mathrm{Frac}(R)$ (since $1_{\mathrm{Frac}(R)} \notin 0$).

7.1 Special cases of localisation

(1) For a ring R and an element $f \in R$, define

$$R\left[\tfrac{1}{f}\right] := R[S^{-1}] \quad \text{where } S = \{f^n : n \geq 0\}.$$

(2) For a ring R and a prime ideal $\mathfrak{p}$ of R the set $R \smallsetminus \mathfrak{p}$ is multiplicatively closed. (This is exactly what it means for $\mathfrak{p}$ to be prime.) So we can define $R_{\mathfrak{p}} := R[S^{-1}]$, called the *localisation of R at the prime ideal $\mathfrak{p}$*.

Example. For p a prime number, the ring $\mathbb{Z}[1/p]$ is given by

$$\mathbb{Z}\left[\tfrac{1}{p}\right] = \left\{\tfrac{a}{p^c} \in \mathbb{Q} : a \in \mathbb{Z},\ c \geq 0\right\},$$

a subring of $\mathbb{Q}$. And by contrast,

$$\mathbb{Z}_{(p)} = \left\{\tfrac{a}{b} \in \mathbb{Q} : a \in \mathbb{Z},\ b \in \mathbb{Z},\ p \nmid b\right\}.$$

We can also invert elements in polynomial rings. For example, define $k[x, x^{-1}]$ to be the subring $k[x, x^{-1}] = k[x][\frac{1}{x}]$ of $k(x)$, the field of rational functions over k. An element of $k[x, x^{-1}]$ is a rational function that can be written as $\frac{f(x)}{x^c}$ for some $f \in k[x]$, $c \geq 0$. Equivalently, $k[x, x^{-1}]$ is the ring of Laurent polynomials

$$a_{-n}x^{-n} + \cdots + a_n x^n, \quad a_i \in k.$$

Thus an element of $\mathbb{C}[x, x^{-1}]$ can be viewed as a function $\mathbb{C} \smallsetminus \{0\} \to \mathbb{C}$, whereas $\mathbb{C}[x]_{(x)}$ is the ring of rational functions defined on some neighbourhood of 0.

7.2 Local rings

Definition. A ring R is *local* if it has exactly one maximal ideal $\mathfrak{m}$. The field $R/\mathfrak{m}$ is called the *residue field* of R.

We will often use the following characterisation of local rings to prove that a ring is local.

Lemma 7.3. A ring R is local if and only if the nonunits in R form an ideal.

Proof. Suppose R is local with maximal ideal $\mathfrak{m}$. If $a \in \mathfrak{m}$ then a is not a unit; else we would have $aa^{-1} = 1 \in \mathfrak{m}$. Conversely, if $a \in R \smallsetminus \mathfrak{m}$ then a is a unit, as we'll show. Suppose for a contradiction that $(a) \neq R$. Then (a) must be contained in some (the only) maximal ideal. But then $(a) \subseteq \mathfrak{m}$, which contradicts our assumption that $a \in R \smallsetminus \mathfrak{m}$. So the non units in R are exactly the elements of $\mathfrak{m}$, which is an ideal.

For the other implication, suppose the set I of nonunits in R forms an ideal. Then $I \neq R$ since $1 \notin I$. And if J is any ideal strictly larger than I, then J contains some unit, so $J = R$. So I is maximal. If $\mathfrak{m} \neq I$ were some maximal ideal distinct from I, then there would be some element of $\mathfrak{m}$ that wasn't an element of I; that element would have to be a unit, which would guarantee that $\mathfrak{m} = R$, a contradiction. Therefore there is no such $\mathfrak{m}$, and I is the only maximal ideal in R. ∎

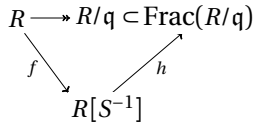
Exercise. For a field k and a positive integer n, the power series ring $k[\![x_1, \ldots, x_n]\!]$ is a local ring. Prove this using the lemma (7.3). Recall an element of $k[\![x_1, \ldots, x_n]\!]$ is an infinite formal sum $\sum_{i_j \geq 0} a_{i_1 \cdots i_n} x_1^{i_1} \cdots x_n^{i_n}$, $a_{i_1 \cdots i_n} \in k$.

Theorem 7.4. Let R be a ring and S a multiplicatively closed subset of R. Then the prime ideals in $R[S^{-1}]$ are in one-to-one correspondence with prime ideals $\mathfrak{p} \subset R$ such that $\mathfrak{p} \cap S = \varnothing$.

Proof. Write $f\colon R \to R[S^{-1}]$ for the ring homomorphism given by the localisation. This induces a (continuous) map of spectra $g\colon \operatorname{Spec} R[S^{-1}] \to \operatorname{Spec} R$ that sends a prime ideal $\mathfrak{p}$ in $R[S^{-1}]$ to its preimage $f^{-1}(\mathfrak{p})$ in R. (cf. Theorem 1.9.) We will show that, for every prime ideal $\mathfrak{p}$ in $R[S^{-1}]$, the intersection $f^{-1}(\mathfrak{p}) \cap S$ is empty. If $s \in S \cap f^{-1}(\mathfrak{p})$, then $f(s) \in \mathfrak{p}$ and $f(s)$ is also a unit in $R[S^{-1}]$; this is impossible since the prime ideal $\mathfrak{p}$ contains no units.

Next we'll show that the map $g\colon \operatorname{Spec} R[S^{-1}] \to \operatorname{Spec} R$ is injective. That is, a prime ideal $\mathfrak{p} \subset R[S^{-1}]$ is determined by its preimage $f^{-1}(\mathfrak{p}) \subset R$. For elements $a \in R$ and $s \in S$, the fraction $\frac{a}{s}$ belongs to $\mathfrak{p}$ if and only if $\frac{a}{1} \in \mathfrak{p}$ since s is a unit in $R[S^{-1}]$. But this is true if and only if $a \in f^{-1}(\mathfrak{p})$ in R. So the prime ideal $\mathfrak{p} \subset R[S^{-1}]$ is determined by its preimage $f^{-1}(\mathfrak{p})$. That is, the map g is injective.

It remains to show that for every prime ideal $\mathfrak{q} \subset R$ disjoint from S, there is a prime ideal $\mathfrak{p} \subset R[S^{-1}]$ such that $f^{-1}(\mathfrak{p}) = \mathfrak{q}$. Consider the diagram



We can construct a ring homomorphism $h\colon R[S^{-1}] \to \operatorname{Frac}(R/\mathfrak{q})$ as shown that makes the diagram commute if and only if the elements of S map to units in $\operatorname{Frac}(R/\mathfrak{q})$ (by the universal property of $R[S^{-1}]$). The elements of S do map to units in the quotient $\operatorname{Frac}(R/\mathfrak{q})$, since $\mathfrak{q} \cap S = \varnothing$. Defining $p := \ker h$, we see that $\mathfrak{p}$ is a prime ideal of $R[S^{-1}]$. We want to show that $f^{-1}(\mathfrak{p}) = \mathfrak{q}$. For an element $a \in R$, we have $a \in f^{-1}(\mathfrak{p})$ if and only if $f(a) \in \mathfrak{p}$, if and only if $h(fa) = 0$ in $\operatorname{Frac}(R/\mathfrak{q})$. This occurs if and only if $a = 0$ in $R/\mathfrak{q}$, since the inclusion $R/\mathfrak{q} \hookrightarrow \operatorname{Frac}(R/\mathfrak{q})$ is injective. But this is equivalent to $a \in \mathfrak{q}$, and so $f^{-1}(\mathfrak{p}) = \mathfrak{q}$, as desired. ∎

Notice that the correspondence described by Theorem 7.4 is compatible with inclusion: if $\mathfrak{p}$ and $\mathfrak{q}$ are prime ideals in R disjoint from S and $\mathfrak{p} \subseteq \mathfrak{q}$, then the inclusion $f^{-1}(\mathfrak{p}) \subseteq f^{-1}(\mathfrak{q})$ certainly also holds.

Corollary 7.5. The localisation of any ring R at any prime ideal $\mathfrak{p}$ is a local ring.

Proof. The prime ideals in $R_{\mathfrak{p}}$ are in one-to-one correspondence with the prime ideals in R that are contained in $\mathfrak{p}$. In this collection of prime ideals, there is a unique maximal element $\mathfrak{p} \subset R$. So $R_{\mathfrak{p}}$ has a unique maximal ideal. ∎

(Explicitly, this maximal ideal is the extended ideal $\mathfrak{p}R_{\mathfrak{p}}$.)

Example. (1) Any field is a local ring.

(2) The rings $\mathbb{Z}_{(p)}$ for a prime number p and the polynomial ring $k[x]_{(x)}$ are local rings. The residue fields of these two local rings are $\mathbb{Z}/(p)$ and k, respectively.

(3) More generally, for any ring R and any prime ideal $\mathfrak{p}$ in R, the residue field of the local ring $R_{\mathfrak{p}}$ is $\mathrm{Frac}(R/\mathfrak{p})$, as you can check (Exercise!).

Exercise. Describe which rational functions are in the local ring $\mathbb{C}[x,y]_{(x)}$. The residue field of $\mathbb{C}[x,y]_{(x)}$ is $\mathbb{C}(y)$; try to say 'geometrically' what the restriction map $\mathbb{C}[x,y]_{(x)} \twoheadrightarrow \mathbb{C}(y)$ is.

In general $R[S^{-1}]$ need not be a local ring.

Exercise. Show $\mathbb{Z}[1/p]$ is not local.

Definition. For a ring R and an element $f \in R$, a subset of $\mathrm{Spec}\, R$ of the form

$$D(f) := \mathrm{Spec}(R) \smallsetminus V((f)) = \{f \neq 0\}$$

is called a *standard open subset* of $\mathrm{Spec}\, R$.

Exercise. Show that the (continuous) map $\mathrm{Spec}[1/f] \to \mathrm{Spec}\, R$ is a homeomorphism onto its image. Show that the image is the standard open set $D(f) \subseteq \mathrm{Spec}(R)$.

Remark. One says a *regular function* on $\{f \neq 0\} \subseteq \mathrm{Spec}(R)$ is exactly an element of $R[1/f]$.

28/10 Insert Pictures.

7.3 Localisation of modules

Let R be a ring, $S \subseteq R$ a multiplicatively closed subset of R, and M an R-module. We define an $R[S^{-1}]$-module $M[S^{-1}]$ in the following way: elements of $M[S^{-1}]$ are written $\frac{m}{s}$, $m \in M$, $s \in S$, and we say that $\frac{m}{s} = \frac{n}{t}$ if there is an element $u \in S$ such that $u(tm - sn) = 0$. This defines an equivalence relation on $M \times S$, so it defines a set $M[S^{-1}]$ of equivalence classes. Addition and multiplication of elements of $M[S^{-1}]$ are defined by the obvious formulas:

$$\frac{m}{s} + \frac{n}{t} = \frac{tm+sn}{st}; \qquad \frac{m}{s} \cdot \frac{n}{t} = \frac{ms}{nt}.$$

In particular, we have $M[\frac{1}{f}]$ for $f \in R$ and $M_{\mathfrak{p}}$ for a prime ideal $\mathfrak{p}$ of R.

An R-linear map $f\colon M \to N$ gives an $R[S^{-1}]$-linear map $f[S^{-1}]\colon M[S^{-1}] \to N[S^{-1}]$ defined by

$$f[S^{-1}]\colon \frac{m}{s} \mapsto \frac{f(n)}{s}.$$

This makes the assignment $M \mapsto M[S^{-1}]$ into a functor from the category R-**Mod** of R-modules to the category $R[S^{-1}]$-**Mod** of $R[S^{-1}]$-modules.

Theorem 7.6. The functor $M \mapsto M[S^{-1}]$ is exact. That is, if $M_1 \xrightarrow{f_1} M_2 \xrightarrow{f_2} M_3$ is an exact sequence of R-modules, then the induced sequence

$$M_1[S^{-1}] \xrightarrow{f_1[S^{-1}]} M_2[S^{-1}] \xrightarrow{f_2[S^{-1}]} M_3[S^{-1}]$$

is exact.

Proof. Since $gf = 0$ the map $g[S^{-1}]f[S^{-1}]$ is also zero (because $M \mapsto M[S^{-1}]$ is a functor). That is, an element $\frac{m}{s} \in M_1[S^{-1}]$ maps first to $\frac{f(m)}{s}$ in $M_2[S^{-1}]$, and then to $\frac{g(f(m))}{s} = \frac{0}{s} = \frac{0}{1}$ in $M_3[S^{-1}]$. Thus we have proven the containment $\mathrm{im}\, f_1[S^{-1}] \subseteq \ker f_2[S^{-1}]$.

Suppose an element $\frac{m}{s} \in M_2[S^{-1}]$ maps to $0 \in M_3[S^{-1}]$ (under $f_2[S^{-1}]$). That is, $\frac{g(m)}{s} = 0$ in $M_3[S^{-1}]$, so there is an element $t \in S$ such that $tg(m) = 0$. Since g is R-linear, it must be that $g(tm) = 0$ in M_3. By the exactness of the first sequence at M_2, there is an element $m_1 \in M_1$ such that $f(m_1) = tm$. Then $f_1[S^{-1}]$ maps the element $\frac{m_1}{st}$ in $M_1[S^{-1}]$ to the element $\frac{f(m_1)}{st} = \frac{tm}{st} = \frac{m}{s}$ in $M_2[S^{-1}]$. Therefore $\mathrm{im}\, f_1[S^{-1}] = \ker f_2[S^{-1}]$, q.e.d. ∎

Theorem 7.7. Let R be a ring, S a multiplicatively closed subset of R, and M and R-module. Then there is an isomorphism of $R[S^{-1}]$-modules

$$M \otimes_R R[S^{-1}] \xrightarrow{\cong} M[S^{-1}].$$

Proof. Omitted. See Atiyah–MacDonald or check it yourself. ∎

Corollary 7.8. For every ring R and multiplicatively closed subset $S \subseteq R$, the localisation $R[S^{-1}]$ is a flat R-algebra.

Proof. Apply Theorems 7.6 and 7.7. ∎

Example. Let M be the $\mathbb{Z}$-module

$$M = \mathbb{Z}^{\oplus 2} \oplus \mathbb{Z}/2 \oplus \mathbb{Z}/8 \oplus \mathbb{Z}/5.$$

The localisation of M at the prime ideal $(0) \subset \mathbb{Z}$ is $M \otimes_{\mathbb{Z}} \mathbb{Q} \cong \mathbb{Q}^2$, since $\mathbb{Q} = \mathbb{Z}_{(0)}$.

The localisation of M at the prime $(2) \subset \mathbb{Z}$ is given by:

$$M \otimes_{\mathbb{Z}} \mathbb{Z}_{(2)} = (\mathbb{Z}_{(2)})^{\oplus 2} \oplus \mathbb{Z}/2 \oplus \mathbb{Z}/8.$$

Another example:

$$M_{(5)} \cong (\mathbb{Z}_{(5)})^{\oplus 2} \oplus \mathbb{Z}/5.$$

For a prime number not equal to 2 or 5, we have

$$M_{(p)} \cong (\mathbb{Z}_{(p)})^{\oplus 2}.$$

Definition. We say a property P of rings R is *local* if R has property P if and only if all localisations of R at prime ideals $\mathfrak{p}$ have the same property.

Likewise, we say a property P of R-modules M is *local* if M has property P if and only if $M_{\mathfrak{p}}$ has property P for every prime ideal $\mathfrak{p} \subset R$.

Lemma 7.9. Let R be a ring and M an R-module. Then the following are equivalent:

(1) $M = 0$;

(2) $M_{\mathfrak{p}} = 0$ for every prime ideal $\mathfrak{p} \subset R$;

(3) $M_{\mathfrak{m}} = 0$ for every maximal ideal $\mathfrak{m} \subset R$.

That is, being 0 is a local property of R-modules.

Proof. The implication (1)⇐(2) is easy, and the implication (2)⇐(3) is trivial.

Suppose M is a nonzero R-module and that x is a nonzero element of M. Let I be the annihilator $\mathrm{Ann}_R(x)$ in R of x, an ideal of R. Note $I \neq R$ since $1 \cdot x \neq 0 \in M$. So I is contained in some maximal ideal $\mathfrak{m} \subset R$. We will show that $x \neq 0$ in $M_{\mathfrak{m}}$. If the equation $\frac{x}{1} = \frac{0}{1}$ holds in $M_{\mathfrak{m}}$, then there is some $s \in R \smallsetminus \mathfrak{m}$ such that $sx = 0$. But then $s \in \mathrm{Ann}_R(x) = I \subseteq \mathfrak{m}$, a contradiction. So in fact $M_{\mathfrak{m}} \neq 0$. ∎

Lemma 7.10. Let R be a ring and $f\colon M \to N$ an R-linear map. The following are equivalent:

(1) f is injective;

(2) f is locally injective: $f_{\mathfrak{p}}\colon M_{\mathfrak{p}} \to N_{\mathfrak{p}}$ is injective for every prime ideal $\mathfrak{p} \subset R$;

(3) $f_{\mathfrak{m}}\colon M_{\mathfrak{m}} \to N_{\mathfrak{m}}$ is injective for every maximal ideal $\mathfrak{m} \subset R$.

Likewise for f 'surjective' or 'an isomorphism'.

Proof. By Theorem 7.7 we can identify $M_{\mathfrak{p}}$ with $M \otimes_R R_{\mathfrak{p}}$. Then the implication (1)⇐(2) holds since $R_{\mathfrak{p}}$ is flat over R. Again, (3) is a special case of (2), so we need only prove that (3) implies (1).

Let $f\colon M \to N$ be an R-linear map such that $f_{\mathfrak{m}}\colon M_{\mathfrak{m}} \to N_{\mathfrak{m}}$ is injective for every maximal ideal $\mathfrak{m} \subset R$. Let $K = \ker f$. We have an exact sequence

$$0 \longrightarrow K \longrightarrow M \xrightarrow{f} N$$

of R-modules. Since localisation is an exact functor (Theorem Theorem 7.6), we have a corresponding exact sequence

$$0 \longrightarrow K_{\mathfrak{m}} \longrightarrow M_{\mathfrak{m}} \xrightarrow{f_{\mathfrak{m}}} N_{\mathfrak{m}}$$

for every maximal ideal $\mathfrak{m} \subset R$. Here $f_{\mathfrak{m}}$ is injective, so $K_{\mathfrak{m}} = 0$ (by exactness). The previous lemma (7.9) guarantees that K must be 0. That is, f is injective.

A similar proof applies when f is surjective or an isomorphism. ∎

Flatness is also a local property of R-modules:

Lemma 7.11. Let R be a ring and M an R-module. The following are equivalent:

(1) M is a flat R-module;

(2) $M_\mathfrak{p}$ is a flat $R_\mathfrak{p}$-module for every prime ideal $\mathfrak{p} \subset R$;

(3) $M_\mathfrak{m}$ is a flat $R_\mathfrak{m}$-module for every maximal ideal $\mathfrak{m} \subset R$.

Proof. First note that flatness is preserved by any extension of scalars: If $R \to S$ is a ring homomorphism and M is a flat R-module, then the extended module $M \otimes_R S$ is a flat S-module. (To prove this, prove that $(M \otimes_R S) \otimes_S N \cong M \otimes_R (S \otimes_R N) = M \otimes_R N$ for any S-module N. Exercise!) So if M is a flat R-module, then $M_\mathfrak{p} = M \otimes_R R_\mathfrak{p}$ is a flat $R_\mathfrak{p}$-module for every prime $\mathfrak{p} \subset R$. This proves that (1) implies (2).

As usual, (3) is a special case of (2).

Suppose M is an R-module such that $M_\mathfrak{m}$ is a flat $R_\mathfrak{m}$-module for every maximal ideal $\mathfrak{m} \subset R$. By Theorem 6.4, it suffices to show that tensoring with M preserves injectivity. Let $A \to B$ be an injective R-linear map. We want to show that the induced map $A \otimes_R M \to B \otimes_R M$ is injective. We know that $A_\mathfrak{m} \to B_\mathfrak{m}$ is injective for every maximal ideal $\mathfrak{m} \subset R$, since localisation defines an exact functor. Since $M\mathfrak{m}$ is a flat $R_\mathfrak{m}$-module, the map $A_\mathfrak{m} \otimes_{R_\mathfrak{m}} M_\mathfrak{m} \to B_\mathfrak{m} \otimes_{R_\mathfrak{m}} M_\mathfrak{m}$ is injective for every maximal ideal $\mathfrak{m} \subset R$. You can check (Exercise!) that this map is the localisation at $\mathfrak{m}$ of the map $A \otimes_R M \to B \otimes_R M$. By the previous lemma, the map $A \otimes_R M \to B \otimes_R M$ is injective. So M is R-flat. ∎

7.4 Nakayama's Lemma

Lemma 7.12 (Nakayama's Lemma)**.** Let M be a finitely generated module over a local ring R with maximal ideal $\mathfrak{m}$. If $M \otimes_R (R/\mathfrak{m}) = 0$, then $M = 0$.

Proof. We have $0 = M \otimes_R (R/\mathfrak{m}) = M/(\mathfrak{m}M)$ (Why?!!!). That is, we have $\mathfrak{m}M = M$. Suppose $M \neq 0$ and let $x_1, \ldots, x_n$ be a set of generators for M as an R-module, with n as small as possible. Then $x_n \in \mathfrak{m}M$, so x_n can be written as:

$$x_n = a_1 x_1 + a_2 x_2 + \cdots + a_n x_n$$

with the a_i in the maximal ideal $\mathfrak{m}$. Rearranging, we have the equation

$$(1 - a_n) x_n = a_1 x_1 + \cdots + a_{n-1} x_{n-1}. \qquad (\dagger)$$

But $1 - a_n$ does not belong to $\mathfrak{m}$ (since $1 = 1 - a_n + a_n$ does not belong to $\mathfrak{m}$), so $1 - a_n$ is a unit in the local ring R. Multiplying each side of (†) by $(1 - a_n)^{-1}$ thus shows that $x_n \in Rx_1 + \cdots + Rx_{n-1}$. But then M is generated as an R-module by the $n-1$ elements $x_1, \ldots, x_{n-1}$, a contradiction. Therefore $M = 0$. ∎

31/10

Example. Beware: Nakayama's lemma fails for non-finitely generated modules over a local ring. Let $R = \mathbb{Z}_{(2)} = \left\{\frac{a}{b} : b \text{ odd}\right\}$, $M = \mathbb{Q}$. Then M is a non-finitely generated R-module. Here $M \neq 0$ but

$$M \otimes_{\mathbb{Z}_{(2)}} \mathbb{Z}/2 = M \otimes_{\mathbb{Z}_{(2)}} \mathbb{Z}_{(2)}/2\mathbb{Z}_{(2)} = M/2M = \mathbb{Q}/2Q = 0.$$

Corollary 7.13 (of Lemma 7.12)**.** Let M be a finitely generated module over a local ring R. Then the elements $x_1, \ldots, x_n$ generate M as an R-module if and only if the images of $x_1, \ldots, x_n$ span the $R/\mathfrak{m}$-vector space $M \otimes_R R/\mathfrak{m} (= M/\mathfrak{m}M)$.

Proof. The 'only if' implication $\Rightarrow$ is trivial.

Suppose that the images of $x_1, \ldots, x_n \in M$ span the $R/\mathfrak{m}$-vector space $M/\mathfrak{m}M$. Let Q be the quotient of M by the R-submodule generated by $x_1, \ldots, x_n$. We want to show that Q is 0 as an R-module. Clearly Q is a finitely generated R-module, so by Nakayama $Q = 0$ if we have $Q \otimes_R R/\mathfrak{m} = 0$. We have an exact sequence

$$R^{\oplus n} \longrightarrow M \longrightarrow Q \longrightarrow 0$$

where the map $R^{\oplus n} \longrightarrow M$ is given by sending the ith generator of $R^{\oplus n}$ to x_i. This induces an exact sequence of modules

$$(R/\mathfrak{m})^{\oplus n} \twoheadrightarrow M \otimes_R R/\mathfrak{m} \longrightarrow Q \otimes_R R/\mathfrak{m} \longrightarrow 0,$$

where the first map is surjective by assumption. Therefore $Q \otimes_R R/\mathfrak{m} = 0$. ∎

Remark. (1) Why is $\mathbb{Z}/8 \otimes_{\mathbb{Z}} \mathbb{Z}_{(2)} \cong \mathbb{Z}/8$? (Recall Example 7.3.) Because all the elements of $S = \mathbb{Z} \smallsetminus (2)$ act invertibly on $\mathbb{Z}/8$, so $(\mathbb{Z}/8)[S^{-1}] \cong \mathbb{Z}/8$. (If $m \in \mathbb{Z}/8$ and $s \in \mathbb{Z} \smallsetminus (2)$, then $\frac{m}{s} \in (\mathbb{Z}/8)[S^{-1}]$ is equal to the element $y \in \mathbb{Z}/8$ such that $sy = m$.)

(2) Notation: $M \overset{f}{\twoheadrightarrow} N$ means f is surjective; $M \overset{f}{\hookrightarrow} N$ means f is injective.

8 Noetherian rings[2]

Definition. A ring R is *noetherian* if every sequence $I_1 \subseteq I_2 \subseteq \cdots$ of ideals in R terminates; that is, there is $N > 0$ such that $I_N = I_{N+1} = \cdots$.

We say R satisfies the *ascending chain condition* (ACC) on ideals in this case. A ring R is *artinian* if it satisfies the *descending chain condition* (DCC) on ideals.

Theorem 8.1. Let R be a ring. The following are equivalent:

(1) R is noetherian (ie, R satisfies ACC for ideals);

(2) every ideal in R is finitely generated.

Proof. First suppose that R is noetherian and suppose I be an ideal in R that is not finitely generated. Then $I \neq 0$, so pick a nonzero element $x_1 \in I$. Then $I \neq (x_1)$ since I is not finitely generated, so can pick $x_2 \in I \smallsetminus (x_1)$. Then $I \neq (x_1, x_2)$, so pick $x_3 \in I \smallsetminus (x_1, x_2)$. Repeat. We get an infinitely increasing sequence of ideals:

$$0 \subsetneq (x_1) \subsetneq (x_1, x_2) \subsetneq \cdots \subsetneq R.$$

This is a contradiction, so I is finitely generated.

Conversely, suppose every ideal in R is finitely generated. Let $I_1 \subseteq I_2 \subseteq \cdots$ be a chain of ideals in R. Let $J = \bigcup_n I_n$, which is an ideal. By assumption J is finitely generated as an ideal: say $J = (x_1, \ldots, x_n)$. Each x_i belongs to some I_j, so, taking the max of these finitely many js, there is a $j > 0$ such that $x_1, \ldots, x_n \in I_j$. So $J = I_j$, whence the sequence terminates: $I_j = I_{j+1} = I_{j+2} = \cdots$. ∎

Examples. (1) Every field is noetherian and artinian.

(2) The ring $\mathbb{Z}$ is noetherian but not artinian. It's not artinian since it contains the strictly decreasing chain

$$(2) \supsetneq (4) \supsetneq (8) \supsetneq \cdots.$$

Every PID is noetherian, since every ideal is generated by one element. So likewise the polynomial ring $k[x]$, for k a field, is noetherian but not artinian. (Exercise!)

(3) The polynomial ring $k[x_1, x_2, \ldots]$ in countably many variables is neither noetherian nor artinian. The chain of ideals

$$0 \subsetneq (x_1) \subsetneq (x_1, x_2) \subsetneq (x_1, x_2, x_3) \subsetneq \cdots$$

shows that it's not noetherian. But $R = k[x_1, x_2, \ldots]$ is a domain, so R is contained in its fraction field $\operatorname{Frac} R$, which is, of course, noetherian. Thus a subring of a noetherian ring need not be noetherian.

(4) Later we'll show that every artinian ring is noetherian: Theorem 12.4.

Lemma 8.2. Any quotient ring of a noetherian ring is noetherian. Likewise for artinian rings.

Proof. Let R be a noetherian ring and I an ideal of R. There is a one-to-one order-preserving correspondence between ideals in R/I and ideals in R containing I. ∎

Theorem 8.3 (Hilbert's Basis Theorem[3])**.** If R is noetherian, then $R[x]$ is noetherian.

[2] Due to Emmy Noether, 1882–1935.

[3] David Hilbert, 1862–1943

Corollary 8.4. If R is noetherian (for example, a field), then any algebra of finite type over R is noetherian.

Proof of corollary. The ring $R[x_1,\dots,x_n] = R[x_1][x_2]\cdots[x_n]$ is noetherian for R noetherian by induction on n. An R-algebra of finite type is isomorphic to $R[x_1,\dots,x_n]/I$ for some ideal I. ∎

This corollary gives us an important example of a noetherian ring: the polynomial ring $k[x_1,\dots,x_n]$ over a field k.

Proof of the Hilbert Basis Theorem. Let R be a noetherian ring. We'll show that any ideal I in $R[x]$ is finitely generated as an ideal. For each $j \in \mathbb{N}$ let I_j be the set of elements $a \in R$ such that there is an element of I of the form $ax^j +$ [lower-degree terms]. (That is, I_j is the set of elements of R that appear as leading coefficients of degree-j members of I.) Since I is an ideal in $R[x]$, it is easy to check that each I_j is an ideal in R. We have a chain of ideals

$$I_0 \subseteq I_1 \subseteq I_2 \subseteq \cdots \subseteq R,$$

since multiplying an element of $I \subseteq R[x]$ by x gives an element of I. Because R is noetherian this sequence of ideals terminates: there is $N \in \mathbb{N}$ such that $I_N = I_{N+1} = \cdots$. For each $j = 0,\dots,N$ choose finitely many generators for the ideal I_j: $I_j = (f_{j,1},\dots,f_{j,m_j}) \subseteq R$. Then for each of these finitely many elements $f_{j,k}$ in R we can choose an element $g_{j,k} \in I$ of the form

$$g_{j,k} = f_{j,k}x^j + \text{ [lower-degree terms]}.$$

We claim I is generated by the finitely many elements $g_{j,k}$, $1 \le k \le m_j$, $0 \le l \le N$. Let h be an element of I. We want to show that h is an $R[x]$-linear combination of the $g_{j,k}$s. Using induction on $\deg h$, we need only prove that we can subtract from h some $R[x]$-linear combination of the $g_{j,k}$s to get something of degree less than $\deg h$.

If $\deg h = d \le N$, then we can subtract some linear combination of $g_{d,1}, g_{d,2},\dots$ from h to get something of degree $< d$. If $d = \deg h > N$, then we can subtract from h the product of x^{d-N} with some R-linear combination of the $g_{N,i}$s to get something of degree less than d, since in this case $I_d = I_N = (f_{N,1},\dots,f_{N,m_N})$. We conclude that I is finitely generated. ∎

Lemma 8.5. Let R be noetherian and $S \subseteq R$ a multiplicatively closed subset of R. Then the localised ring $R[S^{-1}]$ is noetherian.

Proof. Let $\pi\colon R \to R[S^{-1}]$ be the natural ring homomorphism. Then for any ideal $I \subseteq R[S^{-1}]$, we have $I = (p^{-1}(I))\cdot R[S^{-1}]$. (Indeed, if $\frac{r}{f} \in I$, then $\frac{r}{1} \in I$, so $r \in \pi^{-1}(I)$. Therefore every element of I is the product of an element of $\pi^{-1}(I)$ and $\frac{1}{s} \in R[S^{-1}]$.) So if I is any ideal in $R[S^{-1}]$, then $\pi^{-1}(I) \subseteq R$ is finitely generated; say $\pi^{-1}(I) = (x_1,\dots,x_m) \subseteq R$. Then I is generated by the images $x_1,\dots,x_m$ as an ideal of $R[S^{-1}]$. ∎

2/11

Definition. Let R be a ring. An R-module M *satisfies ACC on R-submodules* if any sequence of R-submodules $M_1 \subseteq M_2 \subseteq M_3 \subseteq \cdots$ terminates.

Example. A ring R is noetherian if and only if R satisfies ACC on R-submodules.

Lemma 8.6. Let

$$0 \longrightarrow A \xrightarrow{\alpha} B \xrightarrow{\beta} C \longrightarrow 0$$

be an exact sequence of R-modules. Then B satisfies ACC on R-submodules if and only if both A and C do.

Proof. Exercise! Or see Atiyah–MacDonald, which offers (a condensed version of) the following proof (6.5i):

An ascending chain of submodules in A or C gives rise to an ascending chain in B, hence terminates. This proves the 'only if' implication.

Let $(L_n)_{n\ge1}$ be an ascending chain of submodules in B. Then $(\alpha^{-1}(L_n))_{n\ge1}$ is an ascending chain of submodules in A, and $(\beta(L_n))_{n\ge1}$

is an ascending chain of submodules in C. Each of these chains terminates, so for sufficiently large n we have $\alpha^{-1}(L_n) = \alpha^{-1}(L_{n+1}) = \cdots$ and $\beta(L_n) = \beta(L_{n+1}) = \cdots$.

$\vdots$

■

Corollary 8.7. Let R be a noetherian ring and M a finitely generated R-module. Then every R-submodule of M is finitely generated as an R-module. Also, M satisfies ACC on R-submodules.

Proof. We know R satisfies ACC for R-submodules. So by the lemma (8.6) the free module $R^{\oplus n}$ satisfies ACC on R-submodules for every $n \in \mathbb{N}$. By the lemma, any finitely generated R-module also satisfies ACC for submodules, as it is a quotient module of $R^{\oplus n}$ for some n.

This implies that any submodule $N \subseteq M$ is finitely generated by a proof very similar to the one we used for ideals. (Which theorem? Which proof?!) ■

Next we discuss why noetherian rings are useful geometrically.

8.1 Decomposition of irreducible closed subsets

Theorem 8.8. Let R be a noetherian ring. Then $\operatorname{Spec}(R)$ can be written as a finite union of irreducible closed subsets:

$$\operatorname{Spec}(R) = X_1 \cup X_2 \cup \cdots \cup X_m,$$

with no X_i contained in any X_j for $i \neq j$. Moreover, this decomposition is unique up to the order of $X_1, \ldots, X_m$.

The subsets X_i in the statement of the theorem are called the *irreducible components* of $X = \operatorname{Spec}(R)$. Note that any closed subset of $\operatorname{Spec}(R)$ can be viewed (recall Theorem 1.9) as $\operatorname{Spec}(R/I)$ for some ideal I, so any closed subset of $\operatorname{Spec}(R)$ has a similar decomposition with the same properties.

The idea here is that we're (vaguely) generalising unique factorisation in $\mathbb{Z}$: every ideal is related to a finite list of primes. In the case $R = \mathbb{Z}$ the irreducible components of the closed set $\{n = 0\} = \operatorname{Spec}(\mathbb{Z}/n) \subseteq \operatorname{Spec}(\mathbb{Z})$ (for $n \in \mathbb{Z} \smallsetminus \{0\}$) are the sets $\operatorname{Spec}(\mathbb{Z}/p)$ for the prime divisors p of n.

Since the closed subsets of $\operatorname{Spec}(R)$ correspond to radical ideals in R, we can state the theorem purely algebraicly:

Corollary 8.9. Suppose R is noetherian and I is an ideal of R. Then the ideal $\operatorname{rad} I$ is a finite intersection of prime ideals:

$$\operatorname{rad} I = \mathfrak{p}_1 \cap \cdots \cap \mathfrak{p}_m$$

for some $m > 0$ and some prime ideals $\mathfrak{p}_n$, where $\mathfrak{p}_i \neq \mathfrak{p}_j$ for $i \neq j$.

These ideals are exactly the minimal ideals that contain I. (cf. Example Sheet 1, Question 12.)

Proof of Theorem 8.8. Let $X = \operatorname{Spec}(R)$. Since R is noetherian, R (in particular) satisfies the ACC for radical ideals, so X satisfies the DCC for closed subsets: if we have a sequence $X \subseteq X_1 \subseteq X_2 \subseteq \cdots$ of closed subsets of X, then the sequence terminates.

Suppose X cannot be written as a finite union of irreducible closed subsets. Then $X \neq \varnothing$ (otherwise we'd be done with $m = 0$). Also X is not irreducible; otherwise we'd be done with $m = 1$. So we can write $X = Y_1 \cup Z_1$ for some closed proper subsets Y_1, Z_1 of X. At least one of Y_1, Z_1 cannot be written as a finite union of irreducible closed subsets; say it's Y_1. Then $Y_1 \neq \varnothing$ and Y_1 is not irreducible, so we can write $Y_1 = Y_2 \cup Z_2$ for some pair Y_2, Z_2 of proper closed subsets of Y_1. We can assume that Y_2 is not a finite union of closed irreducible subsets. Repeat to get a strictly decreasing sequence of closed subsets of X:

$$X \supsetneq Y_1 \supsetneq Y_2 \supsetneq \cdots,$$

a contradiction.

Proof of uniqueness of such a decomposition is left as an exercise. ■

This theorem gives a rough description of ideals and modules over a noetherian ring, but there can be many ideals with the same radical.

Example. Let $R = \mathbb{C}[x,y]$ and let I be an ideal of R with $\operatorname{rad} I = (x,y)$. (Think of the ideal (x,y) as the ideal of functions that vanish at $0 \in \mathbb{C}$.) Equivalently, there is some $N > 0$ such that

$$(x,y)^N \subseteq I \subseteq (x,y).$$

(Recall that $(x,y)^N = (x^N, x^{N-1}y, \ldots, y^N)$.) An example of such an I is a *monomial ideal* $I = (x^{a_1}y^{b_1}, x^{a_2}y^{b_2}, \ldots)$. The monomial ideal (y^2, x^2y, x^4) is pictured below. The cells in the grid represent members of a basis for $\mathbb{C}[x,y]$ as a $\mathbb{C}$-vector space, and so the ideal is the set of all $\mathbb{C}$-linear combinations of monomials that appear above or to the right of the ideal's generators (in this case, y^2, x^2y, and x^4).

$\vdots$					
y^3	$\vdots$	$\vdots$	$\vdots$		
$\boxed{y^2}$	xy^2	x^2y^2	x^3y^2	$\cdots$	
y	xy	$\boxed{x^2y}$	x^3y	$\cdots$	
1	x	x^2	x^3	$\boxed{x^4}$	$\cdots$

There are many such examples of ideals with radical (x,y). This picture shows how to produce infinitely many distinct examples, but one can easily write down 'continuous families' of them.

Lemma 8.10. Let R be a noetherian ring and $I \subseteq R$ an ideal. Then for some $N > 0$ we have

$$(\operatorname{rad} I)^N \subseteq I \subseteq \operatorname{rad} I.$$

Proof. We know $\operatorname{rad} I$ is finitely generated as an ideal; say $\operatorname{rad}(I) = (x_1, \ldots, x_m)$. Some positive power of each x_i lies in I. Since there are only finitely many x_i, there is $n > 0$ such that $(x_1)^n \in I, \ldots, (x_m)^n \in I$. Notice that any product of at least $mn+1$ of the generators $x_1, \ldots, x_m$ (allowing repetitions) is a multiple of $(x_i)^n$ for some i. Therefore such a product must belong to I, and we have $(\operatorname{rad} I)^{mn+1} \subseteq I$. ∎

Theorem 8.11. Let R be a noetherian ring and M a finitely generated R-module. Then there exists a chain

$$0 = M_0 \subseteq M_1 \subseteq M_2 \subseteq \cdots \subseteq M_r = M$$

of R-modules such that, for $1 \leq i \leq r$, we have $M_i/M_{i+1} \cong R/\mathfrak{p}_i$ for some prime ideal $\mathfrak{p}_i$.

Remark. Such a 'decomposition' of M is far from unique. Even the set of primes $\mathfrak{p}_i$ that occur is not uniquely determined by M.

Exercise. Give an example for $R = \mathbb{Z}$ and M a finitely generated $\mathbb{Z}$-module of nonuniqueness.

Exercise. Let M be a finitely generated module over a noetherian ring R. Show that in any decomposition as in Theorem 8.11, the intersection $\mathfrak{p}_1 \cap \cdots \cap \mathfrak{p}_r$ is equal to $\operatorname{rad}(\operatorname{Ann}_R(M))$.

The closed subset of $\operatorname{Spec}(R)$ defined by the ideal $\operatorname{Ann}_R(M)$ is called the *support* of M. The support of M is the set of prime ideals $\mathfrak{p} \in \operatorname{Spec}(R)$ such that $M_\mathfrak{p} \neq 0$. The module M can be viewed as an $(R/\operatorname{Ann}_R(M))$-module, so we view M as 'sitting on' its support, the closed subset $\operatorname{Spec}(R/\operatorname{Ann}_R(M))$ of $\operatorname{Spec}(R)$.

4/11

Proof of Theorem 8.11. We will show that for any nonzero module M over a noetherian ring, M contains a submodule isomorphic to $R/\mathfrak{p}$ for some prime $\mathfrak{p} \subset R$. Given that, the theorem follows by the following argument: Let M be a finitely generated module. If $M = 0$ we're gone with $r = 0$. So suppose $M \neq 0$ and let $M_1 \cong R/\mathfrak{p}_1 \neq 0$ for some prime $\mathfrak{p}_1 \subset R$. Look at M/M_1. If this is 0, then we're done with $r = 1$. Otherwise M/M_1 contains a submodule isomorphic to $R/\mathfrak{p}_2$ for some prime $\mathfrak{p}_2 \subset R$. Let M_2 be the inverse image of this submodule in M_1. Repeat. The process stops after finitely many steps, since M satisfies ACC for R-modules.

Now we'll prove the claim: By Example Sheet 2, there is a nonzero element x of M whose annihilator in R is maximal among annihilators of nonzero elements (since R is noetherian). Let $\mathfrak{p} = \operatorname{Ann}_R(x)$. We will

show that $\mathfrak{p}$ is prime. (Then $R/\mathfrak{p}$ as a submodule, $R \cdot x \subseteq M$.) The identity 1 does not belong to $\mathfrak{p}$, since $x \neq 0$. Suppose $r, s \in R$ satisfy $rs \in \mathfrak{p}$ and $s \notin \mathfrak{p}$. That is, we have $rsx = 0$ and $sx \neq 0$. Then $\mathfrak{p} \subseteq \mathrm{Ann}_R(sx)$. By the maximality property of $\mathfrak{p}$, we have $\mathfrak{p} = \mathrm{Ann}_R(sx)$. But $r \in \mathrm{Ann}_R(sx)$, so $r \in \mathfrak{p}$. This completes the proof. ∎

Definition. A *finite* A-algebra is an A-algebra that is finitely generated as an A-module.

Contrast: An A-algebra B is *of finite type* if B is finitely generated as an A-algebra.

Example. The polynomial ring $k[x]$ is of finite type over k, but it is not finite over k.

9 Homological algebra

Lang's *Algebra* is a good reference for this topic. Note that most of the material for today's lecture also works for left modules over noncommutative rings.

A sequence of R-linear maps

$$\cdots M_{i+1} \xrightarrow{d_{i+1}} M_i \xrightarrow{d_i} M_{i-1} \xrightarrow{d_{i-1}} \cdots$$

is a *chain complex* (or just *complex*) if $d_i d_{i+1} = 0$ for every i. Equivalently, $\mathrm{im}(d_{i+1}) \subseteq \ker(d_i)$ for every i. We define the *homology groups* of a chain complex (of R-modules) to be the R-modules

$$H_i(M_*) := \frac{\ker d_i}{\mathrm{im}(d_{i+1})}.$$

Thus the chain complex M_* is an exact sequence if and only if its homology groups are all 0.

Let M_* and N_* be complexes of R-modules. A *chain map* (or *map of chain complexes*) $f\colon M_* \to N_*$ is a collection of R-linear maps $f_i\colon M_i \to N_i$ such that the diagram

$$\begin{array}{ccccccccc}
\cdots & \longrightarrow & M_2 & \xrightarrow{d_2} & M_1 & \xrightarrow{d_1} & M_0 & \longrightarrow & \cdots \\
 & & \downarrow{\scriptstyle f_2} & & \downarrow{\scriptstyle f_1} & & \downarrow{\scriptstyle f_0} & & \\
\cdots & \longrightarrow & N_2 & \xrightarrow{e_2} & N_1 & \xrightarrow{e_1} & N_0 & \longrightarrow & \cdots
\end{array}$$

commutes.

Exercise. A chain map $f\colon M_* \to N_*$ determines an R-linear map $f_*\colon H_i(M_*) \to H_i(N_*)$ on homology groups. (Note $H_i(f)$ is also used to denote f_*.)

Let f and g be chain maps $M_* \to N_*$. A *chain homotopy* F from f to g is a collection of R-linear maps $F_i\colon M_i \to N_{i+1}$ such that $dF + Fd = g - f$ as R-linear maps $M_i \to N_i$ for every $i \in \mathbb{Z}$:

$$\begin{array}{ccccccccccccc}
\cdots & \xrightarrow{d} & M_2 & \xrightarrow{d} & M_1 & \xrightarrow{d} & M_0 & \xrightarrow{d} & \cdots & & & & \\
 & & \downarrow{\scriptstyle g-f} & \swarrow{\scriptstyle F_1} & \downarrow{\scriptstyle g-f} & \swarrow{\scriptstyle F_2} & \downarrow{\scriptstyle g-f} & & & & & & \\
\cdots & \xrightarrow{d} & N_2 & \xrightarrow{d} & N_1 & \xrightarrow{d} & N_0 & \xrightarrow{d} & \cdots & & & &
\end{array}$$

Exercise. Write $f \sim g$ if there is a chain homotopy from f to g. If $f \sim g\colon M_* \to N_*$, then $f_* = g_*$ as R-linear maps $H_i(M_*) \to H_i(N_*)$ on homology.

Finally, a *chain homotopy equivalence* $f\colon M_* \to N_*$ is a chain map such that there is a chain map $g\colon N_* \to M_*$ with $fg \sim 1_{N_*}$ and $gf \sim 1_{M_*}$.

Exercise. If $f\colon M_* \xrightarrow{\simeq} N_*$ is a chain homotopy equivalence, then $f_*\colon H_i(M_*) \to H_i(N_*)$ is an isomorphism for every $n \in \mathbb{Z}$.

Definition. Let M be an R-module. A *projective resolution* of M is an exact sequence of R-modules

$$\cdots \longrightarrow P_1 \longrightarrow P_0 \longrightarrow M \longrightarrow 0 (\longrightarrow 0 \longrightarrow 0 \longrightarrow \cdots)$$

with each P_i a projective R-module.

Every R-module has a projective resolution, in fact a *free resolution*. Say I is a set that generates M; then $P_0 := R^{\oplus I} \twoheadrightarrow M \to 0$ is exact. Choose P_1 free that maps onto $\ker(P_0 \to M)$, etc.

Examples. (1) The $\mathbb{Z}$-module $\mathbb{Z}$ has the projective resolution

$$\cdots \longrightarrow 0 \longrightarrow 0 \longrightarrow \mathbb{Z} \xrightarrow{n} \mathbb{Z} \longrightarrow 0.$$

(2) The $\mathbb{Z}$-module $\mathbb{Z}/n$ (for $n \neq 0$) has the projective resolution

$$\cdots \longrightarrow 0 \longrightarrow 0 \longrightarrow \mathbb{Z} \longrightarrow \mathbb{Z} \longrightarrow \mathbb{Z}/n \longrightarrow 0.$$

More generally, for any commutative ring R and any non-zerodivisor $f \in R$, the quotient $R/(f)$ as an R-module has the projective resolution

$$\cdots \longrightarrow 0 \longrightarrow 0 \longrightarrow R \xrightarrow{f} R \longrightarrow R/(f) \longrightarrow 0.$$

To be precise, we say that the projective resolution of M is the chain complex

$$\cdots \longrightarrow P_2 \longrightarrow P_1 \longrightarrow P_0 \longrightarrow 0$$

(not including M). This is a chain complex P_* with P_i projective and

$$H_i(P_*) \cong \begin{cases} M & \text{if } i = 0 \\ 0 & \text{if } i \neq 0 \end{cases}.$$

Projective resolutions generalise the idea of generators and relations for a module. If we have a projective resolution

$$\cdots \longrightarrow P_2 \longrightarrow P_1 \longrightarrow P_0 \longrightarrow M \longrightarrow 0,$$

then P_0 represents the generators for M, P_1 represents the relations, P_2 represents relations between relations, etc.

Projective resolutions are far from unique, but they do have the following in common:

Theorem 9.1. Let M be an R-module. Then any two projective resolutions of M are chain-homotopy-equivalent.

Proof. See *Lang* for the proof, or do it yourself. (Exercise!) The idea is to use the lifting property of projective modules (Lemma 4.1) to define the homotopy equivalence. ∎

9.1 Derived functors

A functor $T\colon R\text{-}\mathbf{Mod} \to R\text{-}\mathbf{Mod}$ is called *additive* if $T(f+g) = Tf + Tg$ for every pair of R-linear maps $f, g\colon M \to N$.

Example. For a given R-module N, define

$$T_N(M) := M \otimes_R N.$$

Then T_N is an additive functor. By definition T_N is exact if and only if N is a flat R-module. An additive functor $T\colon R\text{-}\mathbf{Mod} \to R\text{-}\mathbf{Mod}$ is *right exact* if for every exact sequence

$$A \to B \to C \to 0$$

of R-modules the sequence

$$TA \to TB \to TC \to 0$$

is also exact.

For example, the functor $- \otimes_R N = T_N$ is right exact for every R-module N (Lemma 6.3).

Definition. Let $T\colon R\text{-}\mathbf{Mod} \to R\text{-}\mathbf{Mod}$ be a right exact functor. The *derived functors* $T_i\colon R\text{-}\mathbf{Mod} \to R\text{-}\mathbf{Mod}$ for $i \geq 0$ are defined in the following way: for an R-module M, let P_* be a projective resolution of M. Then we define $T_i(M) := H_i(T(P_*))$. That is, look at the sequence

$$\cdots \longrightarrow TP_2 \longrightarrow TP_1 \longrightarrow TP_0 \longrightarrow 0,$$

which is, by the functoriality of T, always a chain complex of R-modules (though not necessarily exact).

Remark. It's easy to show that $T_0(M) = T(M)$.

The R-modules $T_i(M)$ are independent of choice of projective resolution P_* because any two projective resolutions of M are chain-homotopy-equivalent. We have $P_* \simeq Q_*$, so $T(P_*) \simeq T(Q_*)$; therefore $T(P_*)$ and $T(Q_*)$ have the same homology groups.

Definition. For R-modules M and N, we write

$$\operatorname{Tor}_i^R(M,N) := (T_N)_i(M),$$

an R-module for every $i \geq 0$.

We have

$$\operatorname{Tor}_0^R(M,N) \cong M \otimes_R N.$$

(Think of Tor as describing how far N is from being flat.)

7/11

More concretely, we can define $\operatorname{Tor}_i^R(M,N)$ for $i \geq 0$ by choosing a projective resolution

$$\cdots \longrightarrow P_1 \longrightarrow P_0 \longrightarrow M \longrightarrow 0.$$

We then look at the chain complex

$$\cdots \longrightarrow P_2 \otimes_R N \longrightarrow P_1 \otimes_R N \longrightarrow P_0 \otimes_R N \longrightarrow 0. \qquad (\star)$$

The Tor groups $\operatorname{Tor}_i^R(M,N)$ are the homology groups of the complex $(\star)$.

Remark (Properties of Tor).

(1) $\operatorname{Tor}_0^R(M,N) \cong M \otimes_R N$. To see this, use that $\otimes_R$ is right exact.

(2) If M is projective, then we have

$$\operatorname{Tor}_i^R(M,N) = \begin{cases} M \otimes_R N & \text{if } i = 0 \\ 0 & \text{if } i \neq 0 \end{cases}.$$

If N is flat, then

$$\operatorname{Tor}_i^R(M,N) = \begin{cases} M \otimes_R N & \text{if } i = 0 \\ 0 & \text{if } i \neq 0 \end{cases}.$$

(3) Relation of Tor to torsion: Compute $\operatorname{Tor}_r^R(R/(f),N)$ with $f \in R$ a non-zerodivisor as follows: Use the projective resolution

$$0 \longrightarrow R \longrightarrow R \longrightarrow R/(f) \longrightarrow 0.$$

So $\operatorname{Tor}_*^R(R/(f),N)$ are the homology of the sequence

$$0 \longrightarrow N \xrightarrow{f} N \longrightarrow 0.$$

That is,

$$\operatorname{Tor}_i^R(R/(f),N) = \begin{cases} N/fN & \text{if } i = 0 \\ N[f] & \text{if } i = 1 \\ 0 & \text{if } i > 1 \end{cases},$$

where $N[f] = \{x \in N : fx = 0\}$ is the f-torsion submodule.

The other fundamental example of a derived functor is Ext. Consider the (contravariant) right exact functor

$$H_N(M) = \operatorname{Hom}_R(M,N) \colon R\text{-}\mathbf{Mod} \to (R\text{-}\mathbf{Mod})^{\mathrm{op}}.$$

An R-linear map $M_1 \to M_2$ gives an R-linear map $\operatorname{Hom}_R(M_2,N) \to \operatorname{Hom}_R(M_1,N)$. The derived functors of H_N are called $\operatorname{Ext}_R^i(M,N)$, $i \geq 0$. That is, let P_* be a projective resolution of M, and then $\operatorname{Ext}_R^*(M,N)$ are the homology groups of the sequence

$$0 \longrightarrow \operatorname{Hom}_R(P_0,N) \longrightarrow \operatorname{Hom}_R(P_1,N) \longrightarrow \cdots.$$

Example. Compute $\operatorname{Ext}_R^i(R/(f),N)$ with f a non-zerodivisor. Use the obvious projective resolution of $R/(f)$ and apply $\operatorname{Hom}_R(-,N)$ to get a chain complex

$$0 \longrightarrow \operatorname{Hom}_R(R,N) \longrightarrow \operatorname{Hom}_R(R,N) \longrightarrow 0 \longrightarrow \cdots.$$

But we have an isomorphism $\operatorname{Hom}_R(R,N) \cong N$, and the map $N \cong \operatorname{Hom}_R(R,N) \longrightarrow \operatorname{Hom}_R(R,N) \cong N$ is just the multiplication-by-f map, so we can read off the homology:

$$\operatorname{Ext}_R^i(R/(f),N) \cong \begin{cases} N[f] & \text{if } i = 0 \\ N/fN & \text{if } i = 1 \\ 0 & \text{if } i > 1 \end{cases}.$$

(Notice that we always have $\operatorname{Ext}_R^0(M,N) \cong \operatorname{Hom}_R(M,N)$.)

Remark. $\mathrm{Ext}^1_R(M,N)$ can be interpreted as the set of isomorphism classes of extensions of R-modules:

$$0 \longrightarrow N \longrightarrow E \longrightarrow M \longrightarrow 0.$$

The 'trivial' extension $E = M \oplus N$ corresponds to $0 \in \mathrm{Ext}^1_R(M,N)$.

Lemma 9.2 (Snake lemma, Example sheet 2)**.** If we have a commutative diagram of R-modules

$$\begin{array}{ccccccccc} 0 & \longrightarrow & A_1 & \longrightarrow & A_2 & \longrightarrow & A_3 & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle f} & & \downarrow{\scriptstyle g} & & \downarrow{\scriptstyle h} & & \\ 0 & \longrightarrow & B_1 & \longrightarrow & B_2 & \longrightarrow & B_3 & \longrightarrow & 0 \end{array}$$

with exact rows, then we have a canonical exact sequence

$$\begin{aligned} 0 &\longrightarrow \ker f \longrightarrow \ker g \longrightarrow \ker h \\ &\longrightarrow \operatorname{coker} f \longrightarrow \operatorname{coker} g \longrightarrow \operatorname{coker} h \longrightarrow 0. \end{aligned}$$

(The interesting map here is, of course, the map $\ker h \to \operatorname{coker} f$.)

This implies, with more diagram-chasing, the following theorem:

Theorem 9.3. Given a short exact sequence of chain complexes of R-modules:

$$\begin{array}{ccccccccc} & & \vdots & & \vdots & & \vdots & & \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 0 & \longrightarrow & A_{i+1} & \longrightarrow & B_{i+1} & \longrightarrow & C_{i+1} & \longrightarrow & 0 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 0 & \longrightarrow & A_i & \longrightarrow & B_i & \longrightarrow & C_i & \longrightarrow & 0 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 0 & \longrightarrow & A_{i-1} & \longrightarrow & B_{i-1} & \longrightarrow & C_{i-1} & \longrightarrow & 0 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ & & \vdots & & \vdots & & \vdots & & \end{array}$$

(a commutative diagram, with chain complexes in columns and rows exact), there is a long exact sequence of R-modules in homology:

$$\cdots \longrightarrow H_i(A) \longrightarrow H_i(B) \longrightarrow H_i(C) \xrightarrow{\partial} H_{i-1}(A) \longrightarrow \cdots$$

Refer to Lang's *Algebra* for a proof. Notice again that the 'boundary map' $\partial\colon H_i(C) \to H_{i-1}(A)$ is the interesting one.

Corollary 9.4 (Long exact sequence for Tor in the second variable)**.** Let M be an R-module, and let $0 \to A \to B \to C \to 0$ be a short exact sequence of R-modules. Then we have a long exact sequence:

$$\begin{aligned} \cdots &\to \mathrm{Tor}^R_i(M,A) \to \mathrm{Tor}^R_i(M,B) \to \mathrm{Tor}^R_i(M,C) \to \mathrm{Tor}^R_{i-1}(M,A) \to \cdots \\ &\to \mathrm{Tor}^R_2(M,C) \to \mathrm{Tor}^R_1(M,A) \to \mathrm{Tor}^R_1(M,B) \to \mathrm{Tor}^R_1(M,A) \\ &\to M \otimes_R A \to M \otimes_R B \to M \otimes_R C \to 0. \end{aligned}$$

Proof. Let P_* be a projective resolution of M. Then we have a short exact sequence of chain complexes:

$$\begin{array}{ccccccccc} & & \vdots & & \vdots & & \vdots & & \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 0 & \longrightarrow & P_{i+1} \otimes_R A & \longrightarrow & P_{i+1} \otimes_R B & \longrightarrow & P_{i+1} \otimes_R C & \longrightarrow & 0 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 0 & \longrightarrow & P_i \otimes_R A & \longrightarrow & P_i \otimes_R B & \longrightarrow & P_i \otimes_R C & \longrightarrow & 0 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ & & \vdots & & \vdots & & \vdots & & \end{array}$$

It's easy to check commutativity (Exercise!), and it's obvious that the columns are chain complexes. The rows are exact because projective modules are flat (Ex Sheet 1). By the theorem (9.3), we get a long exact sequence of homology groups. ∎

Theorem 9.5. Let M and N be modules over R. Then the R-modules $\operatorname{Tor}_i^R(M,N)$ can be computed by a projective resolution of N, or more generally by a flat resolution of N. That is, given any flat resolution of N:

$$\cdots \longrightarrow F_2 \longrightarrow F_1 \longrightarrow F_0 \longrightarrow N \longrightarrow 0 \qquad (F_i \text{ flat}),$$

we have that the modules $\operatorname{Tor}_i^R(M,N)$ are the homology groups of the chain complex

$$\cdots \longrightarrow M \otimes_R F_1 \longrightarrow M \otimes_R F_0 \longrightarrow 0.$$

Proof. Divide the exact sequence $\cdots \longrightarrow F_1 \longrightarrow F_0 \longrightarrow N \longrightarrow 0$ into short exact sequences:

$$0 \longrightarrow I_{j+1} \longrightarrow F_j \longrightarrow I_j \longrightarrow 0$$

where $I_j := \operatorname{im}(F_j \to F_{j-1})$ for $j > 0$ and $I_0 := N$. By 9.4 we get an exact sequence

$$\operatorname{Tor}_{i+1}^R(M,F_j) \to \operatorname{Tor}_{i+1}^R(M,I_j) \to \operatorname{Tor}_i^R(M,I_{j+1}) \to \operatorname{Tor}_i^R(M,F_j). \qquad (\dagger)$$

But $\operatorname{Tor}_{i+1}^R(M,F_j) = \operatorname{Tor}_i^R(M,F_j) = 0$ for $i > 0$, so $(\dagger)$ gives isomorphisms

$$\begin{aligned}\operatorname{Tor}_j^R(M,N) &\cong \operatorname{Tor}_{j-1}^R(M,I_1) \cong \cdots \\ &\cong \operatorname{Tor}_1^R(M,I_{j-1}) \cong \ker(M \otimes I_j \to M \otimes F_{j-1}).\end{aligned}$$

Also, since $\otimes_R$ is right exact and the sequence $F_{j+1} \to F_j \to I_j \to 0$ is exact, the sequence

$$M \otimes_R F_{j+1} \longrightarrow M \otimes_R F_j \longrightarrow M \otimes_R I_j \longrightarrow 0$$

is exact. So $M \otimes_R I_j \cong \operatorname{coker}(M \otimes_R F_{j+1} \to M \otimes_R F_j)$. Therefore $\operatorname{Tor}_j^R(M,N) \cong H_j(M \otimes_R F_{j+1} \to M \otimes_R F_j \to M \otimes_R F_{j-1})$. ∎

From this theorem, we conclude that we can compute $\operatorname{Tor}_j^R(M,N)$ using a projective resolution of M or of N, and we get the same answer. Since $M \otimes_R N \cong N \otimes_R M$, it follows that $\operatorname{Tor}_i^R(M,N) \cong \operatorname{Tor}_i^R(N,M)$ (though this isn't obvious from the definition of Tor). In fact, you could also use a flat resolution of M, not necessarily a projective resolution, and get the same groups. It follows also that we have a long exact sequence for Tor in the first variable.

9/11

10 Integral Extensions

Definition. Let B be a ring and A be a subring of B. An element $x \in B$ is *integral over* A if there are elements $a_0, \ldots, a_{n-1} \in A$ such that

$$x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 = 0,$$

that is, if x is a root of a monic polynomial with coefficients in A.

Example. Every $x \in A$ is integral over A.

We highlight an important special case: suppose $K/\mathbb{Q}$ is a finite extension of fields. Define the set (ring, as we will see shortly) $\mathcal{O}_K$ of *algebraic integers in* K as follows:

$$\mathcal{O}_K = \{x \in K : x \text{ is integral over } \mathbb{Z}\}.$$

Exercise. Show that $\mathcal{O}_{\mathbb{Q}} = \mathbb{Z}$. (To get started, show that $\frac{1}{2} \notin \mathcal{O}_{\mathbb{Q}}$.)

Lemma 10.1. Suppose A is a subring of B. We (unfortunately) write $A[x]$ for the subring of B generated by A and the element x. The following are equivalent:

(1) $x \in B$ is integral over A;

(2) the subring $A[x]$ of B is a finitely generated A-module;

(3) the subring $A[x]$ of B is contained in a subring $C \subseteq B$ that is finitely generated as an A-module;

(4) there exists a faithful[4] module M over the ring $A[x]$ that is finitely generated as an A-module.

Proof. The implication (1)⇒(2) is clear: if x is integral over A, then we have

$$x \in A \cdot 1 + A \cdot x + \cdots + A \cdot x^{n-1}.$$

[4] I don't think we ever defined a *faithful* R-module…An R-module is *faithful* if $\operatorname{Ann}_R(M) = 0$. (Atiyah–MacDonald 20)

Now by induction on m, the element x^{n+m} is also an A-linear combination of the elements $1, x, \ldots, x^{n-1}$ for every $m \geq 0$.

For the second implication, (2)⇒(3), just take $C = A[x]$.

The third implication (3)⇒(4) is also easy: Take $M = C$, viewed as an $A[x]$-module. Observe M is finitely generated by assumption and faithful since $A[x] \subseteq C$.

The heart of the proof is the final implication, (4)⇒(1): Let $m_1, \ldots, m_r$ generate M as an A-module. Then there are elements $a_{ij} \in A$ such that

$$xm_i = \sum_{j=1}^{n} a_{ij} m_j.$$

Consider the matrix $X := xI - (a_{ij})$. If $X = (y_{ij})$ then $\sum y_{ij} m_j = 0$. Now multiply by $\mathrm{adj}(X)$. Recall that for any square matrix, $\mathrm{adj}(X)X = (\det X) \cdot I$, so we get $(\det X) \cdot m_i = 0$ for every i; that is, $(\det X) \cdot M = 0$. But $\det X$ belongs to $A[x]$, which (by assumption) acts faithfully on M. So it must be that $\det X = 0$. But $\det X$ is a monic polynomial in x, with coefficients in A, so x is integral over A. ∎

From just this one technical lemma we can deduce a surprising number of useful facts.

Recall that an A-algebra B is *finite over* A (or a *finite* A*-algebra*) if B is finitely generated as an A-module, whereas B is *of finite type* over A if B is finitely generated as an A-algebra. Accordingly, a morphism $f\colon X \to Y$ of affine schemes is *finite* if $\mathcal{O}_X$ is finite over $\mathcal{O}_Y$ and *of finite type* if $\mathcal{O}_X$ is of finite type over $\mathcal{O}_Y$. (Recall the definition of the ring $\mathcal{O}_X$ of regular functions on X.)

Lemma 10.2. Let $A \subseteq B \subseteq C$ be a chain of subrings. If B is finite over A and C is finite over B, then C is finite over A.

Proof. Let $b_1, \ldots, b_n$ generate B as an A-module and $c_1, \ldots, c_r$ generate C as a B-module. Check (Exercise!) that all elements $b_i c_j$ generate C as an A-module. ∎

Corollary 10.3. Let B be a ring and A a subring. Suppose that each of the elements $x_1, \ldots, x_n \in B$ is integral over A. Then the subring $A[x_1, \ldots, x_n]$ of B is finitely generated as an A-module.

Proof. Induct on n. Induction has $R := A[x_1, \ldots, x_{n-1}]$ finitely generated as an A-module. By assumption x_n is integral over A, so integral over R. Apply Lemmas 10.1 and 10.2 to conclude that $A[x_1, \ldots, x_n]$ is finitely generated as an A-module. ∎

Corollary 10.4. Let A be a subring of a ring B. Let C be defined by

$$C = \{x \in B : x \text{ is integral over } A\}.$$

Then C is a subring of B (and, obviously, $A \subseteq C \subseteq B$).

Proof. Since $A \subseteq C$, we have $0, 1 \in C$. We need to show that for every pair x, y of elements of C, the elements xy, $x + y$, and $-x$ also belong to C. But by the previous corollary, the subring $A[x, y]$ generated by A, x, and y is a finitely generated A-module, so all its elements are integral over A. In particular, the elements xy, $x + y$, and $-x$ are integral over A. ∎

It seems we've cheated somewhere. We shouldn't have been able, in the proof of Corollary 10.4 that C was a ring without somehow exhibiting monic polynomials over A of which xy and $x+y$ are roots (cf. the exercise below). But somehow Lemma 10.1 took care of all the combinatorial work we had to do.

Exercise. Suppose x satisfies the monic polynomial f (with coefficients from A) and y satisfies the monic polynomial g. Can you find monic polynomials satisfied by $x + y$ and xy defined in terms of the coefficients of f and g? (Try f, g quadratic first, as a nice special case.)

Definition. The set $\{x \in B : x \text{ is integral over } A\}$ is called the *integral closure* of A in B. If the integral closure of A is all of B, we say B is *integral over* A; if the integral closure of A is A, we say A is *integrally closed in* B. An integral domain A is called *normal* (or *integrally closed*) if it is integrally closed in its field of fractions.

Example. $\mathbb{Z}$ is normal by the first exercise of this section. A problem on Example Sheet 2 (?) asks to prove that every UFD is normal. So $k[x_1, \ldots, x_n]$ is normal, and $\mathcal{O}_k$ is normal (as we'll see).

Definition. Let $f\colon A \to B$ be a ring homomorphism. We say B is *integral over* A if B is integral over $f(A)$.

We could rephrase Corollary 10.3 to say that 'B is finite over A iff B is of finite type and integral over A'; more concisely, 'finite = finite type + integral'.

Corollary 10.5. Let $A \subseteq B \subseteq C$ be a chain of subrings. If B is integral over A and C is integral over B, then C is integral over A.

Proof. If $x \in C$, then there are elements b_i such that $x^n + b_{n-1}x^{n-1} + \cdots + b_0 = 0$. But $A[b_0, \ldots, b_{n-1}]$ is finitely generated as an A-module, as each b_i is integral over A. Thus x is integral over $R := A[b_0, \ldots, b_{n-1}]$, so the subring $A[b_0, \ldots, b_{n-1}, x]$ is finite over R (hence over A). Therefore x is integral over A. ∎

Corollary 10.6. Let A be a subring of a ring B, and let C be the integral closure of A in B. Then C is integrally closed in B.

Proof. If $x \in B$ is integral over C, then x is integral over A (by the previous corollary, 10.5), so $x \in C$. ∎

Exercise. ('Integrality behaves well with respect to quotients and localisations') Suppose A is a subring of B and suppose B is integral over A. Show:

(1) if J is an ideal in B and $I = J \cap A$, then the quotient B/J is integral over the quotient A/I;

(2) if S is a multiplicatively closed subset of A, then the localisation $B[S^{-1}]$ is integral over the localisation $A[S^{-1}]$.

Lemma 10.7. Let A be a subring of a ring B, and let C be the integral closure of A in B. Let $S \subset A$ be multiplicatively closed. Then $C[S^{-1}]$ is the integral closure of $A[S^{-1}]$ in $B[S^{-1}]$.

Proof. By the exercise above, $C[S^{-1}]$ is integral over $A[S^{-1}]$, so we need only show that every element of $B[S^{-1}]$ that is integral over $A[S^{-1}]$ belongs to $C[S^{-1}]$.

If $b/s \in B[S^{-1}]$ is integral over $A[S^{-1}]$ then we have an equation

$$(b/s)^n + a_{n-1}/s_{n-1}(b/s)^{n-1} + \cdots + a_0/s_0 = 0$$

(in $B[S^{-1}]$) for some elements $a_i \in A$, $s_i \in S$. Clear denominators: put $t = s_0 \ldots s_{n-1}$ and multiply by $(st)^n$, getting

$$(bt)^n + e_{n-1}(bt)^{n-1} + \cdots + e_0 = 0$$

(in $B[S^{-1}]$) for some $e_i \in A$. Multiply by some $u \in S$ to get the equation

$$u(bt)^n + ue_{n-1}(bt)^{n-1} + \cdots + ue_0 = 0$$

in B, by definition of $B[S^{-1}]$. Multiply once more by u^{n-1} to see that the element $btu \in B$ is integral over A. So $btu \in C$, whence $b/s = (btu)/(stu)$ belongs to $C[S^{-1}]$. ∎

Hence normality is a local property:

Lemma 10.8. Let A be an integral domain. The following are equivalent:

(1) A is normal;

(2) $A_\mathfrak{p}$ is normal for every prime $\mathfrak{p} \subset A$;

(3) $A_\mathfrak{m}$ is normal for every maximal ideal $\mathfrak{m} \subset A$.

11/11

Correction to Example Sheet 3: for #9, assume that A is a domain of finite type over a field.

Next we discuss some basic properties of Ext.

Unlike Tor, $\mathrm{Ext}^i_R(M,N)$ is in general not related to $\mathrm{Ext}^i_R(N,M)$ because there is no relation between $\mathrm{Hom}_R(M,N)$ and $\mathrm{Hom}_R(N,M)$. Nonetheless, Ext can be computed by either a projective resolution of M or an injective resolution of N:

$$0 \longrightarrow N \longrightarrow I_0 \longrightarrow I_i \longrightarrow \cdots.$$

Definition. An R-module is *injective* iff for every injective R-linear map $M \hookrightarrow N$, every R-linear map $M \to I$ extends to an R-linear map $N \to I$.

(See Lang's *Algebra* for a discussion of injective modules.)

Also, we have a long exact sequence for Ext in the first or second variable: if M is an R-module and $0 \to A \to B \to C \to 0$ is a short exact sequence of R-modules, then we can define canonical long exact sequences

$$\begin{aligned} 0 &\longrightarrow \mathrm{Hom}_R(M,A) \longrightarrow \mathrm{Hom}_R(M,B) \longrightarrow \mathrm{Hom}_R(M,C) \\ &\longrightarrow \mathrm{Ext}^1_R(M,A) \longrightarrow \mathrm{Ext}^2_R(M,B) \longrightarrow \cdots \end{aligned}$$

and

$$\begin{aligned} 0 &\longrightarrow \mathrm{Hom}_R(C,M) \longrightarrow \mathrm{Hom}_R(B,M) \longrightarrow \mathrm{Hom}_R(A,M) \\ &\longrightarrow \mathrm{Ext}^1_R(C,M) \longrightarrow \mathrm{Ext}^2_R(B,M) \longrightarrow \cdots \end{aligned}$$

Now the application of Tor promised earlier (Theorem 6.4).

Lemma 10.9. Let M be an R-module. Then the following are equivalent:

(1) M is a flat R-module;

(2) for any injective R-linear map $A \to B$, the map $M \otimes_R A \to M \otimes_R B$ is injective;

(3) for any ideal $I \subseteq R$, the induced map $M \otimes_R I \to M \otimes_R R = M$ is injective.

Proof. We showed that (1) and (2) are equivalent and that (2) implies (3) in the proof of Theorem 6.4. We now show that (3) implies (1).

For any ideal $I \subseteq R$, we have a long exact sequence

$$\cdots \longrightarrow \mathrm{Tor}^R_1(M,R) \longrightarrow \mathrm{Tor}^R_1(M,R/I) \longrightarrow M \otimes_R I \longrightarrow M \otimes_R I \longrightarrow \cdots.$$

But $\mathrm{Tor}^R_1(M,R)$ is zero since R is R-flat, and the map $M \otimes_R I \to M \otimes_R I$ is an injection by assumption. Therefore $\mathrm{Tor}^R_1(M,R/I) = 0$ for all ideals $I \subseteq R$.

Next let N be any finitely generated R-module. Say

$$N = Rx_1 + \cdots + Rx_n$$

for some elements $x_1, \ldots, x_n \in N$. Then we can consider the submodules $N_i := Rx_1 + \cdots Rx_i \subseteq N$ for $1 \le i \le n$. We have containments

$$0 \subseteq N_1 \subseteq \cdots \subseteq N_m = N,$$

and each N_i/N_{i-1} is generated by one element so is isomorphic to R/I for some $I \subseteq R$. By (induction and) the long exact sequence for Tor in the second variable, $\mathrm{Tor}^R_1(M,N) = 0$ for every finitely generated module N.

Finally, let N be any R-module. Then N is the direct limit of its finitely generated R-submodules (which always form a directed set). But Tor commutes with direct limits in each variable (cf. Example Sheet 2). So $\mathrm{Tor}^R_1(M,N) = 0$ for any R-module N.

Let $A \to B$ be any injection of R-modules. Then we have a short exact sequence

$$0 \longrightarrow A \longrightarrow B \longrightarrow B/A \longrightarrow 0$$

and hence a long exact sequence

$$\cdots \longrightarrow 0 = \mathrm{Tor}^R_1(M, B/A) \longrightarrow M \otimes_R A \longrightarrow M \otimes_R B \longrightarrow \cdots.$$

That is, the map $M \otimes_R A \to M \otimes_R B$ is injective, so M is flat. ∎

Back to integral extensions:

Recall that we proved (Lemma 10.7) that the integral closure can be computed locally. Therefore normality is a local property:

Theorem 10.10. Let R be a domain. The following are equivalent:

(1) R is normal;

(2) $R_\mathfrak{p}$ is normal for every prime ideal $\mathfrak{p} \subset R$;

(3) $R_\mathfrak{m}$ is normal for every maximal ideal $\mathfrak{m} \subset R$.

Proof. Note that the rings $R_\mathfrak{p}$, $R_\mathfrak{m}$, and R are all domains with the same fraction field: $R \subset R_\mathfrak{p} \subseteq \mathrm{Frac}(R) = K$. Let C be the integral closure of R in K. Let $f\colon R \hookrightarrow C$ be the inclusion; then R is normal if and only if f is surjective. By the locality of the integral closure (Lemma 10.7), $R_\mathfrak{p}$ is normal if and only if the induced map $f_\mathfrak{p}\colon R_\mathfrak{p} \to C_\mathfrak{p}$ is surjective. But the

surjectivity of an R-linear map is a local property (at prime or maximal ideals). So f is surjective if and only if $f_{\mathfrak{p}}$ is surjective, if and only if $\mathfrak{m}$ is surjective. ∎

Geometrically, a ring is normal if and only if $\mathrm{Spec}(R)$ is 'not too singular'. In particular, a *normal affine variety* has a singular set of codimension ≥ 2.

insert pictures here

Let f be the function that maps the affine line A^1_k onto the cusp $\{x^2 = y^3\} \subset A^2_k$. Here f is a finite morphism, and $\mathrm{Frac}(R) \cong k(t)$, so $\mathrm{Spec}(R)$ is not normal. (Note that $\{x^2 = y^3\}$ is not normal.) We have $R = k[x,y]/(x^2 - y^3) \hookrightarrow k[t]$, $x \mapsto t^3$, $y \mapsto t^2$. Indeed the image of R in $k[t]$ is the subring $k\{1, t^2, t^3, \ldots\}$. Clearly $k[t]$ is generated by 1 and t as an R-module, so $k[t]$ is finite over R.

Example. For any field k, the map $A^1_k \xrightarrow{f} A^1_k$, $x \mapsto x^2$ is finite. Indeed, this map induces the map $k[y] \to k[x]$, $y \mapsto x^2$. Here $k[x]$ is generated by 1 and x as a module over the subring $k[y] = k\{1, x^2, x^4, x^6, \ldots\} \subset k[x]$. So f is a finite morphism.

Lemma 10.11. Suppose the ring B is integral over its subring A and that A is a domain. Let $\mathfrak{q} \subset B$ be prime, and put $\mathfrak{p} = \mathfrak{q}^c = \mathfrak{q} \cap A$. (Notice that $\mathfrak{p}$ is a prime ideal in A.) Then $\mathfrak{q}$ is maximal in B if and only if $\mathfrak{p}$ is maximal in A.

For affine varieties X and Y over a field k, a morphism $X \to Y$ has $\mathcal{O}(Y) \to \mathcal{O}(X)$ injective if and only if f is *dominant*: $f(X)$ is dense in Y. So the lemma has the following geometric consequence: if $f\colon X \to Y$ is a finite dominant morphism of f-varieties[5], then a point p in X is closed if and only if $f(p)$ in Y is closed.

Proof. By the exercise following Corollary 10.6, $B/\mathfrak{q}$ is integral over $A/\mathfrak{p} \subseteq B/\mathfrak{q}$. Replace A and B by $A/\mathfrak{p}$ and $B/\mathfrak{q}$, respectively. Thus we have to show that if $A \subseteq B$ are domains with B integral over A, then A is a field if and only if B is a field.

[5] Surely he meant k-varieties here...

Suppose A is a field. Let $y \in B$ be nonzero. Then we can write

$$0 = y^n + a_{n-1}y^{n-1} + \cdots + a_0 \in B$$

for some elements $a_i \in A$. Choose such an equation with n minimal. Then $a_0 \neq 0$ in A, since B is a domain. We have

$$y(y^{n-1} + a_{n-1}y^{n-2} + \cdots + a_1) = -a_0 \neq 0,$$

so y is a unit (as A is a field).

Conversely, suppose B is a field. Let u be a nonzero element of A. Then $\frac{1}{u} \in B$, so $\frac{1}{u}$ is integral over A. That is, there are elements $a_i \in A$ such that

$$0 = (\tfrac{1}{u})^n + a_{n-1}(\tfrac{1}{u})^{n-1} + \cdots + a_0 = 0$$

in B. Multiply by u^{n-1} to get the equation

$$0 = \tfrac{1}{u} + a_{n-1} + a_{n-2}u + \cdots + a_0 u^{n-1}$$

in B. But the sum $a_{n-1} + a_{n-2}u + \cdots + a_0 u^{n-1}$ belongs to A, so $\frac{1}{u} \in A$. Therefore A is a field. ∎

14/11

Corollary 10.12. Suppose B is integral over the subring $A \subseteq B$. Let $\mathfrak{q}$ and $\mathfrak{q}'$ be prime ideals in B such that $q \subseteq q'$ and their contractions in A are equal:

$$\mathfrak{q} \cap A = \mathfrak{q}^c = (\mathfrak{q}')^c = \mathfrak{q}' \cap A.$$

Then $\mathfrak{q} = \mathfrak{q}'$.

Geometrically, this corollary says that, if some irreducible closed subset of $\mathrm{Spec}(B)$ is contained in another irreducible closed subset of $\mathrm{Spec}(B)$, then a finite morphism doesn't map the two irreducible closed subsets onto the same irreducible closed subset of $\mathrm{Spec}(A)$.

Proof. Let $\mathfrak{p} = \mathfrak{q}^c (= (\mathfrak{q}')^c)$. By Lemma 10.7, the localisation $B_{\mathfrak{p}}$ is integral over the localisation $A_{\mathfrak{p}}$. (Here $B_{\mathfrak{p}} = B[(A \smallsetminus \mathfrak{p})^{-1}]$ need not be a local ring.) Notice that $A_{\mathfrak{p}} \subseteq B_{\mathfrak{p}}$, since localisation (an exact functor) preserves

injections (Theorem 7.6). Let $\mathfrak{m} = \mathfrak{p}A_\mathfrak{p}$, the (unique) maximal ideal in $A_\mathfrak{p}$. And set $\mathfrak{n} = \mathfrak{q}B_\mathfrak{p} \subseteq B_\mathfrak{p}$ and $\mathfrak{n}' = \mathfrak{q}'B_\mathfrak{p} \subseteq B_\mathfrak{p}$. We will show that $\mathfrak{n} \subseteq \mathfrak{n}'$ and $\mathfrak{n}^c = (\mathfrak{n}')^c = \mathfrak{m} \subset A_\mathfrak{p}$.

We want to show that $\mathfrak{q}B_\mathfrak{p} \cap A_\mathfrak{p} = \mathfrak{p}A_\mathfrak{p}$, that is that the map

$$A_\mathfrak{p}/\mathfrak{p}A_\mathfrak{p} \longrightarrow B_\mathfrak{p}/\mathfrak{q}B_\mathfrak{p}$$

is injective. We know that the map $A/\mathfrak{p} \hookrightarrow B/\mathfrak{q}$ is an injection. Since localisation is an exact functor on A-modules, it follows that the map $(A/\mathfrak{p})_\mathfrak{p} \hookrightarrow (B/\mathfrak{q})_\mathfrak{p}$ is an A-linear injection. But also, localising commutes with taking quotient rings (Exercise! $(R/I)[S^{-1}] = R[S^{-1}]/I \cdot R[S^{-1}]$ for a multiplicatively closed subset $S \subseteq R$.), so we've proved that the map $A_\mathfrak{p}/\mathfrak{p}A_\mathfrak{p} \to B_\mathfrak{p}/\mathfrak{q}B_\mathfrak{p}$ is injective.

We know that $\mathfrak{n}$ and $\mathfrak{n}'$ are prime ideals in $B_\mathfrak{p}$, so since $\mathfrak{n}^c = \mathfrak{m}$ in $A_\mathfrak{p}$ and the ring $B_\mathfrak{p}$ is integral over $A_\mathfrak{p}$, we've shown that $\mathfrak{n}$ and $\mathfrak{n}'$ are maximal ideals in $B_\mathfrak{p}$. Since $\mathfrak{n} \subseteq \mathfrak{n}'$, it must be that $\mathfrak{n} = \mathfrak{n}'$. Using the one-to-one correspondence between prime ideals in $B_\mathfrak{p}$ and primes in B which do not meet $A \smallsetminus \mathfrak{p}$, we see that $\mathfrak{q} = \mathfrak{q}'$ in B. ∎

Theorem 10.13. Let A be a subring of a ring B, and suppose B is integral over A. Suppose also that $\mathfrak{p}$ is a prime ideal in A. Then there is a prime ideal $\mathfrak{q} \subseteq B$ with $\mathfrak{q} \cap A = \mathfrak{p}$.

Geometrically, this theorem claims that a finite dominant (the image is dense in the target) morphism of varieties over k is surjective. As a non-example, consider the (non-surjective) inclusion $A^1_k \smallsetminus \{0\} \hookrightarrow A^1_k$ induced by the inclusion $k[x] \hookrightarrow k[x, x^{-1}]$. The map of rings is not finite, and the morphism $A^1_k \smallsetminus \{0\} \hookrightarrow A^1_k$ is not a finite morphism.

Proof. We know that the localisation $B_\mathfrak{p}$ is integral over $A_\mathfrak{p}$. Since localisation preserves injections, the following diagram commutes, and its rows are injections:

$$\begin{array}{ccc} A & \hookrightarrow & B \\ \downarrow{\scriptstyle \alpha} & & \downarrow{\scriptstyle \beta} \\ A_\mathfrak{p} & \hookrightarrow & B_\mathfrak{p} \end{array} \qquad (*)$$

Here $A_\mathfrak{p}$ is local, so nonzero. Therefore $B_\mathfrak{p}$ is nonzero, and so there is a maximal ideal $\mathfrak{n}$ in $B_\mathfrak{p}$. Then $\mathfrak{m} := \mathfrak{n} \cap A_\mathfrak{p}$ is maximal in $A_\mathfrak{p}$ by Lemma 10.11. Therefore $\mathfrak{m}$ is the unique maximal ideal in $A_\mathfrak{p}$, so $\mathfrak{m} = \mathfrak{p}A_\mathfrak{p}$. Letting $\mathfrak{q} = \beta^{-1}(\mathfrak{n})$, we see that $\mathfrak{q}$ is a prime ideal in B, and we conclude that $\mathfrak{q} \cap A = \mathfrak{p}$ by the commutativity of the diagram $(*)$. ∎

11 Noether normalisation and Hilbert's Nullstellensatz

Lemma 11.1 (Preparation lemma)**.** Let k be a field and f a nonzero element of the polynomial ring $k[x_1, \ldots, x_n]$. Then there is an isomorphism

$$k[x_1, \ldots, x_n] \xrightarrow{\sim} k[y_1, \ldots, y_n]$$

that sends f to the product of a nonzero constant in k and a polynomial which is monic in y_n. That is,

$$f = a{y_n}^d + \sum_{i=0}^{d-1} a_i(y_1, \ldots, y_{n-1}){y_n}^i$$

for some $a \in k$.

Proof. Let $f = \sum a_I x^I$, where $I = (i_1, \ldots, i_n) \in \mathbb{N}^n$ and $x^I := {x_1}^{i_1} \cdots {x_n}^{i_n}$. Let $(i_1, \ldots, i_n) \in \mathbb{N}^n$ be the element with $a_I \neq 0$ and with i_1 maximal, and i_2 maximal among terms with that value of x_1, and so on. Choose integers $m_1 \gg m_2 \gg \cdots \gg m_{n-1} > 1$. Then

$$f(y_1 + {y_n}^{m_1}, \ldots, y_{n-1} + {y_n}^{m_{n-1}}, y_n) =$$
$$a_{i_1 \ldots i_n} {y_n}^{m_1 i_1 + \cdots + m_{n-1} i_{n-1} + i_n} + \text{ terms of lower total degree in } y_1, \ldots, y_n$$

This polynomial is the product of the nonzero constant $a_{i_1} \cdots a_{i_n} \in k^*$ and a polynomial monic in y_n. So the problem is solved by the isomorphism

$$x_1 \mapsto (y_1 + {y_n}^{m_1}), \ldots, x_{n-1} \mapsto (y_{n-1} + {y_n}^{m_{n-1}}), x_n \mapsto y_n.$$

This defines an isomorphism of k-algebras; indeed, its inverse is given by

$$y_1 \mapsto (x_1 - {x_n}^{m_1}), \ldots, y_{n-1} \mapsto (x_{n-1} - {x_n}^{m_{n-1}}), y_n \mapsto x_n.$$

■

Lemma 11.2 (Noether normalisation lemma)**.** Let k be a field and let R be a nonzero k-algebra of finite type. Then there is $n \in \mathbb{N}$ and an inclusion $k[x_1, \ldots, x_n] \hookrightarrow R$ such that R is finite over $k[x_1, \ldots, x_n]$.

A geometric example: Consider the variety $\{xy = 1\}$ in the affine plane A^2_k, and think of the picture for $k = \mathbb{R}$.

insert picture here

The morphism given by projecting the variety $\{xy = 1\}$ straight down onto the affine line A^1_k cannot be finite, since it isn't surjective (nothing is mapped to 0). But there *are* finite morphisms of $\{xy = 1\}$ onto the affine line A^1_k; you just need to 'rotate a bit' for the projection to be finite.

Proof. Let $k[x_1, \ldots, x_n] \to R$ be a surjective homomorphism of k-algebras with kernel I. If $I = 0$, we're done. Otherwise we can pick a nonzero element $f \in I$. By the Preparation Lemma 11.1, after changing (if necessary) our choice of algebra generators for R, we can assume that f is the product of an element of k^* and a y_n-monic polynomial. Multiplying f by an element of k^*, we can assume that $f \in I$ is y_n-monic. So we have a relation

$${x_N}^d + \sum_{i=0}^{d-1} f_i(x_1, \ldots, x_{N-1}) {x_N}^i = 0$$

in R which shows that x_N is integral over the subring $S := \mathrm{im}(k[x_1, \ldots, x_n] \to R)$. In fact, R is finite over S. By induction on N, S is finite over some polynomial subring. So R is finite over that polynomial subring. ■

Corollary 11.3 (Hilbert's Nullstellensatz, first weak version)**.** Let R be an algebra of finite type over a field k. If R is a field, then R is finite over k.

Proof. We know by Noether normalisation 11.2 that R is finite over some subalgebra $k[x_1, \ldots, x_n] \subseteq R$.[6] If $n = 0$, we're done, so suppose $n \geq 1$. Then since R is a field and $x_1 \neq 0$ in R, there is an inverse $1/x_1$ in R for x_1. So $1/x_1$ is integral over $k[x_1, \ldots, x_n]$, but R contains the rational function field $k(x_1, \ldots, x_n)$, and $1/x_1 \in k(x_1, \ldots, x_n)$ is *not* integral over $k[x_1, \ldots, x_n]$ (as you can easily check). This is a contradiction, so $n = 0$. ■

Theorem 11.4 (Hilbert Nullstellensatz, second weak version)**.** Let $f_1, \ldots, f_r$ be polynomials in $k[x_1, \ldots, x_n]$ over an algebraicly closed field k. Then either there are polynomials $g_1, \ldots, g_r$ such that

$$f_1 g_1 + \cdots + f_r g_r = 1,$$

or there is a point $(a_1, \ldots, a_n) \in k^n$ at which all the f_i are 0.

Remark. Notice first that both possibilities in the theorem cannot simultaneously hold.

Also, the theorem is totally false for k not algebraicly closed: e.g., the polynomial $x^2 + 1$ in $\mathbb{R}[x]$ has no roots in $\mathbb{R}$, but there is no $g(x)$ with $g(x)(x^2 + 1) = 1$.

Proof. Let R be the quotient ring $k[x_1, \ldots, x_n]/(f_1, \ldots, f_r)$. If the first conclusion is false, then $(f_1, \ldots, f_r) \neq k[x_1, \ldots, x_n]$, so $R \neq 0$ and R contains a maximal ideal $\mathfrak{m}$. Then $R/\mathfrak{m}$ is a field of finite type over k, so by the previous result 11.3, $R/\mathfrak{m}$ is finite over k. Since k is algebraicly closed and the only finite extension of an algebraicly closed field is the field itself, it must be that $R/\mathfrak{m} = k$. We have a homomorphism of k-algebras

$$k[x_1, \ldots, x_n] \twoheadrightarrow R \twoheadrightarrow R/\mathfrak{m} = k.$$

[6] Note that here $k[x_1, \ldots, x_n]$ means the polynomial ring, not the smallest subring containing k and some elements x_i.

Let $a_1, \dots, a_n \in k$ be the images of the elements $x_1, \dots, x_n$. Clearly $f_1, \dots, f_r$ map to 0 in k; that is, $f_i(a_1, \dots, a_n) = 0$ for every i. ∎

16/11

Definition. The *Jacobson radical* of a ring R is the intersection of all maximal ideals in R.

Recall that, in any ring, the nilradical is the intersection of all prime ideals (Theorem 1.6). In general, the nilradical won't be the Jacobson radical, but that does turn out to be the case for one class of rings.

Lemma 11.5. The Jacobson radical of an algebra of finite type over a field is the nilradical.

In particular, a local ring typically won't be of finite type over a field.

Proof. Let R be an algebra of finite type over a field k. We have to show that if an element $f \in R$ belongs to all maximal ideals of R then f belongs to all prime ideals. We can just replace R by $R/\mathfrak{p}$ for any prime ideal $\mathfrak{p} \subset R$, so it suffices to show that, if R is a domain of finite type over a field, k and $f \in R$ belongs to all maximal ideals, then $f = 0$. Suppose this is the case, but $f \neq 0$. Then $R[1/f]$ is also a domain of finite type over k, so $R[1/f]$ has a maximal ideal $\mathfrak{m}$. Notice that $R[1/f]/\mathfrak{m}$ is a field of finite type over k, so $R[1/f]/\mathfrak{m}$ is finite over k by the first weak version of the Nullstellensatz (Theorem 11.3). Put

$$\mathfrak{n} = \ker(R \hookrightarrow R[1/f] \twoheadrightarrow R[1/f]/\mathfrak{m}).$$

The map $R/\mathfrak{n} \to R[1/f]/\mathfrak{m}$ is an injection, so $R/\mathfrak{n}$ is a k-subspace of the finite-dimensional k-vector-space $R[1/f]/\mathfrak{m}$. Therefore $R/\mathfrak{n}$ is finite over k. Since $R/\mathfrak{n}$ is a domain of finite type over a field (clearly $\mathfrak{n}$ is prime in R), it must be a field (see Example Sheet 1). So $\mathfrak{n}$ is a maximal ideal in R; but $f \notin \mathfrak{n}$ since f maps to a unit in $R[1/f]$, so not to 0 in $R[1/f]/\mathfrak{m}$. ∎

Theorem 11.6 (Hilbert Nullstellensatz, strong form)**.** For an ideal I in a polynomial ring $k[x_1, \dots, x_n]$ with k algebraicly closed, define

$$Z(I) := \{(a_1, \dots, a_n) \in k^n : f(a_1, \dots, a_n) = 0 \ \forall f \in I\}.$$

Then the ideal of polynomials that vanish on $Z(I) \subseteq k^n$ is the ideal $\operatorname{rad}(I)$.

This fails badly for k not algebraicly closed; e.g., $I = (x^2 + 1)$ in $\mathbb{R}[x]$.

Proof. Let J be the ideal of polynomials that vanish on $Z(I)$. Clearly $I \subseteq J$, so $\operatorname{rad}(I) \subseteq J$. (If $f \in k[x_1, \dots, x_n]$ has, for some $r \geq 1$, f^r vanishes on $Z(I) \subseteq k^n$, then f vanishes on $Z(I)$.) We want to show that $\operatorname{rad}(I) = J$. Let $R = k[x_1, \dots, x_n]/\operatorname{rad}(I)$. Then R is a k-algebra of finite type, so by Lemma 11.5 its Jacobson radical is its nilradical, which is 0. Let f be a polynomial not in $\operatorname{rad}(I)$; we want to show that $f \notin J$. Then f is a nonzero element of R, so there is some maximal ideal $\mathfrak{m} \subset R$ with $f \notin \mathfrak{m}$. The weak Nullstellensatz 11.4 implies that the maximal ideals in $k[x_1, \dots, x_n]$ (with k algebraicly closed) correspond to the elements of k^n: the point $(a_1, \dots, a_n) \in k^n$ corresponds to the maximal ideal $(x_1 - a_1, \dots, x_n - a_n)$. So $\mathfrak{m}$ corresponds to a point $(a_1, \dots, a_n) \in k^n$ with $f(a_1, \dots, a_n) \neq 0$ and $(a_1, \dots, a_n) \in Z(I)$. ∎

Summary of Nullstellensatz.

(1) For k algebraicly closed, the set of closed points in A^n_k is k^n.

(2) For any field k, all points in A^n_k are in one-to-one correspondence with irreducible closed subsets of $\operatorname{Max} k[x_1, \dots, x_n]$.

12 Artinian rings

Recall that a ring is *artinian* if it satisfies the descending chain condition on ideals. Artinian rings are generally uncomplicated, so here we can give a fairly complete description of them.

Lemma 12.1. In any artinian ring, every prime ideal is maximal.

Proof. Let $\mathfrak{p}$ be a prime ideal in an artinian ring R. Then $R/\mathfrak{p}$ is an artinian domain. Let x be a nonzero element in $R/\mathfrak{p}$. The sequence

$$(x) \supseteq (x^2) \supseteq (x^3) \supseteq \cdots$$

terminates; i.e., there is $n > 0$ such that $(x^n) = (x^{n+1})$. So there is an element $a \in R/\mathfrak{p}$ such that $x^{n+1}a = x^n$. Here $x^n \neq 0$ since $x \neq 0$ and $R/\mathfrak{p}$ is a domain, so $xa = 1$, as $R/\mathfrak{p}$ is a domain. Therefore x is a unit in $R/\mathfrak{p}$. We conclude that $R/\mathfrak{p}$ is a field. ∎

The geometric interpretation of this lemma is that in the spectrum of an artinian ring, points are closed.

Lemma 12.2. An artinian ring has only finitely many maximal ideals.

Proof. Let R be an artinian ring, and suppose there are infinitely many maximal ideals. Choose a sequence $\mathfrak{m}_1, \mathfrak{m}_2, \ldots$ of *distinct* maximal ideals. The sequence

$$\mathfrak{m}_1 \supseteq \mathfrak{m}_1 \cap \mathfrak{m}_2 \supseteq \mathfrak{m}_1 \cap \mathfrak{m}_2 \cap \mathfrak{m}_3 \supseteq \cdots$$

terminates: there is $n > 0$ such that $\mathfrak{m}_1 \cap \cdots \cap \mathfrak{m}_n = \mathfrak{m}_1 \cap \cdots \cap \mathfrak{m}_{n+1}$. That is,

$$\mathfrak{m}_1 \cap \cdots \cap \mathfrak{m}_n \subseteq \mathfrak{m}_{n+1}.$$

Recall that if $I \cap J \subseteq \mathfrak{p}$ with $\mathfrak{p}$ prime, then $I \subseteq \mathfrak{p}$ or $J \subseteq \mathfrak{p}$. (See the proof of Theorem 1.5, item (3).) Since $\mathfrak{m}_{n+1}$ is prime, $\mathfrak{m}_{n+1}$ must contain one of $\mathfrak{m}_1, \mathfrak{m}_2, \ldots, \mathfrak{m}_n$. This is a contradiction, as we assumed the $\mathfrak{m}_i$ were distinct. ∎

Lemma 12.3. In an artinian ring R, the nilradical is nilpotent. That is, $\mathrm{rad}(0)^N = 0$ for some N.

Proof. The sequence

$$\mathrm{rad}(0) \supseteq \mathrm{rad}(0)^2 \supseteq \cdots$$

must terminate, so there is a positive integer N with $\mathrm{rad}(0)^N = \mathrm{rad}(0)^{N+1} = \cdots$. Let $I = \mathrm{rad}(0)^N$ and suppose that $I \neq 0$. Consider the set Σ of all ideals J such that $IJ = 0$, partially ordered by $\subseteq$. Clearly $\Sigma \neq \varnothing$, because $(1) \in \Sigma$. Since R is artinian, the set Σ must have a minimal element J. (In fact, every nonempty set of ideals in an artinian ring must have a minimal element.) Since $IJ \neq 0$, there is $x \in J$ such that $xI \neq 0$. Then $(x) \in \Sigma$, and $(x) \subseteq J$, so the minimality of J guarantees $(x) = J$. We have $(xI)I = xI^2 = xI \neq 0$, so the ideal xI also belongs to Σ. Since $xI \subseteq (x)$, the minimality of $(x) = J$ guarantees $xI = (x)$. That is, we can write $x = xy$ for some element $y \in I$. So we have equations

$$x = xy = xy^2 = \cdots.$$

But y belongs to $I = \mathrm{rad}(0)^N$, so y is nilpotent. But then $x = 0$, a contradiction. ∎

Definition. In any ring a *chain of prime ideals of length r* is a chain of the form

$$\mathfrak{p}_0 \subsetneq \mathfrak{p}_1 \subsetneq \cdots \subsetneq \mathfrak{p}_r$$

for prime ideals $\mathfrak{p}_i$. The (*Krull*) *dimension* of a ring is the supremum of the lengths of all chains of prime ideals.[7] (Thus $\dim(R)$ for $R \neq 0$ is a natural number or ∞.)

Geometrically, we say the *dimension of the affine scheme X* is the supremum of the lengths of all chains of irreducible closed subsets.

Example. A field has dimension 0.

The ring $\mathbb{Z}$ has dimension 1: $0 \subsetneq (2)$ or $0 \subsetneq (3)$, etc., are the longest chains.

Example. Clearly $\dim(A^2_k) \geq 2$, since a point, the affine line A^1_k, and the plane form a chain of length 2.

Exercise. If R is nonzero, then $\dim(R) = 0$ if and only if all prime ideals in R are maximal.

Theorem 12.4. A nonzero ring is artinian if and only if it is noetherian of dimension 0.

Proof. First suppose that R is artinian. Clearly $\dim(R) = 0$ by the exercise above. To show R is noetherian, let $\mathfrak{m}_1, \ldots, \mathfrak{m}_n$ be maximal ideals in R. In any ring, the nilradical is the intersection of the prime ideals, so $\mathrm{rad}(0) = \mathfrak{m}_1 \cap \cdots \cap \mathfrak{m}_n$ in R. So by Lemma 12.3, there is $b > 0$ such that

[7] After Wolfgang Krull, 1899–1971.

$(\mathfrak{m}_1 \cap \cdots \cap \mathfrak{m}_n)^b = 0$. The containment $\mathfrak{m}_1 \cdots \mathfrak{m}_n \subseteq \mathfrak{m}_1 \cap \cdots \cap \mathfrak{m}_n$ always holds, so we have

$$\mathfrak{m}_1{}^b \cdots \mathfrak{m}_n{}^b = 0.$$

18/11

Consider the chain of ideals

$$R \supseteq \mathfrak{m}_1{}^1 \supseteq \mathfrak{m}_1{}^2 \supseteq \cdots \supseteq \mathfrak{m}_1{}^b \supseteq \mathfrak{m}_1{}^b \mathfrak{m}_2 \supseteq \cdots \supseteq \mathfrak{m}_1{}^b \cdots \mathfrak{m}_n{}^b = 0.$$

Here each quotient has the form $I/\mathfrak{m}I$ for some maximal ideal $\mathfrak{m}$. This $I/\mathfrak{m}I$ is a $(R/\mathfrak{m})$-vector space which satisfies DCC on $(R/\mathfrak{m})$-linear subspaces. But every vector space is free (i.e., has a basis), so $I/\mathfrak{m}I$ is finite-dimensional as an $(R/\mathfrak{m})$-vector space. Therefore $I/\mathfrak{m}I$ also satisfies ACC on $(R/\mathfrak{m})$-linear subspaces, so R satisfies ACC on submodules. That is, R is noetherian.

For the converse, the proof is very similar. Let R be a noetherian ring of dimension 0. That is, every prime ideal in R is maximal. Since R is noetherian (recall Corollary 8.9), we can write $\mathrm{rad}(0) = \mathfrak{m}_1 \cap \cdots \cap \mathfrak{m}_n$ for some prime (hence maximal) ideals $\mathfrak{m}_i$. By Lemma 8.10, $(\mathrm{rad}(0))^b = 0$ for some b, since R is noetherian. Then we have $\mathfrak{m}_1{}^b \cdots \mathfrak{m}_n{}^b = 0$. Consider some filtration of R as in our proof of the 'only if' direction. Then each subquotient of such a filtration satisfies ACC, hence DCC, so R is artinian. ∎

13 Discrete valuation rings and Dedekind domains

Definition. A *discrete valuation* on a field k is a surjective function $v\colon k \to \mathbb{Z} \cup \{\infty\}$ satisfying each of the following:

(1) $v(x) = \infty$ if and only if $x = 0$;

(2) $v(xy) = v(x) + v(y)$ for all $x, y \in k$;

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

Exercise. If (k, v) is a field with a discrete valuation, then the set $R = \{x \in k : v(x) \geq 0\}$ is a subring of k, called the *valuation ring* of v. (In particular, you'll have to show that $v(1) = 0$ and $v(-x) = v(x)$.)

Examples. (1) For each prime p one can define a valuation on $\mathbb{Q}$ by $v(p^i \frac{a}{b}) = i$, where a and b are coprime to p (and $v(0) = \infty$).

(2) Let k be a field. Let f be an irreducible polynomial in $k[x_1, \ldots, x_n]$. Then the function v_f defined on the field $k(x_1, \ldots, x_n)$ of rational functions by

$$v_f(f^i \tfrac{a}{b}) = i,$$

where $a, b \in k[x_1, \ldots, x_n] \smallsetminus (f)$, is a valuation on $k(x_1, \ldots, x_n)$.

The valuation ring in (1) is the localisation $\mathbb{Z}_{(p)}$, and the valuation ring in (2) is the localisation $k[x_1, \ldots, x_n]_{(f)}$.

A domain R is a *discrete valuation ring* (*dvr*) if there is a valuation v on $K = \mathrm{Frac}(R)$ for which R is the valuation ring $\{x \in K : v(x) \geq 0\}$.

Let $\mathfrak{m} = \{x \in R : v(x) \geq 0\}$. Then $\mathfrak{m}$ is an ideal in R. Moreover, if $x \in R \smallsetminus \mathfrak{m}$, then $v(x) = 0$, so $\frac{1}{x} \in K$ has valuation $v(\frac{1}{x}) = -v(x) = 0$. So $\frac{1}{x} \in R$; that is, $R \smallsetminus \mathfrak{m}$ consists of unites, so R is a local ring with maximal ideal $\mathfrak{m}$.

Next let x be any element of R of valuation n. (Think of a function that vanishes to order n.) Then $v(\frac{y}{x}) \geq 0$, so $\frac{y}{x} \in R$, so $y \in (x) \subseteq R$. In fact, $(x) = \{y \in R : v(y) \geq n\}$.

Now let I be any ideal in a dvr R. If $I = 0$, then we can choose n to be the least valuation of elements of I. Then it follows that $I = \{y \in R : v(y) \geq n\}$. Thus if we choose an element $t \in R$ of $v(t) = 1$ (which exists by the surjectivity of v) then $(t) = \{y \in R : v(y) \geq 1\}$, so all the ideals in R are 0 and the ideals

$$(1 = t^0) \supsetneq (t) \supsetneq (t^2) \supsetneq \cdots.$$

These ideals are distinct, since $v(t^n) = nv(t) = n$.

Therefore a dvr R is a PID, in particular is noetherian. The prime ideals in R are 0 and (t) (check!). So the maximal ideal in R is (t). We conclude that a dvr is a noetherian local domain of dimension 1.

Theorem 13.1. Let R be a noetherian local domain of dimension 1, with maximal ideal $\mathfrak{m}$. Then the following are equivalent:

(1) R is a dvr;

(2) R is a *regular* local ring, that is $\dim_{R/\mathfrak{m}}(\mathfrak{m}/\mathfrak{m}^2) = 1$;

(3) R is normal.

(Note that (2) is equivalent to the assertion that $\mathfrak{m}$ is principal, by Nakayama (Lemma 7.12).)

Proof. Let R be a noetherian local domain of dimension 1. Since R is a domain, 0 is a prime ideal. Since $\dim(R) = 1$ and R is local, the only two prime ideals in R are 0 and the maximal ideal $\mathfrak{m}$. (Otherwise we get a chain of length 2.)

insert picture here

Let I be any nonzero, proper ideal in R: $I \neq 0, R$. Then $\mathrm{rad}(I)$ must be equal to $\mathfrak{m}$, since $\mathrm{rad}(I)$ is an intersection of prime ideals (Corollary 8.9). Since R is noetherian, we have

$$\mathfrak{m}^n \subseteq I \subseteq \mathfrak{m}$$

for some $n > 0$.

First we show the implication (1)⇒(3): Let R be a dvr with valuation v. To show that a ring is normal, we must show that (R is a domain and) for every element $x \in K = \mathrm{Frac}(R)$, if we can write

$$x^n + a_{n-1}x^{n-1} + \cdots + a_0 = 0 \qquad (\dagger)$$

for some elements $a_i \in R$, then $x \in R$ (i.e., R is integrally closed in $\mathrm{Frac}(R)$). Here $R = \{y \in K : v(y) \geq 0\}$. Suppose $x \in K$ is integral over R and satisfies (†). If $v(x) < 0$, then $v(x^n) = nv(x)$, whereas

$$v(-a_{n-1}x^n - \cdots - a_0) \geq (n-1)v(x),$$

a contradiction. So $v(x) \geq 0$, and R is normal.

For a proof of the implication (3)⇒(2), see Atiyah–MacDonald, Proposition 9.2.

Finally, suppose that R is a regular local ring. That is, the $(R/\mathfrak{m})$-vector space $\mathfrak{m}/\mathfrak{m}^2$ is 1-dimensional. Let $x \in \mathfrak{m} \smallsetminus \mathfrak{m}^2$. Nakayama's lemma (7.12) guarantees that $\mathfrak{m} = (x)$. (Since R and noetherian, $\mathfrak{m}$ is a finitely generated R-module.) It follows that $\mathfrak{m}^n = (x^n)$ for every $n \geq 0$. We have $\mathfrak{m}^n \neq \mathfrak{m}^{n+1}$ for all n; indeed, if not, there would be an element $a \in R$ such that $x^n = x^{n+1}a$, but R is a domain (as $x \neq 0$ since R is not a field). We deduce from this that $1 = xa$, whence x is a unit, contradicting our assumption that $x \in \mathfrak{m}$.

Let y be any nonzero element of R. Is $\bigcap_n \mathfrak{m}^n = 0$? No, because the ideal (y) satisfies

$$\mathfrak{m}^n \subseteq (y) \subseteq \mathfrak{m}$$

for some $n > 0$. So $y \notin \mathfrak{m}^{n+1}$ for such an n. Therefore there is a maximal number j such that $y \in \mathfrak{m}^j$; we define $v(y) = j$. Then y has a nonzero image in $\mathfrak{m}^j/\mathfrak{m}^{j+1}$, which is a 1-dimensional $(R/\mathfrak{m})$-vector space spanned by x^j. By Nakayama we have $(x^j) = \mathfrak{m}^j = (y)$. So (since R is a domain), y is the product of x^j and a unit. That is, every nonzero element y of $\mathrm{Frac}(R)$ is also the product of x^j and a unit for some integer $j \in \mathbb{Z}$; define $v(y) = j$ in this case. Clearly $v(ab) = v(a) + v(b)$. The other condition $v(a+b) \geq \min\{v(a), v(b)\}$ follows from the fact that $R = \{y \in K : v(y) \geq 0\}$ is closed under addition. ∎

21/11

Definition. A *Dedekind domain* is a normal noetherian domain of dimension 1. (That is, in a Dedekind domain, the ideal 0 is prime, and there are some maximal ideals, but no other primes.)

For R a Dedekind domain, every local ring of R at a maximal ideal is a dvr. So we have one valuation of $K = \mathrm{Frac}(R)$ for each maximal ideal in R. E.g., $R = \mathbb{C}[x,y]/(x^2 + y^2 - 1)$.

Examples. (1) Any PID which is not a field is a Dedekind domain. (Recall PID ⇒ UFD ⇒ normal.) So $\mathbb{Z}$ and $k[x]$ are Dedekind domains.

(2) For K a number field, that is a field that is finite as a $\mathbb{Q}$-vector space, the *ring of integers* $\mathcal{O}_K$ in K is the integral closure of $\mathbb{Z}$ in K. ($\mathrm{Frac}(\mathcal{O}_K) = K$, so $\mathcal{O}_K$ is normal.) Here $\mathcal{O}_K$ is finite over $\mathbb{Z}$, hence noetherian. You can check that $\dim(\mathcal{O}_K) = 1$ using results on finite morphisms.

Such a ring need not be a PID or factorial. The failure of this is measured by the Picard group $\mathrm{Pic}(\mathcal{O}_K)$, the "ideal class group of K", which is the group of line bundles on $\mathrm{Spec}\, K$ under the tensor product $\otimes$.

(3) Let X be a smooth affine algebraic curve over a field k. (We haven't defined *smooth* in general, but a ring of dimension 1 is *smooth* if $\dim(\mathfrak{m}/\mathfrak{m}^2) = 1$ for every maximal ideal $\mathfrak{m} \subseteq \mathcal{O}(X)$.) Then $\mathcal{O}(X)$ is a Dedekind domain. It is a PID (or a UFD) if and only if $\mathrm{Pic}(X) = 0$, which is the case for k algebraicly closed if and only if the smooth compactification of X has genus 0.

13.1 Krull's Principal Ideal Theorem

Atiyah–MacDonald uses the notion of completeness for a ring and Hilbert polynomials to approach dimension theory. Our approach is more efficient, but the notions discussed in Atiyah–MacDonald are important.

Definition. Let $\mathfrak{p}$ be a prime ideal in a ring R. The *codimension* $\mathrm{codim}(\mathfrak{p})$ of $\mathfrak{p}$ is the supremum of lengths of all chains of prime ideals contained in $\mathfrak{p}$.

Geometrically, think of the codimension as the supremum of lengths of chains of irreducible closed subsets $V(\mathfrak{q})$ containing $V(\mathfrak{p})$ in $\mathrm{Spec}(R)$. Thus codimension measures how far $V(\mathfrak{p})$ is from all of $\mathrm{Spec}(R)$. Recall that prime ideals in $R_\mathfrak{p}$ correspond bijectively to prime ideals in R contained in $\mathfrak{p}$, so $\mathrm{codim}(\mathfrak{p}) = \dim(R_\mathfrak{p})$.

Theorem 13.2 (Krull's Principal Ideal Theorem)**.** Let R be a noetherian ring and $(a) \neq R$ a principal ideal. Then every minimal prime containing (a) has codimension ≤ 1.

Recall that minimal primes containing (a) correspond to irreducible components of the variety $\{a = 0\}$ in $\mathrm{Spec}(R)$, so this theorem disallows irreducible components of $\{a = 0\}$ of large codimension. (A closed point would be a likely candidate for such an irreducible component (and so would be unlikely to occur).)

Proof. Let $\mathfrak{p}$ be a minimal prime ideal containing (a). We want to show that $\dim R_\mathfrak{p} \leq 1$. We're given that the ideal $(a) \subseteq R_\mathfrak{p}$ has $\mathfrak{p}R_\mathfrak{p}$ as a minimal prime over (a), but $\mathfrak{p}R_\mathfrak{p}$ is the only maximal ideal in the local ring $R_\mathfrak{p}$. This means that $\mathfrak{p}R_\mathfrak{p}$ is the only prime in $R_\mathfrak{p}$ that contains (a). Write R for $R_\mathfrak{p}$ from now on.

We now have the following situation: R is a noetherian local ring with maximal ideal $\mathfrak{m}$, $a \in R$, and $\{a = 0\} \subseteq \mathrm{Spec}(R)$ is the closed point in $\mathrm{Spec}(R)$. We want to show that $\dim R \leq 1$. Equivalently, we can show that any prime $\mathfrak{q} \neq \mathfrak{m}$ has codimension 0. (That is, there is no prime strictly smaller than $\mathfrak{q}$.) In particular, $a \notin \mathfrak{q}$. Let $\mathfrak{q}^{(i)}$ be the inverse image of $\mathfrak{q}^i R_\mathfrak{q}$ in R, called the ith *symbolic power* of $\mathfrak{q}$. Consider the following sequence of ideals in R:

$$(a) + \mathfrak{q}^{(1)} \supseteq (a) + \mathfrak{q}^{(2)} \supseteq \cdots \qquad (\star)$$

Since $\mathfrak{m}$ is the only prime ideal in R that contains (a), the quotient ring $R/(a)$ has only one prime ideal. So $R/(a)$ has dimension 0, so is artinian. Therefore the sequence $(\star)$ must terminate: there is a positive integer n such that $(a) + \mathfrak{q}^{(n)} = (a) + \mathfrak{q}^{(n+1)}$; i.e., any element $q \in (a) + \mathfrak{q}^{(n)}$ can be written as $q = ra + q'$ for some elements $r \in R$ and $q' \in \mathfrak{q}^{(n+1)}$. By the definition of $\mathfrak{q}^{(n)}$, since $q - q' = ra \in \mathfrak{q}^{(n)}$ and $a \notin \mathfrak{q}$, we have $r \in \mathfrak{q}^{(n)}$. Thus we have

$$\mathfrak{q}^{(n)} = a\mathfrak{q}^{(n)} + \mathfrak{q}^{(n+1)}.$$

By Nakayama's lemma (7.12) the finitely generated R-module $\mathfrak{q}^{(n)}/\mathfrak{q}^{(n+1)}$ is 0 (since $a \in \mathfrak{m} \subseteq R$). Consequently $\mathfrak{q}^n R_\mathfrak{q} = \mathfrak{q}^{n+1} R_\mathfrak{q} \subseteq R_\mathfrak{q}$. By Nakayama' lemma again, it must be that $\mathfrak{q}^n R_\mathfrak{q} = 0$. That is, the maximal ideal in $R_\mathfrak{q}$ is nilpotent. So $\dim(R_\mathfrak{q}) = 0$, and $\mathfrak{q}$ has codimension 0, as we wanted. ∎

Corollary 13.3. Let R be a noetherian ring and let $x_1, \ldots, x_c$ be elements of R. Every minimal prime over $(x_1, \ldots, x_c)$ has codimension $\leq c$.

Proof. Let $\mathfrak{p}$ be a minimal prime over $(x_1, \ldots, x_c)$. Localising at $\mathfrak{p}$, we reduce to showing the following: Let R be a noetherian local ring with maximal ideal $\mathfrak{m}$, and let $x_1, \ldots, x_c \in \mathfrak{m}$. Suppose $\mathfrak{m}$ is the only prime in R containing $(x_1, \ldots, x_c)$. We want to show that $\dim R \leq c$. Clearly the quotient ring $R/(x_1, \ldots, x_c)$ has only one prime ideal, so it is artinian. So the ideal $\mathfrak{m} \subset R$ is nilpotent modulo $(x_1, \ldots, x_c)$.

Let

$$\mathfrak{p}_0 \subsetneq \cdots \subsetneq \mathfrak{p}_r$$

be a chain of prime ideals in R. We want to show that $r \leq c$. Without loss of generality we can assume that $\mathfrak{p}_r = \mathfrak{m} \subset R$. Since R is noetherian we can also assume that $\mathfrak{p}_{r-1}$ is maximal among primes not equal to $\mathfrak{p}_r = \mathfrak{m}$. We claim that $\mathfrak{p}_{r-1}$ is a minimal prime ideal over some ideal generated by $c-1$ elements. Then we're done by induction on c: we have $r-1 \leq c-1$, so $r \leq c$ as we want.

Let us prove that claim. Since $\mathfrak{p}_{r-1} \neq \mathfrak{m}$, the ideal $\mathfrak{p}_{r-1}$ cannot contain all of $x_1, \ldots, x_c$. Say $x_1 \notin \mathfrak{p}_{r-1}$. Then the maximal ideal $\mathfrak{m}$ is a minimal prime over $\mathfrak{p}_{r-1} + (x_1)$. And so $R/(\mathfrak{p}_{r-1} + (x_1))$ is noetherian of dimension 0, hence artinian. So there is a positive integer n such that ${x_i}^n = a_i x_1 + y_i$ for some $a_i \in R$, $y_i \in \mathfrak{p}_{r-1}$, for $i = 2, \ldots, c$. Therefore the ideal $(x_1, y_2, \ldots, y_c)$ contains a power of $\mathfrak{m}$, and we have arranged that $y_2, \ldots, y_c \in \mathfrak{p}_{r-1}$.

23/11 We know that $\mathfrak{m}$ is a minimal prime over $(x_1, y_2, \ldots, y_c)$, so the image of $\mathfrak{m}$ in the quotient $R/(y_2, \ldots, y_c)$ is a minimal prime over (x_1). By Krull's Principal Ideal Theorem 13.2, the image of $\mathfrak{m}$ in $R/(y_2, \ldots, y_c)$ has codimension 1, since $(y_2, \ldots, y_c) \subseteq \mathfrak{p}_{r-1} \subseteq \mathfrak{p}_r$. Therefore the image of $\mathfrak{p}_{r-1}$ in $R/(y_2, \ldots, y_c)$ has codimension 0. Equivalently, $\mathfrak{p}_{r-1}$ is a minimal prime over the ideal $(y_2, \ldots, y_c)$. By induction on c for this corollary, it follows that $\operatorname{codim} \mathfrak{p}_{r-1} \leq c-1$. Therefore $r \leq c$. ∎

Corollary 13.4. Every noetherian local ring R has finite dimension.

Proof. Since R is noetherian, its unique maximal ideal $\mathfrak{m}$ is finitely generated as an ideal: say $\mathfrak{m} = (x_1, \ldots, x_c)$. By Corollary 13.3 we have $\operatorname{codim} \mathfrak{m} \leq c$. So R has dimension $\leq c$. ∎

Remark.

(1) By Nakayama's lemma (7.12) this proof shows that for R noetherian and local,

$$\dim R \leq \dim_{R/\mathfrak{m}}(\mathfrak{m}/\mathfrak{m}^2).$$

(2) This implies that any prime ideal in any (not necessarily local) noetherian ring has finite codimension.

(3) In 1962 Masayoshi Nagata constructed a noetherian ring of infinite dimension. In such a ring R, there is no upper bound for $\dim R_{\mathfrak{m}}$ at maximal ideals $\mathfrak{m} \subset R$. (See Examples Sheet 3.)

14 Dimension theory for finitely generated algebras over a field

Lemma 14.1. Let k be a field, $n \in \mathbb{N} = \{0, 1, \ldots\}$. Then every maximal ideal in the polynomial ring $k[x_1, \ldots, x_n]$ can be generated by n elements.

Proof. If k is algebraicly closed, then the Nullstellensatz (11.6) says that every maximal ideal $\mathfrak{m} \subset k[x_1, \ldots, x_n]$ is of the form $(x_1 - a_1, \ldots, x_n - a_n)$ for some element $(a_1, \ldots, a_n) \in k^n$.

In general, let $\mathfrak{m}$ be a maximal ideal in $k[x_1, \ldots, x_n]$. Then the field $F := k[x_1, \ldots, x_n]/\mathfrak{m}$ is finite over k by the Nullstellensatz (11.3). For $0 \leq i \leq n$ define

$$F_i := \operatorname{im}(k[x_1, \ldots, x_n] \to F).$$

So we have a chain

$$k = F_0 \subseteq F_1 \subseteq \cdots \subseteq F_n = F.$$

Each F_i is a domain finite over k, so is a field (ES 1, Question 4). And each F_{i+1} is a quotient of F_i by some maximal ideal, so each F_{i+1} is isomorphic to $F_i[x_{i+1}]/(f_{i+1}(x_{i+1}))$ for some $f_{i+1} \in F_i[x_{i+1}]$. (Recall that a polynomial ring in one variable over a field is a PID.) We can think of f_{i+1} as a k-polynomial in the variables $x_1, \ldots, x_i, x_{i+1}$. Then we have

$$F = k[x_1, \ldots, x_n]/(f_1(x_1) = 0,\ f_2(x_1, x_2) = 0, \ldots, f_n(x_1, \ldots, x_n) = 0).$$

Therefore $\mathfrak{m}$ is generated by n elements. ∎

Corollary 14.2. $\dim k[x_1, \ldots, x_n] = n$.

Proof. The chain of prime ideals

$$0 \subset (x_1) \subset (x_1, x_2) \subset \cdots \subset (x_1, \ldots, x_n)$$

shows that $\dim k[x_1,\dots,x_n] \geq n$.

Conversely, we showed that every maximal ideal in $R := k[x_1,\dots,x_n]$ is generated by n elements (14.1), so $\dim R_{\mathfrak{m}} \leq n$ for every maximal ideal $\mathfrak{m} \subset R$. (Notice that the maximal ideal in $R_{\mathfrak{m}}$ is $\mathfrak{m}R_{\mathfrak{m}}$.) But $\dim R = \sup_{\mathfrak{m}} \dim R_{\mathfrak{m}} \leq n$ (where the supremum is taken over all maximal ideals $\mathfrak{m} \subset R$). ∎

Fact from field theory: for any fields $F \subseteq E$, there is some set $I \subseteq E$ such that the subfield $F(x : x \in I)$ of E generated by I and F is isomorphic to the field $F(x : x \in I)$ of F-rational functions in variables from I, and E is algebraic over $F(x : x \in I)$. One shows that $|I|$ is independent of choice of I. In light of this, $|I|$ is defined to be the *transcendence degree* of the field extension E/F and is denoted $\operatorname{tr\,deg}(E/F)$.

Lemma 14.3. Let R be a domain of finite type over a field k. Then $\dim R$ is at most the transcendence degree of $\operatorname{Frac}(R)$ over k.

In fact, $\dim R = \operatorname{tr\,deg}(\operatorname{Frac}(R)/k)$, and we will prove this later.

Proof. By Noether's normalisation lemma 11.2 R is finite over a subring isomorphic to the polynomial ring $k[x_1,\dots,x_n]$ for some $n \in \mathbb{N}$, so $\operatorname{Frac}(R)$ is a finite extension of $\operatorname{Frac}(k[x_1,\dots,x_n]) = k(x_1,\dots,x_n)$. It's an easy fact of field theory that finite extensions of fields are algebraic, so $\operatorname{tr\,deg}(\operatorname{Frac}(R)/k) = n$.

Let

$$\mathfrak{p}_0 \subsetneq \mathfrak{p}_1 \subsetneq \cdots \subsetneq \mathfrak{p}_r$$

be a chain of prime ideals in R. We want to show that $r \leq n$. Restricting to the subring gives a chain of primes in $k[x_1,\dots,x_n]$:

$$\mathfrak{q}_0 \subsetneq \mathfrak{q}_1 \subsetneq \cdots \subsetneq \cdots \mathfrak{q}_n.$$

(The containments are strict by 10.12.) Therefore $r \leq n$ since $\dim k[x_1,\dots,x_n] = n$. ∎

Lemma 14.4. Let X be an affine variety over a field k (that is, X is Spec of a ring of finite type over k.) Let n be the transcendence degree of the function field

$$k(X) := \operatorname{Frac}(\mathscr{O}(X))$$

over k. Let $g \in \mathscr{O}(X)$ and suppose $g \neq 0$. Then any irreducible component Y of $\{g = 0\} \subset X$ satisfies $\operatorname{tr\,deg}(k(Y)/k) = n-1$.

Proof. After replacing X by a standard open subset $\{h \neq 0\} = \operatorname{Spec}(\mathscr{O}(X)[1/h])$, we can assume that $\{g = 0\}$ is irreducible: set $Y = \{g = 0\}$. Write X for that open subset $\{h = 0\}$. We want to show that $\operatorname{tr\,deg}(k(Y)/k) = n-1$.

We first prove this for $X = A^n_k$. Use the Preparation Lemma 11.1: our function $g \in k[x_1,\dots,x_n]$ can be written (after some k-algebra automorphism of $k[x_1,\dots,x_n]$) as

$$g = c{x_n}^e + \sum_{i=0}^{e-1} a_i(x_1,\dots,x_{n-1}){x_n}^i$$

with $c \in k^*$. So the map $Y \to A^{n-1}$ is finite and surjective. Therefore $\mathscr{O}(Y)$ is finite over $k[x_1,\dots,x_{n-1}]$, so $\operatorname{tr\,deg}(k(Y),k) = n-1$.

For the general case, we use Noether's normalisation lemma 11.2 to find a finite surjective morphism $f\colon X \to A^n_k$. Consider the morphism $H = (f,g)\colon X \to A^{n+1}$. The morphism H is finite, since f is finite. Also, because $f\colon X \to A^n_k$ is finite, the element $g \in \mathscr{O}(X)$ satisfies some monic polynomial equation 25/11

$$g^e + a_{e-1}g^{e-1} + \cdots + a_0 = 0,$$

where $a_i \in k[x_1,\dots,x_n]$. That is, H maps X onto a hypersurface (codimension-1 subvariety) in A^{n+1} defined by

$$Z = \{\Phi(x_{n+1}) := (x_{n+1})^n + a_{e-1}(x_{n+1})^{e-1} + \cdots + a_0 = 0\}.$$

Since $\mathscr{O}(X)$ is a domain, we can assume that the polynomial Φ is irreducible. (Φ is still monic in x_{n+1}.) That is, H maps X to an irreducible

hypersurface $Z \subseteq A^{n+1}$ and Z is finite over A^n (because Φ is monic). Since the maps $X \to Z$ and $Z \to A^n$ are finite morphisms and their composite $X \to A^n$ is dominant (equivalently, surjective), it follows that $H\colon X \to Z$ is dominant. (Recall 10.12, which describes the behaviour of prime ideals in the integral extension $\mathscr{O}(A^n) \subseteq \mathscr{O}(Z)$.) The hypersurface $Y = \{g = 0\} \subseteq X$ is the inverse image of $S = \{x_{n+1} = 0\} \subseteq Z$, which by the equation for Z can be described as

$$\begin{aligned} S &= \{\Phi(x_1, \ldots, x_{n+1}) = 0 \text{ and } x_{n+1} = 0\} \\ &= \{a_0(x_1, \ldots, x_n) = 0 \text{ and } x_{n+1} = 0\} \subseteq A^{n+1}. \end{aligned}$$

Here $a_0 \neq 0 \in k[x_1, \ldots, x_n]$ since Φ is irreducible. So S is isomorphic to an irreducible hypersurface in A^{n+1}, so (as we showed in the case $X = A^n$) $\operatorname{tr\,deg}(k(S)/k) = n+1$. But we have a finite surjective morphism $Y \to S$ (a restriction of the finite surjective morphism $X \twoheadrightarrow Z$), so $\mathscr{O}(Y)$ is a finite extension of $\mathscr{O}(S)$. Hence $\operatorname{tr\,deg}(k(Y)/k) = n-1$, as desired. ∎

We can now prove the main results on dimension for algebras of finite type over a field.

Theorem 14.5. Let X be an (irreducible) affine variety over the field k. The following numbers are equal:

(1) the Krull dimension $\dim(X)$;

(2) $\operatorname{tr\,deg}(k(X)/k)$;

(3) the Krull dimension $\dim(\mathscr{O}(X)_{\mathfrak{m}})$ of the localisation at any maximal ideal $\mathfrak{m} \subset \mathscr{O}(X)$.

Recall that, by definition of affine variety, $\mathscr{O}(X)$ is a domain of finite type over k.

Proof. It suffices to show that, for an affine variety X over k we have $\dim(\mathscr{O}(X)_{\mathfrak{m}}) = \operatorname{tr\,deg}(k(X)/k)$ for every maximal ideal $\mathfrak{m} \subset \mathscr{O}(X)$, for $\dim \mathscr{O}(X) = \sup_{\mathfrak{m}} \dim(\mathscr{O}(X)_{\mathfrak{m}})$.

We've shown (cf. 14.3) that

$$\dim(\mathscr{O}(X)_{\mathfrak{m}}) \leq \dim \mathscr{O}(X) \leq \operatorname{tr\,deg}(k(X)/k).$$

To prove the inequality $\operatorname{tr\,deg}(k(X)/k) \leq \dim(\mathscr{O}(X)_{\mathfrak{m}})$ fix a maximal ideal $\mathfrak{m} \subset \mathscr{O}(X)$, that is, a fixed point (corresponding to $\mathfrak{m}$) $p \in X$. We want to produce one chain of subvarieties

$$p = Y_0 \subsetneq Y_1 \subsetneq \cdots \subsetneq Y_n = X,$$

where $n = \operatorname{tr\,deg}(k(X)/k)$. There is nothing to do if $n = 0$, so suppose $n > 0$. We will show that the closed point p is not all of X; suppose, for a contradiction, that $X = \{p\}$. Then $\mathscr{O}(X)$ has only one prime ideal, which must be 0 since $\mathscr{O}(X)$ is a domain. So the ideal 0 is maximal in $\mathscr{O}(X)$; that is, every proper ideal in $\mathscr{O}(X)$ is a domain, so $\mathscr{O}(X)$ is a field. By the Nullstellensatz (Corollary 11.3), $\mathscr{O}(X)$ is finite over k, so we have

$$n = \operatorname{tr\,deg}(k(X)/k) = \operatorname{tr\,deg}(\mathscr{O}(X)/k) = 0,$$

a contradiction. Thus if $n > 0$ the closed point p is not all of X, so there is a *nonzero* regular function $g \in \mathscr{O}(X)$ that vanishes at p. The lemma above (14.4) shows that every irreducible component Y of $\{g = 0\} \subset X$ satisfies $\operatorname{tr\,deg}(k(Y)/k) = n-1$. Pick a component Y containing p. By induction on n, there is a chain of subvarieties of length $n-1$ in Y through p:

$$\{p\} \subsetneq Y_1 \subsetneq \cdots \subsetneq Y_{n-1} \subseteq X.$$

This completes the proof. ∎

Definition. A noetherian ring R is *catenary*[8] if for any pair of prime ideals $\mathfrak{p} \subseteq \mathfrak{q}$ in R, any two maximal chains of primes from $\mathfrak{p}$ to $\mathfrak{q}$ have the same length.

Example. If R is a catenary local ring and $\mathfrak{p} \subset R$ is prime, then it's easy to check that

$$\dim(R) = \dim(R/\mathfrak{p}) + \operatorname{codim}(\mathfrak{p}).$$

This is a nice property of dimension to have, since we think of $\dim(R/\mathfrak{p})$ as measuring the chains from $\mathfrak{p}$ to R and of $\operatorname{codim}(\mathfrak{p})$ as measuring chains from 0 to $\mathfrak{p}$.

[8] In Latin "catena" means "chain".

We've shown that every noetherian local ring has finite dimension (Corollary 13.4), but not every noetherian local ring is catenary. (Nagata provided an example in 1956 — see Reid's book for an outline of the construction.)

Theorem 14.6. All algebras of finite type over a field, and also all localisations of such rings, are catenary.

Notice the localisation of a ring of finite type over a field need not be a ring of finite type over a field. For example, the localisation

$$\mathbb{C}[x]_{(x)} = \mathbb{C}[x][\tfrac{1}{(x-a)} : a \in C,\ a \neq 0]$$

is not finitely generated as a $\mathbb{C}$-algebra.

Proof. Prime ideals in a localisation $R[S^{-1}]$ are in one-to-one correspondence with primes in $R \smallsetminus S$. So if R is catenary, then so is $R[S^{-1}]$.

Let R be an algebra of finite type over a field k. Suppose we're given closed subvarieties $X \subseteq Y \subsetneq \operatorname{Spec} R$; we want to show that any two maximal chains

$$X = X_0 \subsetneq X_1 \subsetneq \cdots \subsetneq X_r = Y$$

of subvarieties have the same length. In fact, we'll show that any such maximal chain of subvarieties has length $r = \dim Y - \dim X$. For any such chain it's clear by the definition of Krull dimension that

$$\dim X_0 < \dim X_1 < \cdots < \dim X_r.$$

So such a chain has length $\leq \dim Y - \dim X$. We need to show that every maximal chain has length $\dim Y - \dim X$. It suffices to show the following: if $S \subsetneq T$ are subvarieties of $\operatorname{Spec}(R)$ with $\dim T - \dim S \geq 2$, then there is an intermediate subvariety V: $S \subsetneq V \subsetneq T$. To show this notice there is a regular function g on T that vanishes on S but is not identically 0 on T. We know that every irreducible component V of $\{g = 0\}$ satisfies $\operatorname{tr\,deg}(k(V)/k) = n - 1$ (Lemma 14.4), so $\dim V = n - 1$. We have $S \subseteq \{g = 0\}$, so S is contained in some irreducible component V of $\{g = 0\}$. Then $\dim S \neq \dim V \neq \dim T$, so $S \subsetneq V \subsetneq T$, as desired. ∎

28/11

15 Regular local rings

We've seen that the dimension of a noetherian local ring $(R, \mathfrak{m})$ is at most $\dim_{R/\mathfrak{m}}(\mathfrak{m}/\mathfrak{m}^2)$. We will argue that this value, $\dim_{R/\mathfrak{m}}(\mathfrak{m}/\mathfrak{m}^2)$, is easy to compute. (In algebraic geometry, the quotient module $\mathfrak{m}/\mathfrak{m}^2$ is called the *Zariski cotangent space*.)

Definition. Say a noetherian local ring R is *regular* if equality holds:

$$\dim_{R/\mathfrak{m}}(\mathfrak{m}/\mathfrak{m}^2) = \dim R.$$

Example. Let $R = k[x_1, \ldots, x_n]_{(x_1,\ldots,x_n)}$, the polynomial ring over k localised at the origin. Then the maximal ideal in R is $\mathfrak{m} = (x_1, \ldots, x_n) \subset R$. So $f \in \mathfrak{m}$ is a rational function on A^n_k that is defined and takes the value 0 at the origin. What is the class of a function f in the quotient $\mathfrak{m}/\mathfrak{m}^2$? Answer: it's given by the *first derivatives* of f at 0: $(\frac{\partial f}{\partial x_1}|_0, \ldots, \frac{\partial f}{\partial x_n}|_0) \in k^n$.

Definition. For $f \in k[x_1, \ldots, x_n]$ over a field k, we define the *partial derivatives of* f on monomials as follows:

$$\frac{\partial}{\partial x_1}({x_1}^{a_1} \cdots {x_n}^{a_n}) = a_1 {x_1}^{a_1 - 1} {x_2}^{a_2} \cdots {x_n}^{a_n}$$

(and similarly for x_i, $i \neq 1$) and extending linearly.

Thus defined, $\frac{\partial}{\partial x_i} : k[x_1, \ldots, x_n] \to k[x_1, \ldots, x_n]$ is a k-linear function, as you can check. Note that $a_1 \in \mathbb{N}$ gives an element of k:

$$a_1 = \underbrace{1_k + \cdots + 1_k}_{a_1 \text{ summands}}.$$

The partial derivative has the usual properties:

$$\frac{\partial}{\partial x_i}(\alpha f + g) = \alpha \frac{\partial f}{\partial x_i} + \frac{\partial g}{\partial x_i},$$

$$\frac{\partial}{\partial x_i}(fg) = f \frac{\partial g}{\partial x_i} + \frac{\partial f}{\partial x_i} g,$$

etc. These facts are easy to show. Exercise!

One can also define the partial derivatives of a rational function, by the usual formulas for $\frac{\partial}{\partial x_i}(\frac{f}{g})$.

Next let X be an affine scheme of finite type over a field k. We can embed X as a closed subscheme of A^n_k, $X \hookrightarrow A^n_k$. (This corresponds to a map $\phi\colon k[x_1,\dots,x_n] \twoheadrightarrow \mathcal{O}(X)$.) Here X will be defined by some equations, $X = \{f_1 = 0,\dots,f_r = 0\} \subseteq A^n_k$. That is, in algebraic terms, $\ker\phi = (f_1,\dots,f_r)$.

Definition. A k-rational point of a k-scheme X is a closed point $p \in X$ whose residue field is k.

(Notice that the residue field of a point in X of finite type over k is always a finite extension of k. (?))

Write $X(k)$ for the set of k-rational points of X. Then for $X \hookrightarrow A^n$,

$$X(k) = \{(a_1,\dots,a_n) \in k^n : f_1(a_1,\dots,a_n) = 0,\dots,f_r(a_1,\dots,a_n) = 0\}$$

(with the situation as in the previous paragraph).

When is the local ring of X at a k-rational point regular? Answer: when X is *smooth*.

Definition. Let X be an affine scheme of finite type over a field k. Choose an embedding $X \hookrightarrow A^{m+n}_k$ as a closed subscheme. We say X is *smooth of dimension n over k* if all irreducible components of X have dimension n, and the matrix of partial derivatives

$$\left(\frac{\partial f_i}{\partial x_j}\right)_{r\times(m+n)}$$

has rank exactly m everywhere on X. (Here the f_i are the defining polynomials for X.)

It is a fact that smoothness of X is independent of the choice of embedding and defining equations.

Remark. Given that $\dim X = n$, we can (equivalently) weaken the requirement to rank $\geq m$.

To be more explicit, an $n \times n$ matrix over a field k has *rank* at least m if and only if there is some $m \times m$ minor in A that is nonzero. Notice that each $m \times m$ minor of the matrix $(\frac{\partial f_i}{\partial x_j})$ is a polynomial in $k[x_1,\dots,x_n]$. The zeroset of each such minor is a closed subset of A^n, hence a closed subset of X. So X is smooth of dimension n if and only if the intersection of these closed subsets of X is empty.

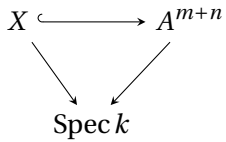
Example. Let k be a field and put $X = \{xy = 0\} \subset A^2$. Then all irreducible components of X have dimension 1, so the matrix of derivatives is

$$\begin{pmatrix}\frac{\partial f_1}{\partial x} & \frac{\partial f_1}{\partial y}\end{pmatrix} = \begin{pmatrix} y & x\end{pmatrix}.$$

So X is smooth if and only if this matrix has rank ≥ 1 everywhere on X, so X is non-smooth over k where $x = y = 0$ and $(x,y) \in X$. (Note the non-smooth locus is a set of points where a bunch of polynomials are 0, so is closed in X.)

Lemma 15.1. Let X be an affine scheme of finite type over a field k. Let $p \in X(k)$ be a k-rational point in X. Then the local ring of X at p is regular if and only if the smooth locus of X (which is an open subset of X) contains p.

Proof. Choose a closed embedding of X into A^{m+n} over k.



Let $n = \dim X$. What is $\mathfrak{m}_p/{\mathfrak{m}_p}^2$, where $\mathfrak{m}_p = \mathcal{O}(X)_p$? (This is equal to the quotient $\mathfrak{m}/\mathfrak{m}^2$ in $\mathcal{O}(X)_p$, where $\mathfrak{m}$ is the maximal ideal corresponding to p.) We claim $\mathfrak{m} \subset \mathcal{O}(X)$ is the image of the maximal ideal $\mathfrak{n} = k[x_1,\dots,x_{m+n}]$ corresponding to p. Let $I = \ker\phi (= (f_1,\dots,f_r))$ in the following diagram:

$$k[x_1,\dots,x_{m+n}] \xrightarrow{\phi} \mathcal{O}(X) \xrightarrow{\text{eval}^{\underline{n}} \text{ at } p} k$$

We have a map $R \twoheadrightarrow R/I$, where $R = k[x_1, \dots, x_{m+n}]$. Next $\mathfrak{m}^2 \subset R/I$ is the image of $\mathfrak{n}^2 \subset R$. ("This is obvious if you think about it.") So the inverse image of $\mathfrak{m}^2 \subset R/I$ in R is the ideal $\mathfrak{n}^2 + I$. (Think abelian groups: $\operatorname{im} C$ under the map $A \twoheadrightarrow A/B$ is $(B+C)/B \cap C$.) So $\mathfrak{m}/\mathfrak{m}^2 \cong \mathfrak{n}/\mathfrak{n}^2 + I$. Here $\mathfrak{n}/\mathfrak{n}^2$ is a k-vector space of dimension $m+n$ (given by the first derivatives of a function that vanishes at p). So $\mathfrak{m}/\mathfrak{m}^2$ is k^{m+n} modulo the k-linear subspace spanned by

$$\left(\left.\frac{\partial f_1}{\partial x_1}\right|_p, \dots, \left.\frac{\partial f_1}{\partial x_{m+n}}\right|_p \right) \in k^{m+n},$$

$$\vdots$$

$$\left(\left.\frac{\partial f_r}{\partial x_1}\right|_p, \dots, \left.\frac{\partial f_r}{\partial x_{m+n}}\right|_p \right) \in k^{m+n},$$

So the local ring $\mathcal{O}(X)_p$ is regular if and only if the matrix of derivatives $(\frac{\partial f_i}{\partial x_j})$ has rank exactly m, because $\dim_k(\mathfrak{m}/\mathfrak{m}^2) = m+n$. But this is true if and only if X is smooth of dimension n at p.[9] ∎

30/11

15.1 Miscellaneous questions answered

What is the affine line A^1_k for a field k that's not algebraicly closed?

Spec $k[x]$ is the generic point (0) and the closed points (f) for $f \in k[x]$ irreducible (monic, say).

Definition. A polynomial $f \in k[x]$ is *separable* iff it is coprime to its derivative: $\gcd(f, f') = 1$. (Recall that this is equivalent to the condition that f factors as a product of distinct linear terms $(x-a)$ over the algebraic closure $\overline{k}$.)

Definition. A field k is *perfect* if either $\operatorname{char} k = 0$ or $\operatorname{char} k = p > 0$ and every element of k is a pth power in k.

[9] Recall we set $n = \dim X$.

For example, $\mathbb{F}_p$ is perfect, $\overline{\mathbb{F}_p}$ is perfect, but $\mathbb{F}_p(x)$ is not perfect.

Remark. If k is perfect, then every irreducible polynomial in $k[x]$ is separable.

Let k be a perfect field, and let $f \in k[x]$ be irreducible (so f is separable). Then in $\overline{k}[x]$ we have

$$f = (x - a_1) \cdots (x - a_n)$$

for some distinct $a_1, \dots, a_n \in \overline{k}$. Then $a_1, \dots, a_n$ form a $\operatorname{Gal}(\overline{k}/k)$-orbit in $\overline{k}$. Recall the *Galois group* $\operatorname{Gal}(\overline{k}/k)$ is the group of automorphisms of the field $\overline{k}$ that fix k pointwise (that is, are the identity on k). Conclusion: if k is perfect, the set of closed points in the affine line A^1_k can be identified with $\overline{k}/\operatorname{Gal}(\overline{k}/k)$, the set of orbits of $\operatorname{Gal}(\overline{k}/k)$ on $\overline{k}$.

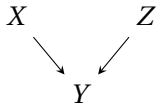
Example. The closed points in $A^1_{\mathbb{R}}$ are $\mathbb{C}/\operatorname{Gal}(\mathbb{C}/\mathbb{R}) = \mathbb{C}/(\mathbb{Z}/2)$, which can be identified with the closed upper half-plane in $\mathbb{C}$. The monic irreducible polynomials in $\mathbb{R}$ are $x - a$ for $a \in \mathbb{R}$ and $x^2 + bx + c$ with $b^2 - 4c < 0$.

What is the geometric meaning of $M \otimes_A C$ or $A \otimes_B C$?

A finitely generated projective A-module M corresponds geometrically to a vector bundle on Spec(A), and elements of M are *sections* of the vector bundle over Spec(A).

A ring homomorphism $A \to B$ corresponds to a morphism $f\colon \operatorname{Spec} B \to \operatorname{Spec} A$ of affine schemes, and f^*M corresponds to $M \otimes_A B$ ("pullback of vector bundles"). Under this correspondence, $M \otimes_A A/\mathfrak{m}$ is the fibre of M at $\mathfrak{m}$.

For rings and homomorphisms $B \to A$ and $B \to C$, we have morphisms of affine schemes



Then $\operatorname{Spec}(A \otimes_B C) = X \times_Y Z$, where $\times_Y$ is fibre product of affine schemes. For example, $\operatorname{Spec}(k[x] \otimes_k k[y]) = A^1_k \times_{\operatorname{Spec} k} A^1_k = A^2_k$. (Recall $k[x] \otimes_k k[y] \cong k[x,y]$.)

What is the geometric meaning of normality?

Let R be a domain. Recall that, by definition, R is normal iff R is integrally closed in $\operatorname{Frac}(R)$. Equivalently: for any finite extension $R \subseteq S$ of domains such that $\operatorname{Frac}(R) = \operatorname{Frac}(S)$, it must be that $R = S$. Assume now that R is a domain of finite type over a field. Then $X = \operatorname{Spec}(R)$ is normal iff every finite *birational* morphism $f\colon Y \to X$ of affine varieties is an isomorphism. (Geometrically, a morphism of varieties over a field k is *birational* iff it restricts to an isomorphism from some dense open subset of X to some dense open subset of Y.)

Example. The variety $X = \{x^2 = y^3\} \subset k^2$ is not normal (is "abnormal"?) since we can write down a finite birational morphism to X which is not an isomorphism, namely $A^1_k \to X$, $t \mapsto (t^3, t^2)$.

But, for instance, A^1_k is normal. There are finite morphisms to A^1_k that are not isomorphisms, but they cannot be birational (e.g., the map $A^1_k \to A^1_k$, $t \mapsto t^2$ is finite, but not birational).

15.2 Regular local rings, concluded

Examples. (1) The local ring $\mathbb{Z}_{(p)}$ is a regular local ring of dimension 1 (equivalently, a dvr: Recall Theorem 13.1).

(2) $k[x_1,\dots,x_n]_{(x_1,\dots,x_n)}$ is a regular local ring of dimension n.

(3) The power series ring $k[\![x_1,\dots,x_n]\!]$ is a regular local ring of dimension n with maximal ideal $\mathfrak{m} = (x_1,\dots,x_n)$.

(4) The ring $\mathbb{Z}_p$ of p-adic integers (i.e., the inverse limit $\varprojlim_n \mathbb{Z}/p^n$) is a regular local ring of dimension 1, with maximal ideal $\mathfrak{m} = (p)$.

Theorem 15.2. Let X be a smooth affine scheme of dimension n??? over a field k. Then every local ring of X (not just at closed points!) is regular.

Notice that for $R = \mathcal{O}(X)$ and $\mathfrak{p} \subset R$ prime, we have $\dim R_{\mathfrak{p}} = \operatorname{codim}(\mathfrak{p})$.

Insert picture of cone & stuff here

Geometrically this theorem means that if X is smooth of dimension n, $Y \subset X$ is a subvariety of codimension r, then Y is defined over a dense open subset by only r equations ("complete intersection").

Theorem 15.3 (Auslander–Buchsbaum 1959)**.** Every regular local ring is a factorial domain (UFD).

In light of this theorem, we have a string of implications

$$\text{regular local ring} \Rightarrow \text{factorial domain} \Rightarrow \text{normal domain} \Rightarrow \text{domain}.$$

The proof of Theorem 15.3 uses homological algebra (Ext & Tor). If you're interested, see Eisenbud's book or Kaplansky's *Fields and rings*.

Corollary 15.4. Let X be a smooth affine variety of dimension n over a field k. Then let $Y \subset X$ be a codimension-1 subvariety. The local ring $\mathcal{O}_{X,Y} = \mathcal{O}(X)_{\mathfrak{p}}$ (where $\mathfrak{p}$ corresponds to Y) is a dvr.

So we get a valuation $v\colon k(X) \to \mathbb{Z} \cup \{\infty\}$ that measures the order of zeros along Y of a rational function on X. (Here $\operatorname{Frac}\mathcal{O}(X)_{\mathfrak{p}} = \operatorname{Frac}\mathcal{O}(X) = k(X)$.)

Lemma 15.5. Let R be a factorial domain. Every codimension-1 prime ideal in R is principal.

Proof. Let $\mathfrak{p} \subset R$ be a codimension-1 prime ideal. Here 0 is prime in R, so $\mathfrak{p} \neq 0$ and there is no prime $\mathfrak{q}$ such that $0 \subsetneq \mathfrak{q} \subsetneq \mathfrak{p}$. Since $\mathfrak{p} \neq 0$ there is a nonzero element $f \in \mathfrak{p}$. And f is not a unit, so (since R is factorial) we can write f as a product of irreducible elements: $f = f_1 \cdots f_r$. Since $\mathfrak{p}$ is prime, at least one f_i, say f_1, belongs to $\mathfrak{p}$. Then (f_1) is prime and nonzero, so $\mathfrak{p} = (f_1)$. ∎

Geometrically, this means a codimension-1 subvariety Y of $X = \operatorname{Spec}(R)$ is defined by one equation: $Y = \{f = 0\}$.

Corollary 15.6. Let X be a smooth affine variety over a field k, and suppose $Y \subset X$ is a codimension-1 subvariety. The ideal $I = \ker(\mathcal{O}(X) \to \mathcal{O}(Y))$ is locally generated by 1 element, so I is a locally free $\mathcal{O}(X)$-module of rank 1. Geometrically, that means I corresponds to a line bundle, called $\mathcal{O}(-Y)$, on X.

This correspondence between line bundles and codimension-1 subvarieties is fundamental to algebraic geometry.