commutative algebra

Lectures delivered by Jacob Lurie
Notes by Akhil Mathew

Fall 2010, Harvard

Last updated 12/1/2010

Contents

Lecture 36 11/19

Lecture 37 11/22

Lecture 38 11/24

Lecture 39 11/29

Lecture 40 12/1

Introduction

Jacob Lurie taught a course (Math 221) on commutative algebra at Harvard in Fall 2010. These are my "live-TEXed" notes from the course.

Conventions are as follows: Each lecture gets its own "chapter," and appears in the table of contents with the date. Some lectures are marked "section," which means that they were taken at a recitation session. The recitation sessions were taught by Jerry Wang.

These notes were typeset using LATEX 2.0. I used `vim` to take the notes. I ran the Perl script `latexmk` in the background to keep the PDF output automatically updated throughout class. The `article` class was used for the notes as a whole. The LATEX package `xymatrix` was used to generate diagrams.

Of course, these notes are not a faithful representation of the course, either in the mathematics itself or in the quotes, jokes, and philosophical musings; in particular, the errors are my fault. By the same token, any virtues in the notes are to be credited to the lecturer and not the scribe.

Please email corrections to `amathew@college.harvard.edu`.

Lecture 1
9/1

§1 Unique factorization

Fermat's last theorem states that the equation

$$x^n + y^n = z^n$$

has no nontrivial solutions in the integers. There is a long history, and there are many fake proofs. Factor this expression for n odd. Let ζ be a primitive nth root of unity; then we find

$$(x + y)(x + \zeta y)(x + \zeta^2 y) \dots (x + \zeta^{n-1} y) = z^n.$$

We are tempted to ask how the product decomposition interacts with the power decomposition. The caveat is that though z is an integer, and $x + y \in \mathbb{Z}$, the others actually live in $\mathbb{Z}[\zeta]$.

The problem is the ring $\mathbb{Z}[\zeta]$. While this is a legitmate ring, and we can talk about primes and things like that, and try to factor into primes, things go wrong. Over $\mathbb{Z}$, factorization is unique up to permuting the factors. Over $\mathbb{Z}[\zeta]$, you can still get a decomposition into irreducible factors, but in gneeral it is not unique. The ring does not always have unique factorization. In order to think about the failure of unique factorization, Dedekind introduced the theory of ideal numbers, now called ideals.

Let us look at a failure of unique factorization. Consider $\mathbb{Z}[\sqrt{-5}]$, i.e. complex numbers that look like $a + \sqrt{-5}b, a, b \in \mathbb{Z}$. We can write

$$6 = 2 \times 3 = (1 + \sqrt{-5})(1 - \sqrt{-5});$$

you can convince yourself that these are two fundamentally different factorizations, even though all these are irreducible. So 6 admits a nonunique factorization into irreducibles.

Dedekind was trying to get to the bottom of what was going on. Let us look at the problem. Ideally, if you have a prime factor of 6, and a decomposition $6 = ab$, then that prime factor must divide a or b. This is not true, however. There is a new idea.

Imagine an **ideal number** x such that x divides 2, $1 + \sqrt{-5}$. It doesn't live in the ring $\mathbb{Z}[\sqrt{-5}]$; it can't, because they have no common factor. Yet we can talk about divisibility. We know that 2 and $1 + \sqrt{-5}$ are divisible by x. For instance, $2 + 1 + \sqrt{-5}$ should be divisible by x. We're going to identify x with the set of all numbers divisible by x. This led to the introduction of an ideal.

§2 Basic definitions

1.1 Definition. A **commutative ring** is a set R with an addition map $R \times R \to R$ and a multiplication map $R \times R \to R$ that satisfy all the usual identities. For instance, it should form a group under addition. E.g. $x + y = y + x$, and there are zeros and additive inverses. Actually, I will not write out all the properties.

We do not review the definition of a **subring**, though Lurie did in the class.

1.2 Definition. Let R be a ring. An **ideal** in R is a subset $I \subset R$ ("the set of all elements divisible by something, not necessarily in R") satisfying

1. $0 \in I$
2. $x, y \in I$ implies $x + y \in I$
3. $x \in I, y \in R$, then $xy \in I$.

1.3 Example. If R is a ring, $x \in R$, then the set of things divisible by x (i.e. xR) is an ideal. This is denoted (x). It is in fact the smallest ideal containing x.

You can do some of the same things with ideals as you can do with numbers.

1.4 Definition. If I, J are ideals in a ring R, the product IJ is defined as the smallest ideal containing xy for all $x \in I, y \in J$. More explicitly, this is the set of all expressions

$$\sum x_i y_i$$

for $x_i \in I, y_i \in J$.

1.5 Example. We have $(x)(y) = (xy)$.

1.6 Example. Let $R = \mathbb{Z}[\sqrt{-5}]$. Is there a common factor of 2 and $1 + \sqrt{-5}$? No, we said. But the "common factor" is the ideal

$$(2, 1 + \sqrt{-5})$$

generated by both of them.

This is not trivial (1); this is easy to check (exercise?). However, it is also not principal.

The theory of ideals saves unique factorization.

1.7 Theorem (Dedekind)**.** *Let $R = \mathbb{Z}[\sqrt{-5}]$ or $\mathbb{Z}[\zeta]$ (or more generally, any ring of integers in a finite extension of $\mathbb{Q}$). Let $I \subset R$ be an ideal, nonzero.*

Then I factors uniquely $I = \mathfrak{p}_1 \dots \mathfrak{p}_n$, where the $\mathfrak{p}_i$ are ideals that cannot be factored further, i.e. ***prime****.*

This is a theorem that belongs to a number theory class, but we will talk about it too.

Here are more examples of interesting rings.

§3 Rings of holomorphic functions

There is a fruitful analogy in number theory between $\mathbb{Z}$ and $\mathbb{C}[t]$, the latter being the polynomial ring over $\mathbb{C}$ in one variable. Why are they analogous? Both of these rings have a theory of unique factorization: factorization into primes or irreducible polynomials. (In the latter, the irreducible polynomials have degree one.)

1.8 Example. There is another way of thinking of $\mathbb{C}[t]$ in terms of complex analysis. This is equal to the ring of holomorphic functions on $\mathbb{C}$ which are meromorphic at infinity. Let's draw a picture. (I won't.) Here is the Riemann sphere $\mathbb{C} \cup \{\infty\}$; then the ring $\mathbb{C}[t]$ consists of meromorphic functions on the sphere that have poles at infinity at most. When you describe it in this way, there are generalizations. Let X be a Riemann surface. (Example: take the complex numbers modulo a lattice, i.e. an elliptic curve.) Say that $x \in X$. Define R to be the ring of meromorphic functions on X which are allowed poles only at x (so are everywhere else holomorphic).

1.9 Example. Fix the notations of the previous example. Fix $y \neq x \in X$. Let R be the ring of meromorphic functions on the Riemann surface. Then the collection of functions that vanish at y form an ideal in R. There are lots of other ideals. Instead of fixing y, fix two points $y_0, y_1 \neq x$; we look at the ideal of R that vanish at both y_0, y_1.

For any Riemann surface X, Dedekind's theorem applies. In other words, R has unique factorization of ideals, i.e. is a Dedekind domain.

1.10 Example. Let $f \in R$, nonzero. It may have a pole at x, but no poles elsewhere. f vanishes at finitely many points $y_1, \dots, y_n$. When X was the Riemann sphere, knowing the zeros of f told us something about f, because f was just a polynomial, and we have a nice factorization into functions that vanish only at one point. In general Riemann surfaces, this is not generally possible. This failure turns out to be very interesting.

Let $X = \mathbb{C}/\Lambda$ be an elliptic curve, suppose $x = 0$. Suppose we are given $y_1, y_2, \dots, y_m \in X$ that are nonzero; we ask whether there exists a function f having simple zeros at $y_1, \dots, y_m$ and nowhere else. The answer is interesting, and turns out to recover the group structure on the lattice.

Answer: yes, if and only if $y_1 + y_2 + \cdots + y_n = 0$ (modulo Λ). So this problem of finding a function with specified zeros is equivalent to checking that the specific zeros add up to zero with the group structure.

In any case, there might not be such a nice function, but we have at least an ideal I of functions that have zeros (not necessarily simple) at $y_1, \dots, y_n$. This ideal has unique factorization into the ideals of functions vanishing at y_1, functions vanishing at y_2, so on.

So Dedekind's theory is useful in complex analysis too.

Go back to and recall the ring $\mathbb{C}[t]$. More generally, if R is a ring, $R[t]$ is a ring; this gives another example of a ring. This is a construction that can be iterated, to get a polynomial ring in several variables over R.

1.11 Example. Consider the polynomial ring $\mathbb{C}[x_1, \dots, x_n]$. Recall that before we thought of the ring $\mathbb{C}[t]$ as a ring of meromorphic functions. Similarly each element of the polynomial ring $\mathbb{C}[x_1, \dots, x_n]$ gives a function $\mathbb{C}^n \to \mathbb{C}$; we can think of the polynomial ring as sitting inside the ring of all functions $\mathbb{C}^n \to \mathbb{C}$.

A question you might ask: What are the ideals in this ring? One way to get an ideal is to pick a point $x = (x_1, \dots, x_n) \in \mathbb{C}^n$; consider the collection of all functions $f \in \mathbb{C}[x_1, \dots, x_n]$ which vanish on x; by the usual argument, this is an ideal.

There are, of course, other ideals. More generally, if $Y \subset \mathbb{C}^n$, consider the collection of functions f such that $f = 0$ on Y. This is easily seen to be an ideal in the polynomial ring. We thus have a way of taking a subset of $\mathbb{C}^n$ and producing an ideal. This construction is not injective. Many different subsets can produce the same ideal. Let I_Y be the ideal corresponding to Y.

You can have $Y \neq Y'$ but $I_Y = I_{Y'}$. For instance, if Y is dense in $\mathbb{C}^n$, then $I_Y = (0)$, because the only way a continuous function on $\mathbb{C}^n$ can vanish on Y is for it to be zero.

There is a much closer connection in the other direction. You might ask whether all ideals can arise in this way. The quick answer is no. Not even when $n = 1$. The ideal $(x^2) \subset \mathbb{C}[x]$ cannot be obtained in this way. It is easy to see that the only way we could get this as I_Y is for $Y = \{0\}$, but I_Y in this case is just (x), not (x^2). What's going wrong in this example is that (x^2) is not a *radical* ideal.

1.12 Definition. An ideal $I \subset R$ is **radical** if whenever $x^2 \in I$, then $x \in I$.

The ideals I_Y in the polynomial ring are all radical. This is obvious. You might now ask whether this is the only obstruction. We now state a theorem that we will prove later in this class.

1.13 Theorem (Hilbert's Nullstellensatz)**.** *If $I \subset \mathbb{C}[x_1, \dots, x_n]$ is a radical ideal, then $I = I_Y$ for some $Y \subset \mathbb{C}^n$. In fact, the canonical choice of Y is the set of points where all the functions in Y vanish.*[1]

So this has been a little advertisement for commutative algebra and why you might care about it.

Lecture 2
9/3

§1 R-modules

We will now establish some basic terminology. Suppose R is a ring.

2.1 Definition. An R**-module** M is an abelian group M with a map $R \times M \to M$ such that $(ab)m = a(bm)$, i.e. there is an associative law. Moreover, $1m = m$; the unit acts as the identity. Finally, there should be distributive laws on both sides: $(a + b)m = am + bm$ and $a(m + n) = am + an$.

Another definition is as follows.

2.2 Definition. If M is an abelian group, $End(M) = \{f : M \to M, \text{ homomorphisms}\}$. This is a noncommutative ring, because you can add homomorphisms termwise, and multiply by composition.

2.3 Definition. If R, R' are rings (possibly noncommutative) then $f : R \to R'$ is a **ring-homomorphism** or **morphism** if it is compatible with the ring structure, i.e

1. $f(x + y) = f(x) + f(y)$
2. $f(xy) = f(x)f(y)$

[1] Such a subset is called an algebraic variety.

3. $f(1) = 1$.

The last condition is not redundant because otherwise the zero map would automatically be a homomorphism.

Remark. If R is a ring and $R \to End(M)$ a homomorphism, then M is made into an R-module, and vice versa.

2.4 Example. if R is a ring, then R is an R-module by multiplication on the left.

2.5 Definition. If M is an R-module, a subset $M_0 \subset M$ is a **submodule** if it is a subgroup (closed under addition and inversion) and is closed under multiplication by elements of R, i.e. $aM_0 \subset M_0$ for $a \in R$. A submodule is a module in its own right. There is a commutative diagram explaining this:

$$\begin{tikzcd}
R \times M_0 \arrow[r] \arrow[d] & M_0 \arrow[d] \\
R \times M \arrow[r] & M
\end{tikzcd}$$

2.6 Example. Let R be a (**comm**) ring; then an ideal in R is the same thing as a submodule.

2.7 Example (Construction)**.** Suppose M is an R-module and M_0 a submodule. Then the abelian group M/M_0 (of cosets) is an R-module. If you have a coset $x + M_0 \in M/M_0$, this is multiplied by $a \in R$ to $ax + M_0$. This does not depend on the coset representative.

2.8 Example. If R is a ring and $I \subset R$ an ideal, then R/I is an R-module. The multiplication is $a(b + I) = ab + I$.

This descends further to multiplication

$$R/I \times R/I \to R/I$$

such that there is a commutative diagram

$$\begin{tikzcd}
R \times R/I \arrow[rr] \arrow[dr] & & R/I \\
& R/I \times R/I \arrow[ur] &
\end{tikzcd}$$

In particular, R/I is a ring, under multiplication $(a+I)(b+I) = ab+I$. The reduction map $\phi : R \to R/I$ is a ring-homomorphism with a universal property. The following is that property. For any ring B, there is a map

$$\text{Hom}(R/I, B) \to \text{Hom}(R, B)$$

by composing with the ring-homomorphism ϕ; this map is injective and the image consists of all homomorphisms $R \to B$ which vanish on I.

The reason is that any map $R/I \to B$ pulls back to a map $R \to R/I \to B$ which annihilates I since $R \to R/I$ annihilates I. Conversely, if we have a map

$$f : R \to B$$

killing I, then we can define $R/I \to B$ by sending $a+I$ to $f(a)$; this is uniquely defined since f annihilates I.

Let us introduce a few more basic notions.

2.9 Definition. Let R be a ring. Suppose M, N are R-modules. A map $f : M \to N$ is a **module-homomorphism** if it preserves all the relevant structures.

First, it should be a map of abelian groups, $f(x+y) = f(x) + f(y)$, and second, it preserves multiplication: $f(ax) = af(x)$ for $a \in R, x \in M$.

In this case, the **kernel** $\ker f$ of f, the set of elements killed by f, is a submodule of M, as is easy to see. The **image** $\mathrm{Im} f$ of f (the set-theoretic image, i.e. the collection of all $f(x), x \in M$) is a submodule of N. The **cokernel** of f is defined by

$$N/\mathrm{Im}(f);$$

it's what you get from N by killing off everything that came from M.

§2 Ideals

Now we will introduce terminology related to the theory of ideals.

If R is any ring, there are two obvious ideals. The zero ideal (0) consisting of the zero element, and the unit element (1) consisting of all of R.

2.10 Definition. An ideal $I \subset R$ is said to be **prime** if

1. $1 \notin I$ (by convention, 1 is not a prime number)
2. If $xy \in I$, either $x \in I$ or $y \in I$.

2.11 Definition. An ideal $I \subset R$ is called **maximal**[2] if

1. $1 \notin I$
2. Any larger ideal contains 1 (i.e., is all of R).

2.12 Proposition. *A maximal ideal is prime.*

Proof. First, a maximal ideal doesn't contain 1. We need to show that if $xy \in I$, then one of $x, y \in I$. If $x \notin I$, then $(I, x) = I + (x)$ (the ideal generated by I and x) strictly contains I, so by maximality contains 1. In particular, $1 \in I + (x)$, so we can write

$$1 = a + xb$$

where $a \in I, b \in R$. Multiply both sides by y:

$$y = ay + bxy.$$

[2] Maximal with respect to not being the unit ideal.

Both terms on the right here are in I ($a \in I$ and $xy \in I$), so we find that $y \in I$.

But Lurie did something different to get a contradiction. Suppose $y \notin I$. Then we can write

$$1 = a' + yb'$$

in the same way for $a' \in I$. We have

$$1 = (a + xb)(a' + yb') = aa' + ayb + a'xb + xybb'.$$

Since $xy \in I$, and $a, a' \in I$, everything here is in I, and we find $1 \in I$, contradiction since I is maximal.

Given a ring R, what can we say about the collection of ideals in R. There are two obvious ideals in R, namely $(0), (1)$. These are the same if and only if $0 = 1$, i.e. R is the zero ring. So for any nonzero commutative ring, we have at least two distinct ideals.

▲

Recall: A commutative ring R is called a **field** if $1 \neq 0$ and for every $x \in R - \{0\}$ there exists an inverse $x^{-1} \in R$ such that $xx^{-1} = 1$. This condition has an obvious interpretation in terms of ideals.

2.13 Proposition. *A commutative ring with* $1 \neq 0$ *is a field iff it has only the two ideals* $(1), (0)$ *iff* (0) *is a maximal ideal.*

Proof. It is clear that just have to show that the first two statements are equivalent.

Assume R is a field. Suppose $I \subset R$. If $I \neq (0)$, then there is a nonzero $x \in I$. Then there is an inverse x^{-1}. We have $x^{-1}x = 1 \in I$, so $I = (1)$. In a field, there's no room for ideals other than (0) and (1).

To prove the converse, assume every ideal of R is (0) or (1). Then for each $x \in R$, $(x) = (0)$ or (1). If $x \neq 0$, the first can't happen, so that means that the ideal generated by x is the unit ideal. So 1 is a multiple of x, implying that x has a multiplicative inverse. ▲

So fields also have an uninteresting ideal structure.

2.14 Corollary. *If* R *is a ring and* $I \subset R$ *is an ideal, then* I *is maximal if and only if* R/I *is a field.*

Proof. Well, denote again by $\phi : R \to R/I$ the reduction map. There is a construction mapping ideals of R/I to ideals of R. This sends an ideal to its inverse image. This is easily seen to map to ideals of R containing I. The map from ideals of R/I to ideals of R containing I is a bijection.

Once you have this bijection, it follows that R/I is a field precisely if R/I has precisely two ideals, i.e. precisely if there are precisely two ideals in R containing I, i.e. I is maximal.

▲

There is a similar characterization of prime ideals.

2.15 Definition. A commutative ring R is an **integral domain** if $\forall x, y \in R$, $x \neq 0$ and $y \neq 0$ imply $xy \neq 0$.

2.16 Proposition. *An ideal $I \subset R$ is prime iff R/I is a domain.*

Proof. This is just a matter of translating the definition. Note that being zero in R/I corresponds to being in I, so this is clear. ▲

Remark. Any field is an integral domain. This is because in a field, nonzero elements are invertible, and the product of two invertible elements is invertible. This statement translates in ring theory to the statement that a maximal ideal is prime.

2.17 Definition. A ring R is a **principal ideal domain** or **PID** if $R \neq 0$, R is not a field, R is a domain, and every ideal of R is principal.

These have the next simplest theory of ideals. Each ideal is very simple, though there might be a lot of ideals.

2.18 Example. $\mathbb{Z}$ is a PID. The only nontrivial fact is that:

2.19 Proposition. *Any nonzero ideal $I \subset \mathbb{Z}$ is principal.*

Proof. If $I = (0)$, then this is obvious. Else there is $n \in I - \{0\}$; we can assume $n > 0$. Choose $n \in I$ as small as possible and positive. Then the ideal I is generated by (n). Indeed, we have $(n) \subset I$ obviously. If $m \in I$ is another integer, then divide m by n, to find $m = nb + r$ for $r \in [0, n)$. We find that $r \in I$ and $0 \leq r < n$, so $r = 0$, and m is divisible by n. And $I \subset (n)$.

So $I = (n)$. ▲

Lecture 3
9/8

§1 Localization

Let R be a commutative ring.

3.1 Definition. A subset $S \subset R$ is a **multiplciative subset** if $1 \in S$ and $x, y \in S$ implies $xy \in S$.

We define localization now. Formally this means inverting things.

3.2 Definition. If M is an R-module, we write

$$S^{-1}M = \{m/s, m \in M, s \in S\}$$

modulo an equivalence relation: where $m/s = m'/s'$ if and only if

$$t(s'm - m's) = 0$$

for some $t \in S$. The reason we need to add the t is that otherwise the equivalence relation would not be transitive (i.e. would not be an equivalence relation). So two fractions agree if they agree when clearing denominators and multiplication.

It is easy to check that this is indeed an equivalence relation. Moreover $S^{-1}M$ is an abelian group with the usual addition of fractions

$$\frac{m}{s}+\frac{m'}{s'}=\frac{s'm+sm'}{ss'}$$

and it is easy to check that this is a legitimate abelian group.

Moreover, this is an R-module. We define

$$x(m/s)=(xm)/s.$$

It is easy to check that this is well-defined and makes it into a module. There are distributive laws and so far, which are left to your imagination.

3.3 Example. Let $M=R$. Then $S^{-1}R$ is an R-module, and it is in fact a commutative ring in its own right. This has a ring structure:

$$(x/s)(y/s')=(xy/ss').$$

There is a map $R\to S^{-1}R$ sending $x\to x/1$, which is a ring-homomorphism.

We can, in fact, describe $\phi:R\to S^{-1}R$ by a universal property. Note that for each $s\in S$, $\phi(s)$ is invertible. This is because $\phi(s)=s/1$ which has a multiplicative inverse $1/s$. This property characterizes $S^{-1}R$.

For any commutative ring B, $\mathrm{Hom}(S^{-1}R,B)$ is naturally isomorphic to the subset of $\mathrm{Hom}(R,B)$ that send S to units. The map takes $S^{-1}R\to B$ to the pull-back $R\to S^{-1}R\to B$. The proof of this is very simple. Suppose that $f:R\to B$ is such that $f(s)\in B$ is invertible for each $s\in S$. Then we must define $S^{-1}R\to B$ by sending r/s to $f(r)f(s)^{-1}$. It is easy to check that this is well-defined and that the natural isomorphism as claimed is true.

3.4 Example. Let R be an integral domain and let $S=R-\{0\}$. This is a multiplicative subset because R is a domain. In this case, $S^{-1}R$ is just the ring of fractions by allowing arbitrary nonzero denominators; it is a field, and is called the **quotient field**. The most familiar example is the construction of $\mathbb{Q}$ as the quotient field of $\mathbb{Z}$.

We'd like to generalize this example.

3.5 Example. Let R be arbitrary and $\mathfrak{p}$ is a prime ideal. This means that $1\notin\mathfrak{p}$ and $x,y\in R-\mathfrak{p}$ implies that $xy\in R-\mathfrak{p}$. I.e., the complement S of $\mathfrak{p}$ is multiplicatively closed. We get a ring $S^{-1}R$.

3.6 Definition. This ring is denoted $R_{\mathfrak{p}}$ and is called the **localization at $\mathfrak{p}$.**

This generalizes the previous example (where $\mathfrak{p}=(0)$).

There is a nice property of the rings $R_{\mathfrak{p}}$.

3.7 Lemma. *Let R be a nonzero commutative ring. The following are equivalent:*

1. *R has a unique maximal ideal.*

2. If $x \in R$, then either x or $1-x$ is invertible.

3.8 Definition. In this case, we call R **local**. A local ring is one with a unique maximal ideal.

Pf of the lemma. First we prove (2) $\implies$ (1). We need a sub-lemma.

3.9 Lemma. *Let R be a commutative ring. Then $I \subset R$ be a proper ideal. Then I is contained in a maximal ideal.*

Proof. This requires the axiom of choice in the form of Zorn's lemma. Let P be the collection of all ideals $J \subset R$ such that $I \subset J$ and $J \neq R$. Then P is a poset w.r.t. inclusion. P is nonempty because it contains I. Note that given a (nonempty) linearly ordered collection of ideals $J_\alpha \in P$, the union $\bigcup J_\alpha \subset R$ is an ideal: this is easily seen in view of the linear ordering (if $x, y \in \bigcup J_\alpha$, then both x, y belong to some J_γ, so $x + y \in J_\gamma$; multiplicative closure is even easier). The union is not all of R because it does not contain 1.

This implies that P has a maximal element by Zorn. This maximal element may be called $\mathfrak{M}$; it's a proper element containing I. I claim that $\mathfrak{M}$ is a maximal ideal, because if it were contained in a larger ideal, that would be in P (which can't happen by maximality) unless it were all of R. ▲

3.10 Corollary. *Let R be a nonzero commutative ring. Then R has a maximal ideal.*

Proof. Apply the lemma to the zero ideal. ▲

Now back to the original lemma about local rings. Assume R is such that for each x, either x or $1-x$ is invertible. We will find the maximal ideal. Let $\mathfrak{M}$ be the collection of noninvertible elements of R. This is a subset of R, not containing 1, and it is closed under multiplication. Any proper ideal must be a subset of $\mathfrak{M}$, because otherwise that proper ideal would contain an invertible element.

We just need to check that $\mathfrak{M}$ is closed under addition. Suppose to the contrary that $x, y \in \mathfrak{M}$ but $x + y$ is invertible. We get

$$1 = \frac{x}{x+y} + \frac{y}{x+y} = a + (1-a).$$

Then one of $a, 1-a$ is invertible. So either $x(x+y)^{-1}$ or $y(x+y)^{-1}$ is invertible, which implies that either x, y is invertible, contradiction.

Now prove the reverse direction. This is where we will have to use the lemma on the existence of maximal ideals. Assume R has a unique maximal ideal $\mathfrak{M}$. I claim that $\mathfrak{M}$ consists precisely of the noninvertible elements. The proof of the claim is as follows: $\mathfrak{M}$ can't contain any invertible elements since it is proper. Conversely, suppose x is not invertible, i.e. $(x) \subsetneq R$. Then (x) is contained in a maximal ideal so $(x) \subset \mathfrak{M}$ since $\mathfrak{M}$ is unique. Thus $x \in \mathfrak{M}$.

Suppose $x \in R$; we can write $1 = x + (1-x)$. Since $1 \notin \mathfrak{M}$, one of $x, 1-x$ must not be in $\mathfrak{M}$, so one of those must not be invertible. So (1) $\implies$ (2). The lemma is proved. ▲

Let us give some examples of local rings.

3.11 Example. Any field is a local ring because the unique maximal ideal is (0).

3.12 Example. Let R be any commutative ring and $\mathfrak{p} \subset R$ a prime ideal. Then $R_{\mathfrak{p}}$ is a local ring.

We state this as a result.

3.13 Proposition. *$R_{\mathfrak{p}}$ is a local ring.*

Proof. Let $\mathfrak{m} \subset R_{\mathfrak{p}}$ consist of elements x/s for $x \in \mathfrak{p}$ and $s \in R - \mathfrak{p}$. (Whether something belongs to $\mathfrak{m}$ does not belong to the representation; this is left to the reader.) Then $\mathfrak{m}$ is the unique maximal ideal. We'll prove this in exactly the same way as we just argued.

What can we say about $\mathfrak{m}$? First, note that $\mathfrak{m}$ is an ideal; this is evident since the numerators form an ideal. If $x/s, y/s'$ belong to $\mathfrak{m}$ with appropriate expressions, then the numerator of

$$\frac{xs' + ys}{ss'}$$

belongs to $\mathfrak{p}$, so this sum belongs to $\mathfrak{m}$. Moreover, $\mathfrak{m}$ is a proper ideal because $\frac{1}{1}$ is not of the appropriate form.

We claim that $\mathfrak{m}$ contains all other proper ideals, which will imply that it is the unique maximal ideal. Let $I \subset R_{\mathfrak{p}}$ be any proper ideal. Suppose $x/s \in I$. We want to prove $x/s \in \mathfrak{m}$. In other words, we have to show $x \in \mathfrak{p}$; if not x/s would be invertible, and $I = (1)$, contradiction. This proves locality. ▲

3.14 Example. Let $R = \mathbb{Z}$. This is not a local ring; the maximal ideals are given by (p) for p prime. We can thus construct the localizations $\mathbb{Z}_{(p)}$ of all fractions $a/b \in \mathbb{Q}$ where $b \notin (p)$. So, all rational numbers that don't have powers of p in the denominator.

Remark. Let R be a ring, M an R-module, $S \subset R$ a multiplicatively closed subset. We defined a ring of fractions $S^{-1}R$ and an R-module $S^{-1}M$. But in fact this is a module over the ring $S^{-1}R$. We just multiply $(x/t)(m/s) = (xm/st)$.

Why is this process such a useful one? Let us give a small taste.

3.15 Proposition. *Let $f : M \to N$ be a homomorphism of R-modules. Then f is injective if and only if for every maximal ideal $\mathfrak{m} \subset R$, we have that $f_{\mathfrak{m}} : M_{\mathfrak{m}} \to N_{\mathfrak{m}}$ is injective.*

By definition, $M_{\mathfrak{m}}$ is the localization at $R - \mathfrak{m}$.

There are many variants on this (e.g. replace with surjectivity, bijectivity). This is a general observation that lets you reduce lots of commutative algebra to local rings, which are easier to work with.

Proof. Suppose first that each $f_{\mathfrak{m}}$ is injective. I claim that f is injective. Suppose $x \in M - \{0\}$. We must show that $f(x) \neq 0$. If $f(x) = 0$, then $f_{\mathfrak{m}}(x) = 0$ for every maximal ideal $\mathfrak{m}$. Then by injectivity it follows that x maps to zero in each $M_{\mathfrak{m}}$. We would now like to get a contradiction.

Let $I = \{a \in R : ax = 0 \in M\}$. This is proper since $x \neq 0$. I is contained in some maximal ideal $\mathfrak{m}$. Then x maps to zero in $M_{\mathfrak{m}}$ by the previous paragraph; this means that there is $s \in R - \mathfrak{m}$ with $sx = 0 \in M$. But $s \notin I$, contradiction.

Now let us do the other direction. Suppose f is injective and $\mathfrak{m}$ a maximal ideal; we prove $f_{\mathfrak{m}}$ injective. Suppose $f_{\mathfrak{m}}(x/s) = 0 \in N_{\mathfrak{m}}$. This means that $f(x)/s = 0$ in the localized module, so that $f(x) \in M$ is killed by some $t \in R - \mathfrak{m}$. We thus have $f(tx) = t(f(x)) = 0 \in M$. This means that $tx = 0 \in M$ since f is injective. But this in turn means that $x/s = 0 \in M_{\mathfrak{m}}$. This is what we wanted to show. ▲

Lecture 4
9/10

Today, we will talk about the Zariski topology on the spectrum of a commutative ring.

§1 Spec$R$ and the Zariski topology

4.1 Definition. Let R be a commutative ring. The **spectrum** of R, denoted Spec$R$, is the collection of prime ideals of R.

If $I \subset R$ is an ideal, let

$$V(I) = \{\mathfrak{p} : \mathfrak{p} \supset I\} \subset \mathrm{Spec} R.$$

4.2 Proposition. *There is a topology on* Spec$R$ *such that the closed subsets are of the form $V(I)$ for $I \subset R$ an ideal.*

4.3 Definition. This is called the **Zariski topology**

Proof. Indeed:

1. $\emptyset = V((1))$ because (1) is not prime.

2. Spec$R = V((0))$ because any ideal contains zero.

3. We show the closed sets are stable under intersections. Let $K_\alpha = V(I_\alpha)$ be closed subsets of Spec$R$. Let $I = \sum I_\alpha$. Then

$$V(I) = \bigcap K_\alpha = \bigcap V(I_\alpha),$$

which follows because I is the smallest ideal containing each I_α, so a prime contains every I_α iff it contains I.

4. The closed sets are closed under pairwise unions. If $K, K' \subset$ Spec$R$ are closed, we show $K \cup K'$ is closed. Say $K = V(I), K' = V(I')$. Then we claim:

$$K \cup K' = V(II').$$

Here II' is the ideal generated by products $ii', i \in I, i' \in I'$. If $\mathfrak{p}$ is **prime** and contains II', it must contain one of I, I'; this implies the displayed equation above and implies the result.

▲

4.4 Example. Let $R = Z$. Consider Spec$\mathbb{Z}$. Then every prime is generated by one element, since $\mathbb{Z}$ is a PID. We have that Spec$\mathbb{Z} = (0) \cup \bigcup_{p \text{ prime}} (p)$. The picture is that you have all the primes $(2), (3), (5), \dots$, and then a special point (0).

What are the closed subsets? They are the prime ideals containing (n) for some integer n.

1. If $n = 0$, and the closed subset is all of Spec$\mathbb{Z}$.
2. If $n \neq 0$, and has finitely many prime divisors. So $V((n))$ consists of the prime ideals corresponding to these prime divisors.

The only closed subsets besides the entire space are the finite subsets (not containing (0)).

4.5 Example. Let's say $R = \mathbb{C}[x, y]$ is a polynomial ring in two variables. What is Spec$R$? We won't give a complete answer. But we will write down several prime ideals.

1. For every pair of complex numbers s, t, the collection of polynomials $f \in R$ such that $f(s, t) = 0$ is a prime ideal $\mathfrak{m}_{s,t}$. In fact, it is maximal, as the residue field is all of $\mathbb{C}$. Indeed, $R/\mathfrak{m}_{s,t} \simeq \mathbb{C}$ under the map $f \to f(s, t)$.

   In fact,

   4.6 Theorem (Nullstellensatz)**.** *The $\mathfrak{m}_{s,t}$ are all the maximal ideals in R.*

   Proof. Omitted. ▲

2. $(0) \subset R$ is a prime ideal since R is a domain.
3. If $f(x, y) \in R$ is an irreducible polynomial, then (f) is a prime ideal. This is equivalent to unique factorization in R.[3]

To draw Spec$R$, we start by drawing $\mathbb{C}^2$, the collection of maximal ideals. Spec$R$ has additional points, too. The closed subsets of Spec$R$ are subsets $V(I)$ where I is an ideal, generated by some polynomials $\{f_\alpha(x, y)\}$. You might ask:

> What points of $\mathbb{C}^2$ (with (s, t) identified with $\mathfrak{m}_{s,t}$) lie in $V(I)$?

I.e., when is $I \subset \mathfrak{m}_{s,t}$? This is true iff all the $f_\alpha \in \mathfrak{m}_{s,t}$, i.e. if $f_\alpha(s, t) = 0$ for all α. So the closed subsets of $\mathbb{C}^2$ are precisely the subsets that can be defined by polynomial equations. This is **much** coarser than the usual topology. For instance, $\{(x, y) : Re(x) \geq 0\}$ is not Zariski-closed.

The Zariski topology is so coarse because you only have algebraic data (namely, $R = \text{Spec}R$).

We go back to the case of R any commutative ring. If $I \subset R$, we get a closed subset $V(I) \subset \text{Spec}R$. It is called $V(I)$ because you are supposed to think of it as the places where the elements of I "vanish" if you think of I as functions. But many I's may yield the same $V(I)$.

[3] To be proved later.

4.7 Example. If $R = \mathbb{Z}$ and p is prime, then $I = (p), I' = (p^2)$ define the same subset (namely, $\{(p)\}$) of Spec$R$.

We want to know:

When does $V(I) = V(J)$ for $I \neq J$?

4.8 Definition. If I is an ideal, then the **radical** $\mathrm{Rad}(I) = \sqrt{I} = \{x \in R : x^n \in I \text{ for some } n\}$.

4.9 Lemma. *If I an ideal, so is* $\mathrm{Rad}(I)$.

Proof. Clearly $\mathrm{Rad}(I)$ is closed under multiplication since I is. Suppose $x, y \in \mathrm{Rad}(I)$; we show $x + y \in \mathrm{Rad}(I)$. Then $x^n, y^n \in I$ for some n (large) and all larger n. Then

$$(x+y)^{2n} = x^{2n} + \binom{2n}{1} x^{2n-1}y + \cdots + y^{2n}$$

and every term contains either x, y with power $\geq n$, so every term belongs to I. Thus $(x+y)^{2n} \in I$ and $x + y \in \mathrm{Rad}(I)$. ▲

Remark. If I, J have the same radical $\mathrm{Rad}(I) = \mathrm{Rad}(J)$, then $V(I) = V(J)$.

Proof. Indeed, $V(I) = V(\mathrm{Rad}(I)) = V(\mathrm{Rad}(J)) = V(J)$ by:

4.10 Lemma. *For any I, $V(I) = V(\mathrm{Rad}(I))$.*

Proof. Indeed, $I \subset \mathrm{Rad}(I)$ and $V(\mathrm{Rad}(I)) \subset V(I)$. We have to show the converse inclusion. Namely, we must prove:

If $\mathfrak{p} \supset I$, then $\mathfrak{p} \supset \mathrm{Rad}(I)$.

So suppose $x \in \mathrm{Rad}(I)$; then $x^n \in I \subset \mathfrak{p}$ for some n. But $\mathfrak{p}$ is prime, so whenever a product of things belongs to $\mathfrak{p}$, a factor does. Thus since $x^n = x.x \ldots .x$, we must have $x \in \mathfrak{p}$. So

$$\mathrm{Rad}(I) \subset \mathfrak{p}$$

proving the quoted claim, and thus the lemma. ▲

▲

There is a converse to this remark:

4.11 Proposition. *If $V(I) = V(J)$, then* $\mathrm{Rad}(I) = \mathrm{Rad}(J)$.

So two ideals define the same closed subset iff they have the same radical.

Proof. We write down a formula for $\mathrm{Rad}(I)$ that will imply this at once.

4.12 Lemma.

$$\mathrm{Rad}(I) = \bigcap_{\mathfrak{p} \supset I} \mathfrak{p}.$$

From this, it follows that $V(I)$ determines $\mathrm{Rad}(I)$. This will thus imply the proposition. We now prove the lemma:

Proof. 1. We show $\mathrm{Rad}(I) \subset \bigcap_{\mathfrak{p} \in V(I)} \mathfrak{p}$. In particular, this follows if a prime contains I, it contains $\mathrm{Rad}(I)$; but we have already discussed this above.

2. If $x \notin \mathrm{Rad}(I)$, we show that there is a prime ideal $\mathfrak{p} \supset I$ not containing x. This will imply the reverse inclusion and the lemma.

We want to find $\mathfrak{p}$ not containing x, more generally not containing any power of x. In particular, $\mathfrak{p} \cap \{1, x, x^2 \dots, \} = \emptyset$. This set $S = \{1, x, \dots\}$ is multiplicatively closed. More generally, we will prove:

> Let S be multiplicatively closed in any ring R and let I be any ideal with $I \cap S = \emptyset$. There is a prime ideal $\mathfrak{p} \supset I$ and does not intersect S.

Any ideal missing S can be enlarged to a prime ideal missing S.

This is a fancy version of a previous approach. We showed that any ideal not containing the multiplicatively closed subset $\{1\}$ can be contained in a prime ideal not containing 1.

Note that the quoted statement clearly implies the lemma when applied to $S = \{1, x, \dots\}$.

Let $P = \{J : J \supset I, J \cap S = \emptyset\}$. Then P is a poset w.r.t. inclusion. Note that $P \neq \emptyset$ because $I \in P$. Also, for any nonempty linearly ordered subset of P, the union is in P (i.e. there is an upper bound). We can invoke Zorn's lemma to get a maximal element of P. This element is an ideal $\mathfrak{p} \supset I$ with $\mathfrak{p} \cap S = \emptyset$. I claim that $\mathfrak{p}$ is prime.

Well, first off, $1 \notin \mathfrak{p}$ because $1 \in S$. We need only check that if $xy \in \mathfrak{p}$, then $x \in \mathfrak{p}$ or $y \in \mathfrak{p}$. Suppose otherwise, that neither $x, y \in \mathfrak{p}$. Then $(x, \mathfrak{p}) \notin P$ or $\mathfrak{p}$ would not be maximal. Ditto for $(y, \mathfrak{p})$. In particular, we have that these bigger ideals both intersect S. This means that there are

$$a \in \mathfrak{p}, r \in R \text{ s.t. } a + rx \in S$$

and

$$b \in \mathfrak{p}, r' \in R \text{ s.t. } b + r'y \in S.$$

Now S is multiplicatively closed, so multiply $(a + rx)(b + r'y) \in S$. We find:

$$ab + ar'y + brx + rr'xy \in S.$$

Now $a, b \in \mathfrak{p}$ and $xy \in \mathfrak{p}$, so all the terms above are in $\mathfrak{p}$, and the sum is too. But this contradicts $\mathfrak{p} \cap S = \emptyset$. ▲

▲

The upshot:

> **There is a bijection between the closed subsets of** Spec$R$ **and radical ideals $I \subset R$ (i.e. ideals with $I = \mathrm{Rad}(I)$).**

The construction $R \to \mathrm{Spec}R$ is functorial in R in a contravariant sense. I.e. if $f : R \to R'$, there is a continuous map $\mathrm{Spec}R' \to \mathrm{Spec}R$. This map sends $\mathfrak{p} \subset R'$ to $f^{-1}(\mathfrak{p}) \subset R$, which is easily seen to be a prime ideal in R. Call this map $F : \mathrm{Spec}R' \to \mathrm{Spec}R$.

We need to check that this map is continuous, i.e. F^{-1} sends closed subsets of $\mathrm{Spec} R$ to closed subset of $\mathrm{Spec} R'$. More precisely, if $I \subset R$ and we take the inverse image $F^{-1}(V(I)) \subset \mathrm{Spec} R'$, it is just $V(f(I))$.

This is because if $\mathfrak{p} \in \mathrm{Spec} R'$, then $F(\mathfrak{p}) = f^{-1}(\mathfrak{p}) \supset I$ if and only if $\mathfrak{p} \supset f(I)$. So $F(\mathfrak{p}) \in V(I)$ if and only if $\mathfrak{p} \in V(f(I))$.

4.13 Example. Let R be a commutative ring, $I \subset R$ an ideal, $f : R \to R/I$. There is a map of topological spaces

$$F : \mathrm{Spec}(R/I) \to \mathrm{Spec} R.$$

This map is a closed embedding whose image is $V(I)$. Most of this follows because there is a bijection between ideals of R containing I and ideals of R/I, and this bijection preserves primality.

As an exercise, show that this map is indeed a homeomorphism from $\mathrm{Spec} R/I \to V(I)$.

Lecture 5
[Section] 9/12

§1 The ideal class group

This was taught by X. Wang at a recitation.

5.1 Example. Consider the nonprincipal ideal $I = (2, 1 + \sqrt{-5}) \subset \mathbb{Z}[\sqrt{-5}]$. It is nonprincipal (exercise), but its square is (2), which is principal. So I is not principal, but its square is. How can we make this more general?

In an integral domain R, we define $\mathrm{Cl}(R)$ to be the set of all nonzero ideals $I \subset R$ modulo the relation that $I \sim J$ if there is $\alpha, \beta \in R^*$ such that $\alpha I = \beta J$.

5.2 Definition. We define $\mathrm{Cl}(R)$ to be the **ideal class set** of R.

We need to check that this is a group. Clearly we can define a notion of multiplication by multiplying ideals. The unit ideal is the unit element. But do inverses exist? Given I, is there an ideal J such that

$$IJ \text{ is principal?}$$

§2 Dedekind domains

5.3 Theorem. *Let R be a domain such that:*

1. *R is noetherian (i.e. every ideal is finitely generated).*
2. *Every nonzero prime ideal of R is maximal. (I.e. R has Krull dimension one.)*
3. *R is integrally closed.*

Then the ideal class set is a group.

Proof. We need to prove that for any I, there is another ideal J such that IJ is prinicpal. Pick $I \subset R$. We can assume $I \subsetneq R$. Take an element $\alpha \in I - \{0\}$. If we can find an ideal J such that $IJ = (\alpha)$, we should take J to be the set

$$J = \{x : xI \subset (\alpha)\}.$$

We have $IJ \subset (\alpha)$. Now consider $\mathfrak{b} = \frac{1}{\alpha} IJ$; this is an ideal, because it is a submodule of R. We are to prove that it is equal to R.

Suppose not. Suppose $c \in \mathfrak{b} - \{0\}$. We know that $\mathfrak{b}$ is contained in a maximal ideal $\mathfrak{m}$ since $\mathfrak{b} \neq R$ by assumption. We have a chain of ideals

$$(c) \subset \mathfrak{b} \subset \mathfrak{m}.$$

5.4 Lemma. *If R is noetherian, then every ideal contains a product of nonzero prime ideals.*

Proof. Consider the set of all ideals that do not contain a product of nonzero primes. Then this set S has a maximal element if it is nonempty. Call this element $\mathfrak{n}$. Clearly $\mathfrak{n}$ isn't prime or it wouldn't be in S. This means that there are $a, b \notin \mathfrak{n}$ with $ab \in \mathfrak{n}$. In particular, if we look at the ideals

$$\mathfrak{n} + (a), \mathfrak{n} + (b) \supsetneq \mathfrak{n}$$

then these contain products of primes. So their product

$$(\mathfrak{n} + (a))(\mathfrak{n} + (b)) \subset \mathfrak{n}$$

contains a product of primes. Thus $\mathfrak{n}$ contains a product of primes. ▲

In particular, (c) contains a product of primes $\mathfrak{p}_1 \dots \mathfrak{p}_r$. Suppose r is the minimal possible so (c) does not contain any product of $r-1$ ideals. We have that

$$\mathfrak{p}_1 \dots \mathfrak{p}_r \subset \mathfrak{m}$$

so one $\mathfrak{p}_i$, wlog $\mathfrak{p}_1$, must lie in the prime (and maximal) ideal $\mathfrak{m}$.

But every nonzero prime ideal is maximal, so $\mathfrak{m} = \mathfrak{p}_1$.

5.5 Lemma. *Under the above hypotheses, there is $\gamma \in K - R$ with $\gamma\mathfrak{b} \subset R$.*

Proof. Suppose $r = 1$. We have

$$\mathfrak{m} \supset \mathfrak{b} \supset (c) \supset \mathfrak{p}_1 = \mathfrak{m}.$$

So $\frac{1}{c}\mathfrak{b} \subset R$.

Suppose $r > 1$. We know then that $\mathfrak{p}_2 \dots \mathfrak{p}_r \not\subset (c)$, and we can choose an element $d \in \mathfrak{p}_2 \dots \mathfrak{p}_r - (c)$. Then

$$\frac{d}{c}\mathfrak{b} \subset \frac{d}{c}\mathfrak{m} \subset \frac{1}{c}\mathfrak{p}_2 \dots \mathfrak{p}_r\mathfrak{p}_1 \subset R.$$

▲

So we have something in the fraction field such that when we multiply by it, we get something in R.

Recap: We started with an ideal $I \neq 0 \subset R$ and chose $\alpha \in I - \{0\}$. We took J to be the conductor of I in (α). We took $\mathfrak{b} = \frac{1}{\alpha} IJ$, which we want to prove to be R. Now we have found something outside of R which takes $\mathfrak{b}$ into tiself.

5.6 Lemma. *$\gamma J \subset J$.*

Proof. We need to show

$$\gamma JI \subset (\alpha),$$

i.e.

$$\gamma \frac{IJ}{\alpha} \subset R$$

which we showed earlier as $\mathfrak{b} = \frac{IJ}{\alpha}$. ▲

Now since J is finitely generated, we see that γ is integral over R. (This will be talked about in class.) So $\gamma \in R$, contradiction. ▲

5.7 Definition. A **Dedekind domain** is a domain if it satisfies the above three conditions: it is noetherian, every nonzero prime is maximal, and it is integrally closed.

So in a Dedekind domain, we have a notion of an ideal class group. I.e., $\mathrm{Cl}(R)$ is a group.

5.8 Corollary. *R admits unique factorization into ideals.*

Proof. Exercise. ▲

5.9 Example.

1. $\mathbb{Z}$. More generally, any PID (which is a UFD, hence integrally closed). Any ideal is generated by one element, and every prime is maximal. This is an uninteresting example because the ideal class group is $\{1\}$.

2. The ring of integers of a number field. Let's discuss this.

Recall that a **number field** is a finite extension of $\mathbb{Q}$. An element of a number field K is **integral** if it satisfies a monic polynomial with coefficients in $\mathbb{Z}$. It is known (and probably will be proved in class) that the set of all integral elements form a ring $\mathcal{O}_K$.

5.10 Proposition. *$\mathcal{O}_K$ is a Dedekind domain.*

Proof. $\mathcal{O}_K$ is an integral closure, so it is integrally closed.[4] We cheat again and quote another result:

5.11 Lemma. *There is a finite $\mathbb{Z}$-basis for $\mathcal{O}_K$.*

In particular, $\mathcal{O}_K$ is a finite $\mathbb{Z}$-module, and consequently is a noetherian ring.

We need now only to show that any prime ideal is maximal. Let $\mathfrak{p} \subset \mathcal{O}_K$ be prime; we must show that it is maximal. It is easy to check that $\mathcal{O}_K/\mathfrak{p}$ is a finite integral domain by choosing a triangular $\mathbb{Z}$-basis for $\mathfrak{p}$. But a finite integral domain is a field. ▲

[4] This will be discussed in class! This is not a complete proof.

We denote by h_K the size of the class group $\mathrm{card}\mathrm{Cl}(\mathcal{O}_K)$. This is finite for number fields, which is a very important result.

5.12 Exercise. In the field $K = \mathbb{Q}(\sqrt{-5})$, one can show that the ring of integers is $\mathbb{Z}[\sqrt{-5}]$. The ideal $I = (2, 1 + \sqrt{-5})$ is a nontrivial element of $\mathrm{Cl}(\mathcal{O}_K)$, but its square is trivial.

Using the Minkowski bound, one can show that any ideal is equivalent to any ideal of norm at most two or three, whence it can be shown that I generates $\mathrm{Cl}(\mathcal{O}_K)$.

Note that in the exercise, $\mathcal{O}_K$ was also not a UFD, because 6 admitted two different factorizations. This is no coincidence:

5.13 Proposition. *If R is a Dedekind domain, then R is a UFD if and only if* $\mathrm{Cl}(R) = \{1\}$.

Proof. One way is clear because a PID is a UFD. The other direction is an exercise. ▲

Lecture 6
9/13

§1 A basis for the Zariski topology

Last time, we were talking about the Zariski topology. Let us recall what that is. If R is a commutative ring, then $\mathrm{Spec}R$ is defined to be the collection of prime ideals in R. This has a topology where the closed sets are the sets of the form

$$V(I) = \{\mathfrak{p} \in \mathrm{Spec}R : \mathfrak{p} \supset I\}.$$

There is another way to describe the Zariski topology.

6.1 Definition. If $f \in R$, we let

$$U_f = \{\mathfrak{p} : f \notin \mathfrak{p}\}$$

so that U_f is the subset of $\mathrm{Spec}R$ consisting of primes not containing f. This is the complement of $V((f))$, so it is open.

6.2 Proposition. *The sets U_f form a basis for the Zariski topology.*

Proof. Suppose $U \subset \mathrm{Spec}R$ is open. We claim that U is a union of basic open sets U_f.

Now $U = \mathrm{Spec}R - V(I)$ for some ideal I. Then

$$U = \bigcup_{f \in I} U_f$$

because if an ideal is not in $V(I)$, then it fails to contain some $f \in I$, i.e. is in U_f for that f. Alternatively, we could take complements, whence the above statement becomes

$$V(I) = \bigcap_{f \in I} V((f))$$

which is clear. ▲

The basic open sets have nice properties.

1. $U_1 = \text{Spec}R$ because prime ideals are not allowed to contain the unit element.
2. $U_0 = \emptyset$ because every prime ideal contains 0.
3. $U_{fg} = U_f \cap U_g$ because fg lies in a prime $\mathfrak{p}$ if and only if one of f, g does.

Now let us describe what the Zariski topology has to do with localization.

6.3 Example. Let R be a ring and $f \in R$. Consider $S = \{1, f, f^2, \dots\}$; this is a multiplicatively closed subset. Last week, we defined $S^{-1}R$.

6.4 Definition. For S the powers of f, we write $R[f^{-1}] = S^{-1}R$.

There is a map $\phi : R \to R[f^{-1}]$ and a corresponding map

$$\text{Spec}R[f^{-1}] \to \text{Spec}R$$

sending a prime $\mathfrak{p} \subset R[f^{-1}]$ to $\phi^{-1}(\mathfrak{p})$.

6.5 Proposition. *This map induces a homeomorphism of* $\text{Spec}R[f^{-1}]$ *onto* $U_f \subset \text{Spec}R$*.*

So if you take a commutative ring and invert an element, you just get an open subset of Spec. This is why it's called localization: you are restricting to an open subset on the Spec level when you invert something.

Proof.

1. First, we show that $\text{Spec}R[f^{-1}] \to \text{Spec}R$ lands in U_f. If $\mathfrak{p} \subset R[f^{-1}]$, then we must show that the inverse image $\phi^{-1}(\mathfrak{p})$ can't contain f. If otherwise, that would imply that $\phi(f) \in \mathfrak{p}$; however, $\phi(f)$ is invertible, and then $\mathfrak{p}$ would be (1).

2. Let's show that the map surjects onto U_f. If $\mathfrak{p} \subset R$ is a prime ideal not containing f, i.e. $\mathfrak{p} \in U_f$. We want to construct a corresponding prime in the ring $R[f^{-1}]$ whose inv. image is $\mathfrak{p}$.

   Let $\mathfrak{p}[f^{-1}]$ be the collection of all fractions

   $$\{\frac{x}{f^n}, x \in \mathfrak{p}\} \subset R[f^{-1}],$$

   which is evidently an ideal. Note that whether the numerator is in $\mathfrak{p}$ is **independent** of the representing fraction $\frac{x}{f^n}$ used.[5] In fact, $\mathfrak{p}[f^{-1}]$ is a prime ideal. Indeed, suppose

   $$\frac{a}{f^m}\frac{b}{f^n} \in \mathfrak{p}[f^{-1}].$$

   Then $\frac{ab}{f^{m+n}}$ belongs to this ideal, which means $ab \in \mathfrak{p}$; so one of $a, b \in \mathfrak{p}$ and one of the two fractions $\frac{a}{f^m}, \frac{b}{f^n}$ belongs to $\mathfrak{p}[f^{-1}]$. Also, $1/1 \notin \mathfrak{p}[f^{-1}]$.

   It is clear that the inverse image of $\mathfrak{p}[f^{-1}]$ is $\mathfrak{p}$, because the image of $x \in R$ is $x/1$, and this belongs to $\mathfrak{p}[f^{-1}]$ precisely wehn $x \in \mathfrak{p}$.

[5] Suppose $\frac{x}{f^n} = \frac{y}{f^k}$ for $y \in \mathfrak{p}$. Then there is N such that $f^N(f^k x - f^n y) = 0 \in \mathfrak{p}$; since $y \in \mathfrak{p}$ and $f \notin \mathfrak{p}$, it follows that $x \in \mathfrak{p}$.

3. The map Spec$R[f^{-1}] \to$ Spec$R$ is injective. Suppose $\mathfrak{p}, \mathfrak{p}'$ are prime ideals in the localization and the inverse images are the same. We must show that $\mathfrak{p} = \mathfrak{p}'$.

   Suppose $\frac{x}{f^n} \in \mathfrak{p}$. Then $x/1 \in \mathfrak{p}$, so $x \in \phi^{-1}(\mathfrak{p}) = \phi^{-1}(\mathfrak{p}')$. This means that $x/1 \in \mathfrak{p}'$, so $\frac{x}{f^n} \in \mathfrak{p}'$ too. So a fraction that belongs to $\mathfrak{p}$ belongs to $\mathfrak{p}'$. By symmetry the two ideals must be the same.

4. We now know that the map $\psi : \mathrm{Spec}R[f^{-1}] \to U_f$ is a continuous bijection. It is left to see that it is a homeomorphism. We will show that it is open. In particular, we have to show that a basic open set on the left side is mapped to an open set on the right side. If $y/f^n \in R[f^{-1}]$, we have to show that $U_{y/f^n} \subset \mathrm{Spec}R[f^{-1}]$ has open image under ψ. We'll in fact show what open set it is .

   I claim that
   $$\psi(U_{y/f^n}) = U_{fy} \subset \mathrm{Spec}R.$$

   To see this, $\mathfrak{p}$ is contained in U_{f/y^n}. This mean that $\mathfrak{p}$ doesn't contain y/f^n. In particular, $\mathfrak{p}$ doesn't contain the multiple $yf/1$. So $\psi(\mathfrak{p})$ doesn't contain yf. This proves the inclusion $\subset$.

   To complete the proof of the claim, and the result, we must show that if $\mathfrak{p} \subset \mathrm{Spec}R[f^{-1}]$ and $\psi(\mathfrak{p}) = \phi^{-1}(\mathfrak{p}) \in U_{fy}$, then y/f^n doesn't belong to $\mathfrak{p}$. (This is kosher and dandy because we have a bijection.) But the hypothesis implies that $fy \notin \phi^{-1}(\mathfrak{p})$, so $fy/1 \notin \mathfrak{p}$. Dividing by f^{n+1} implies that
   $$y/f^n \notin \mathfrak{p}$$
   and $\mathfrak{p} \in U_{f/y^n}$.

▲

If Spec$R$ is a space, and f is thought of as a "function" defined on Spec$R$, the space U_f is to be thought of as the set of points where f "doesn't vanish" or "is invertible." Thinking about rings in terms of their spectra is a very useful idea, though we don't make too much use of it.

We will bring it up when appropriate.

Remark. The construction $R \to R[f^{-1}]$ as discussed above is an instance of localization. More generally, we can define $S^{-1}R$ for $S \subset R$ multiplicatively closed. We can define maps
$$\mathrm{Spec}S^{-1}R \to \mathrm{Spec}R.$$

How can you think about the construction in general? You can think of it as
$$\varinjlim_{f \in S} R[f^{-1}]$$
which is a direct limit when you invert more and more elements.

As an example, consider $S = R - \mathfrak{p}$ for a prime $\mathfrak{p}$, and for simplicity that R is countable. We can write $S = S_0 \cup S_1 \cup \dots$, where each S_k is generated by a finite number of elements $f_0, \dots, f_k$. Then $R_{\mathfrak{p}} = \varinjlim S_k^{-1}R$. So we have
$$S^{-1}R = \varinjlim_k R[f_0^{-1}, f_1^{-1}, \dots, f_k^{-1}] = \varinjlim R[(f_0 \dots f_k)^{-1}].$$

The functions we invert in this construction are precisely those which do not contain $\mathfrak{p}$, or where "the functions don't vanish." The idea is that to construct $\mathrm{Spec} S^{-1}R = \mathrm{Spec} R_{\mathfrak{p}}$, we keep cutting out from $\mathrm{Spec} R$ vanishing locuses of various functions that do not intersect $\mathfrak{p}$. In the end, you don't restrict to an open set, but to a direct limit of this.

§2 Localization is exact

Localization is to be thought of as a very mild procedure.

Let us recall:

6.6 Definition. Let $f : M \to N$ be a morphism of R-modules.[6] Suppose $g : N \to P$ is another morphism of R-modules.

The pair of maps is a **complex** if $g \circ f = 0$. So $M \to N \to P$ is zero. In particular, $\mathrm{Im}(f) \subset \ker(g)$.

This complex is **exact** (or exact at N) if $\mathrm{Im}(f) = \ker(g)$. So anything that is killed when you map to P actually comes from something in M.

The next result says how inoffensive localization is.

6.7 Proposition. *Suppose $f : M \to N, g : N \to P$ and $M \to N \to P$ is exact. Let $S \subset R$ be multiplicatively closed. Then*

$$S^{-1}M \to S^{-1}N \to S^{-1}P$$

is exact.

6.8 Corollary. *If $f : M \to N$ is surjective, then $S^{-1}M \to S^{-1}N$ is too.*

Proof. To say that $A \to B$ is surjective is the same as saying that $A \to B \to 0$ is exact. From this the corollary is evident. ▲

Similarly:

6.9 Corollary. *If $f : M \to N$ is injective, then $S^{-1}M \to S^{-1}N$ is too.*

Proof. To say that $A \to B$ is injective is the same as saying that $0 \to A \to B$ is exact. From this the corollary is evident. ▲

Proof of the proposition. We adopt the notation of the proposition. If the composite $g \circ f$ is zero, clearly the localization $S^{-1}M \to S^{-1}N \to S^{-1}P$ is zero too. Call the maps $S^{-1}M \to S^{-1}N, S^{-1}N \to S^{-1}P$ as ϕ, ψ. We know that $\psi \circ \phi = 0$ so $\ker(\psi) \supset \mathrm{Im}(\phi)$. Conversely, suppose something belongs to $\ker(\psi)$. This can be written as a fraction

$$x/s \in \ker(\psi)$$

where $x \in N, s \in S$. This is mapped to

$$g(x)/s \in S^{-1}P,$$

[6] f will no longer denote an element of the ring.

which we're assuming is zero. This means that there is $t \in S$ with $tg(x) = 0 \in P$. This means that $g(tx) = 0$ as an element of P. But $tx \in N$ and its image of g vanishes, so tx must come from something in M. In particular,

$$tx = f(y) \text{ for some } y \in M.$$

In particular,

$$\frac{x}{s} = \frac{tx}{ts} = \frac{f(y)}{ts} = \phi(y/ts) \in \mathrm{Im}(\phi).$$

This proves that anything belonging to the kernel of ψ lies in $\mathrm{Im}(\phi)$. ▲

Lecture 7
9/15

Today we will discuss some basic constructions you can do with a module over a commutative ring.

§1 Hom and the tensor product

Let R be a commutative ring and M, N to be R-modules. We let $\mathrm{Hom}_R(M, N)$ for the set of all R-module homomorphisms $M \to N$.

Remark. $\mathrm{Hom}_R(M, N)$ is an R-module. You can add homomorphisms $f, g : M \to N$ by adding them pointwise

$$(f + g)(m) = f(m) + g(m)$$

and we can multiply homomorphisms by elements in R:

$$(af)(m) = a(f(m)), \forall a \in A.$$

In particular, if we have three R-modules M, N, P, we can think about homomorphisms

$$M \to^{\lambda} \mathrm{Hom}_R(N, P).$$

Suppose $x \in M, y \in N$. Then we can consider

$$\lambda(x) \in \mathrm{Hom}_R(N, P)$$

and thus

$$\lambda(x)(y) \in y.$$

We denote this by $\lambda(x, y)$; it is a function of two variables. There are certain properties:

1. $\lambda(x, y + y') = \lambda(x, y) + \lambda(x, y')$; because $\lambda(x)$ is an additive map.
2. $\lambda(x, ay) = a\lambda(x, y)$ because $\lambda(x)$ is an R-homomorphism.
3. We have $\lambda(x + x', y) = \lambda(x, y) + \lambda(x', y)$ because λ is additive.

4. We have $\lambda(ax, y) = a\lambda(x, y)$ because λ is an R-module homomorphism.

7.1 Definition. An **R-bilinear map** $\lambda : M \times N \to P$ is a map satisfying the above conditions. In particular, it has to be R-linear in each variable.

The previous discussion shows that there is a bijection between R-bilinear maps $M \times N \to P$ with R-module maps $M \to \mathrm{Hom}_R(N, P)$. This is nice because the first thing is symmetric in M, N; the second, by contrast, can be interpreted in terms of the old concepts of an R-module map. Both are useful.

Now the interpretation of bilinear maps as maps $M \to \mathrm{Hom}_R(N, P)$ was one thing; we changed the target from P to something else. What if we would make the source different.

7.2 Definition. An R-bilinear map $\lambda : M \times N \to P$ is called **universal** if for all R-modules Q, the composition of $P \to Q$ with $M \times N \to P$ gives a **bijection**

$$\mathrm{Hom}_R(P, Q) \simeq \{\text{bilinear maps } M \times N \to Q\}$$

So, given a bilinear map $M \times N \to Q$, there is a **unique** map $P \to Q$ making the diagram

$$\begin{tikzcd}
 & P \arrow[dd] \\
M \times N \arrow[ur] \arrow[dr] & \\
 & Q
\end{tikzcd}$$

General nonsense says the following:

> Given M, N, an universal R-bilinear map $M \times N \to P$ is **unique** up to isomorphism (if it exists). This is a general category theoretic observation.

Suppose $M \times N \to P$ was universal and $M \times N \to P'$ was also universal. Then there would be maps $P \to P'$ and $P' \to P$ making the diagram commutative:

$$\begin{tikzcd}
 & P \arrow[dd, leftrightarrow] \\
M \times N \arrow[ur] \arrow[dr] & \\
 & P'
\end{tikzcd}$$

These compositions $P \to P' \to P, P' \to P \to P'$ have to be the identity because of the definitions.

7.3 Proposition. *Given M, N, a universal bilinear map out of $M \times N$ exists.*

Before proving it we make:

7.4 Definition. We denote the codomain of the universal map out o f $M \times N$ by $M \otimes_R N$. This is called the **tensor product** of M, N.

Proof. Take the free R-module $M \otimes_R N$ generated by the symbols $\{x \otimes y\}_{x \in M, y \in N}$ and quotient out by the relations forced upon us by the definition of a bilinear map

1. $(x + x') \otimes y = x \otimes y + x' \otimes y$.
2. $(ax) \otimes y = a(x \otimes y) = x \otimes (ay)$.
3. $x \otimes (y + y') = x \otimes y + x \otimes y'$.

We will abuse notation and denote $x \otimes y$ for its image in $M \otimes_R N$ (as opposed to the symbol generating the free module).

There is a bilinear map $M \times N \to M \otimes_R N$ sending $(x, y) \to x \otimes y$; these relations mean that we have a bilinear map. We have to check that this is universal, but this is by definition.

Suppose we had a bilinear map $\lambda : M \times N \to P$. We must construct a linear map $M \otimes N \to P$. This sends $x \otimes y \to \lambda(x, y)$. This factors through the relations on $x \otimes y$ by bilinearity and leads to an R-linear map $M \otimes_R N \to P$ such that the diagram

$$\begin{tikzcd}
M \times N \arrow[r] \arrow[dr, "\lambda"] & M \otimes_R N . \arrow[d] \\
 & P
\end{tikzcd}$$

It is easy to see that $M \otimes_R N \to P$ is unique because the $x \otimes y$ generate it. ▲

The theory of the tensor product allows you to do away with bilinear maps and just think of linear maps.

We make some observations.

1. The tensor product is symmetric: $M \otimes_R N \simeq N \otimes_R M$ canonically. This is clear from the universal properties: giving a bilinear map from $M \times N$ is the same as a bilinear map from $N \times N$; it is also clear from the explicit construction.

2. $\forall M$, there is a canonical isomorphism $M \to M \otimes_R R$. Tensoring with R itself doesn't do anything. If we think in terms of bilinear maps, this statement is equivalent to the statement that a bilinear map $\lambda : M \times R \to P$ is the same as a linear map $M \to N$. Indeed, to do this, restrict λ to $\lambda(\cdot, 1)$. Given $f : M \to N$, similarly, we take for λ as $\lambda(x, a) = af(x)$. This gives a bijection as claimed.

3. The tensor product is associative. There are canonical isomorphisms $M \otimes_R (N \otimes_R P) \simeq (M \otimes_R N) \otimes_R P$. There are a few ways to see this: one is to build it explicitly from the construction given, sending $x \otimes (y \otimes z) \to (x \otimes y) \otimes z$.

   More conceptually, both have the same universal property: by general categorical nonsense (Yoneda's lemma), we need to show that for all Q, there is a canonical bijection
   $$\mathrm{Hom}_R(M \otimes (N \otimes P)), Q) \simeq \mathrm{Hom}_R((M \otimes N) \otimes P, Q)$$

where the R's are dropped for simplicity. But both of these sets can be identified with the set of trilinear maps[7] $M \times N \times P \to Q$. Indeed

$$\begin{aligned}\mathrm{Hom}_R(M \otimes (N \otimes P), Q) &\simeq \text{bilinear } M \times (N \otimes P) \to Q \\ &\simeq \mathrm{Hom}(N \otimes P, \mathrm{Hom}(M, Q)) \\ &\simeq \text{bilinear } N \times P \to \mathrm{Hom}(M, Q) \\ &\simeq \mathrm{Hom}(N, \mathrm{Hom}(P, \mathrm{Hom}(M, Q)) \\ &\simeq \text{trilinear maps.}\end{aligned}$$

§2 Exactness

We know discuss the exactness properties of this. Recall:

> A sequence $M \xrightarrow{f} N \xrightarrow{g} P$ is exact if $\ker g = \mathrm{Im} f$.

7.5 Definition. A sequence $M_0 \xrightarrow{f_1} M_1 \xrightarrow{f_2} \cdots \xrightarrow{f_n} M_n$ is **exact** if each consecutive three-term sequence is exact.

You typically see this definition applied to sequences of the form

$$0 \to M' \xrightarrow{f} M \xrightarrow{g} M'' \to 0,$$

which is called a **short exact sequence** (if it is exact). Exactness here means that f is injective, g is surjective, and f maps onto the image of g. So M'' can be thought of as the quotient M/M'.

Suppose you have a functor F from the category of R-modules to the category of R-modules. Then:

7.6 Definition.

1. F is called **additive** if F preserves direct sums.
2. F is called **exact** if F is additive and preserves exact sequences.
3. F is called **left exact** if F is additive and preserves exact sequences of the form $0 \to M' \to M \to M''$. In particular, F preserves kernels.
4. F is **right exact** if F is additive and F preserves exact sequences of the form $M' \to M \to M'' \to 0$, i.e. F preserves cokernels.

A functor is exact if and only if it is both left and right exact.

7.7 Example. If $S \subset R$ is multiplicatively closed, then localization $M \to S^{-1}M$ is an exact functor.

7.8 Example. If M is an R-module, then the construction

$$N \to \mathrm{Hom}_R(M, N)$$

[7] Easy to define.

is left exact (but *not exact*). This means that if

$$0 \to N' \to N \to N''$$

is exact, then

$$0 \to \mathrm{Hom}_R(M, N') \to \mathrm{Hom}_R(M, N) \to \mathrm{Hom}_R(M, N'')$$

is exact as well. Why is this? Well, first we have to show that the map $\mathrm{Hom}_R(M, N') \to \mathrm{Hom}_R(M, N)$ is injective; this is because $N' \to N$ is injective, and composition with $N' \to N$ can't kill any nonzero $M \to N'$. Similarly, exactness in the middle can be checked easily. We leave it to the reader.

This functor $\mathrm{Hom}_R(M, \cdot)$ is not exact in general. Indeed:

7.9 Example. Suppose $R = \mathbb{Z}$, $M = \mathbb{Z}/2\mathbb{Z}$. There is a short exact sequence

$$0 \to 2\mathbb{Z} \to \mathbb{Z} \to \mathbb{Z}/2\mathbb{Z} \to 0.$$

Let us apply $\mathrm{Hom}_R(M, \cdot)$. We get

$$0 \to \mathrm{Hom}(\mathbb{Z}/2\mathbb{Z}, 2\mathbb{Z}) \to \mathrm{Hom}(\mathbb{Z}/2\mathbb{Z}, \mathbb{Z}) \to \mathrm{Hom}(\mathbb{Z}/2\mathbb{Z}, \mathbb{Z}/2\mathbb{Z}) \to 0.$$

The last term is $\mathbb{Z}/2\mathbb{Z}$; everything else is zero. This is not exact at the last point.

§3 Projective modules

Sometimes, however, we do have exactness.

7.10 Definition. An R-module M is called **projective** if $\mathrm{Hom}_R(M, \cdot)$ is exact.

7.11 Proposition. *The following are equivalent for an R-module M:*

1. *M is projective.*
2. *Given any map $M \to N/N'$ from M into a quotient N/N', we can lift it to a map $M \to N$.*
3. *There is a module M' such that $M \oplus M'$ is free.*

Proof. The equivalence of 1 and 2 is just unwinding the definition of projectivity, because we just need to show that $\mathrm{Hom}_R(M, \cdot)$ preserves surjective maps, i.e. quotients. ($\mathrm{Hom}_R(M, \cdot)$ is already left-exact, after all.) To say that $\mathrm{Hom}_R(M, N) \to \mathrm{Hom}_R(M, N/N')$ is just the statement that maps can be lifted.

Let us first show that 2 implies 3. Suppose M satisfies 2. Then choose a surjection $P \to M$ where P is free. (E.g. P the free module generated by all the elements of M.) Then we can write $M \simeq P/P'$ for $P' \subset P$. The isomorphism map $M \to P/P'$ leads to a lifting $M \to P$. In particular, there is a section of $P \to M$, namely this lifting. Then $P \simeq \ker(P \to M) \oplus \mathrm{Im}(M \to P) \simeq \ker(P \to M) \oplus M$, verifying 3 since P is free.

Now let us show that 3 implies 2. Suppose $M \oplus M'$ is free, isomorphic to P. Then a map $M \to N/N'$ can be extended to

$$P \to N/N'$$

by declaring it to be trivial on M'. But now $P \to N/N'$ can be lifted to N because P is free; we just lift the image of a basis, and this defines $P \to N$. Compose this with the inclusion $M \to P$, and get $M \to P \to N$ which is the lifting of $M \to N/N'$. ▲

Lecture 8
9/17

§1 Right-exactness of the tensor product

We will start by talking about the exactness properties of the tensor product. First, let's recall what we did last time. If M, N are R-modules over the commutative ring R, we defined another R-module $\mathrm{Hom}_R(M, N)$ of morphisms $M \to N$. This is left-exact as a functor of N. In other words, if we fix M and let N vary, then the construction of homming out of M preserves kernels.

In the language of category theory, this construction $N \to \mathrm{Hom}_R(M, N)$ has an adjoint. The other construction we discussed last time was the tensor product. Namely, given M, N we defined a **tensor product** $M \otimes_R N$ such that giving a map $M \otimes_R N \to P$ is the same as giving a bilinear map $\lambda : M \times N \to P$, which in turn is the same as giving an R-linear map

$$M \to \mathrm{Hom}_R(N, R).$$

So we have a functorial isomorphism

$$\mathrm{Hom}_R(M \otimes_R N, P) \simeq \mathrm{Hom}_R(M, \mathrm{Hom}_R(N, P)).$$

The category-theoretic language is that tensoring is the left-adjoint to the hom functor. By abstract nonsense, it follows that since $\mathrm{Hom}(M, \cdot)$ preserves cokernels, the left-adjoint preserves cokernels and is right-exact. We shall see this directly.

8.1 Proposition. *The functor $N \to M \otimes_R N$ is right-exact, i.e. preserves cokernels.*

In fact, the tensor product is symmetric, so it's right exact in either variable.

Proof. We have to show that if $N' \to N \to N'' \to 0$ is exact, then so is

$$M \otimes_R N' \to M \otimes_R N \to M \otimes_R N'' \to 0.$$

There are a lot of different ways to think about this. For instance, we can look at the direct construction. The tensor product is a certain quotient of a free module.

$M \otimes_R N''$ is the quotient of the free module generated by $m \otimes n'', m \in M, n \in N''$ modulo the usual relations. The map $M \otimes N \to M \otimes N''$ sends $m \otimes n \to m \otimes n''$ if n'' is the image of n in N''. Since each n'' can be lifted to some n, it is obvious that the map $M \otimes_R N \to M \otimes_R N''$ is surjective.

Now we know that $M \otimes_R N''$ is a quotient of $M \otimes_R N$. But which relations do you have to impose on $M \otimes_R N$ to get $M \otimes_R N''$? In fact, each relation in $M \otimes_R N''$ can be lifted to a relation in $M \otimes_R N$, but with some redundancy. So the only thing to quotient out by is the statement that $x \otimes y, x \otimes y'$ have the same image in $M \otimes N''$. In particular, we have to quotient out by

$$x \otimes y - x \otimes y' \ , y - y' \in N'$$

so that if we kill off $x \otimes n'$ for $n' \in N' \subset N$, then we get $M \otimes N''$. This is a direct proof.

You can also give a conceptual proof. We'd like to know that $M \otimes N''$ is the cokernel of $M \otimes N' \to M \otimes N''$. In other words, we'd like to know that if we mapped $M \otimes_R N$ into some P and the pull-back to $M \otimes_R N'$, it'd factor uniquely through $M \otimes_R N''$. Namely, we need to show that

$$\mathrm{Hom}_R(M \otimes N'', P) = \ker(\mathrm{Hom}_R(M \otimes N, P) \to \mathrm{Hom}_R(M \otimes N'', P)).$$

But the first is just $\mathrm{Hom}_R(N'', \mathrm{Hom}_R(M, P))$ by the adjointness property. Similarly, the second is just

$$\ker(\mathrm{Hom}_R(N, \mathrm{Hom}(M, P)) \to \mathrm{Hom}_R(N', \mathrm{Hom}_R(M, P))$$

but this last statement is $\mathrm{Hom}_R(N'', \mathrm{Hom}_R(M, P))$ by just the statement that $N'' = \mathrm{coker}(N' \to N)$. To give a map N'' into some module (e.g. $\mathrm{Hom}_R(M, P)$) is the same thing as giving a map out of N which kills N'. So we get the functorial isomorphism. ▲

Remark. Formation of tensor products is, in general, **not** exact.

8.2 Example. Let $R = \mathbb{Z}$. Let $M = \mathbb{Z}/2\mathbb{Z}$. Consider the exact sequence

$$0 \to \mathbb{Z} \to \mathbb{Q} \to \mathbb{Q}/\mathbb{Z} \to 0$$

which we can tensor with M, yielding

$$0 \to \mathbb{Z}/2\mathbb{Z} \to \mathbb{Q} \otimes \mathbb{Z}/2\mathbb{Z} \to \mathbb{Q}/\mathbb{Z} \otimes \mathbb{Z}/2\mathbb{Z} \to 0$$

I claim that the second thing $\mathbb{Q} \otimes \mathbb{Z}/2\mathbb{Z}$ is zero. This is because by tensoring with $\mathbb{Z}/2\mathbb{Z}$, we've made multiplication by 2 identically zero. By tensoring with $\mathbb{Q}$, we've made multiplication by 2 invertible. The only way to reconcile this is to have the second term zero. In particular, the sequence becomes

$$0 \to \mathbb{Z}/2\mathbb{Z} \to 0 \to 0 \to 0$$

which is not exact.

§2 Flatness

It is exact in some cases, though.

8.3 Definition. Let R be a commutative ring. An R-module M is called **flat** if the functor $N \to M \otimes_R N$ is exact. We already know that it's right exact, so the only thing to be checked is that tensoring by M preserves injections.

8.4 Example. $\mathbb{Z}/2\mathbb{Z}$ is not flat as a $\mathbb{Z}$-module by the above example.

If R is a ring, then R is flat as an R-module, because tensoring by R is the identity functor.

8.5 Example. If P is a projective module (i.e., homming out of P is exact), then P is flat.

Proof. If $P = \bigoplus_A R$ is free, then tensoring with P corresponds to taking the direct sum A times, i.e.

$$P \otimes_R M = \bigoplus_A M.$$

This is because tensoring with R preserves (finite or direct) infinite sums. You can observe this directly from the construction, or using the universal property. This statement, together with right-exactness, implies that:

Remark. Tensoring with M commutes with all colimits in the category of R-modules.

Anyway, back to the proof. The functor $M \to \bigoplus_A M$ is exact, so free modules are flat.

A projective module, as discussed earlier, is a direct summand of a free module. So if P is projective, $P \oplus P' \simeq \bigoplus_A R$ for some P'. Then we have that

$$(P \otimes_R M) \oplus (P' \otimes_R M) \simeq \bigoplus_A M.$$

If we had an injection $M \to M'$, then there is a direct sum decomposition yields a sequence of maps

$$P \otimes_R M' \to P \otimes_R M \to P \otimes_R M \oplus P \otimes_R M' \to \bigoplus_A M$$

and the composition map is injective since its sum with $P' \otimes M' \to P' \otimes M'$ is injective. FIX ▲

We now interpret localization as a tensor product.

8.6 Theorem. *Let R be a commutative ring, $S \subset R$ a multiplicative subset. Then there exists a canonical isomorphism*

$$\phi : S^{-1}M \simeq S^{-1}R \otimes_R M.$$

In particular, $S^{-1}R$ is a flat R-module, because localization is an exact functor.

Proof. Here is a construction of ϕ. If $x/s \in S^{-1}M$ where $x \in M, s \in S$, we define

$$\phi(x/s) = (1/s) \otimes m.$$

Let us check that this is well-defined. Suppose $x/s = x'/s'$; then this means there is $t \in S$ with

$$xs't = x'st.$$

From this we need to check that $\phi(x/s) = \phi(x'/s')$, i.e. that $1/s \otimes x$ and $1/s' \otimes x'$ represent the same elements in the tensor product. But we know from the last statement that

$$\frac{1}{ss't} \otimes xs't = \frac{1}{ss't} x'st \in S^{-1}R \otimes M$$

and the first is just

$$s't(\frac{1}{ss't} \otimes x) = \frac{1}{s} \otimes x$$

by linearity, while the second is just

$$\frac{1}{s'} \otimes x'$$

similarly. One next checks that ϕ is an R-module homomorphism, which we leave to the reader.

Finally, we need to describe the inverse. The inverse $\psi : S^{-1}R \otimes M \to S^{-1}M$ is easy to construct because it's a map out of the tensor product, and we just need to give a bilinear map

$$S^{-1}R \times M \to S^{-1}M,$$

and this sends $(r/s, m)$ to mr/s.

It is easy to see that ϕ, ψ are inverses to each other by the definitions. ▲

Let us make a few other comments.

Remark. Let $\phi : R \to R'$ be a homomorphism of rings. Then, first of all, any R'-module can be regarded as an R-module by composition with ϕ. In particular, R' is an R-module.

If M is an R-module, we can define

$$M \otimes_R R'$$

as an R-module. But in fact this tensor product is an R'-module; it has an action of R'. If $x \in M$ and $a \in R'$ and $b \in R'$, multiplication of $(x \otimes a) \in M \otimes_R R'$ by $b \in R'$ sends this, *by definition*, to

$$b(x \otimes a) = x \otimes ab.$$

It is easy to check that this defines an action of R' on $M \otimes_R R'$. (One has to check that this action factors through the appropriate relations, etc.)

Lecture 9
[Section] 9/19

§1 Discrete valuation rings

We will talk about discrete valuation rings today.

First, we review the idea of localization. Let R be a commutative ring and S a multiplicative subset. Then there is a correspondence between prime ideals in $S^{-1}R$ and prime ideals of R not intersecting S.

Recall also that a domain R is a **Dedekind domain** if:

1. R is noetherian.

2. Every prime ideal of R is maximal.

3. R is integrally closed.

Fix a Dedekind domain R. Take a nonzero prime ideal $\mathfrak{p} \subset R$, and look at the localization $R_{\mathfrak{p}}$. The prime ideals of this local ring are just $\mathfrak{p}$ and 0, because every nonzero prime ideal is maximal. In particular,

$$\mathrm{Spec} R_{\mathfrak{p}} = \{(0), \mathfrak{p}R_{\mathfrak{p}}\}\,.$$

The closed subsets are just $\{\mathfrak{p}R_{\mathfrak{p}}\}$ and the whole space. So $\mathfrak{p}R_{\mathfrak{p}}$ is called a **closed point** while (0) is called a **generic point** because its closure is the whole space.

Consider an ideal of $R_{\mathfrak{p}}$. This can be written as the form $IR_{\mathfrak{p}}$ for I an ideal in R. But R is a Dedekind domain. So we have that

$$I = \prod \mathfrak{p}_i$$

for some (not necessarily distinct) prime ideals $\mathfrak{p}_i$ of R, by unique factorization of ideals. Thus we get a factorization of $IR_{\mathfrak{p}}$ as

$$IR_{\mathfrak{p}} = \prod \mathfrak{p}_i R_{\mathfrak{p}}$$

which is just a power of

$$\mathfrak{p}R_{\mathfrak{p}},$$

though, since $\mathfrak{p}_i R_{\mathfrak{p}} = R_{\mathfrak{p}}$ if $\mathfrak{p}_i \neq \mathfrak{p}$. Suppose $IR_{\mathfrak{p}} = (\mathfrak{p}R_{\mathfrak{p}})^n$.

9.1 Definition. Then n is called the **$\mathfrak{p}$-adic valuation** of I and is denoted $v_{\mathfrak{p}}(I)$. The $\mathfrak{p}$-adic valuation of $x \in R - \{0\}$ is defined to be the valuation of (x) and is denoted $v_{\mathfrak{p}}(x)$.

Here are some properties of $v_{\mathfrak{p}}$:

1. $v_{\mathfrak{p}}(xy) = v_{\mathfrak{p}}(x) + v_{\mathfrak{p}}(y)$.
2. $v_{\mathfrak{p}}(x + y) \geq \min(v_{\mathfrak{p}}(x), v_{\mathfrak{p}}(y))$.

It is clear that $v_{\mathfrak{p}}(x) = 0$ if and only if x is a unit in $R_{\mathfrak{p}}$. Also, if $v_{\mathfrak{p}}(x) = 1$, then

$$(x)R_{\mathfrak{p}} = \mathfrak{p}R_{\mathfrak{p}}$$

implying that x generates $\mathfrak{p}R_{\mathfrak{p}}$.

It is not obvious that there exists such an x with valuation one, though. However:

9.2 Proposition. *$R_{\mathfrak{p}}$ is a PID.*

Proof. We know that $\mathfrak{p} \neq \mathfrak{p}^2$ in R because otherwise we could multiply by an inverse to get $(1) \in \mathfrak{p}$. Take $a \in \mathfrak{p} - \mathfrak{p}^2$. Then it is clear that

$$(a)R_{\mathfrak{p}} \subset \mathfrak{p}R_{\mathfrak{p}}$$

but

$$(a)R_{\mathfrak{p}} \not\subset (\mathfrak{p}^2)R_{\mathfrak{p}}$$

so that a has valuation one. ▲

We now make:

9.3 Definition. A ring R is a **discrete valuation ring (DVR)** if it is a PID and has a unique nonzero prime ideal $\mathfrak{m}$. Any element generating $\mathfrak{m}$ is called a **uniformizer**.

If $\mathfrak{p} \subset R$ is a nonzero prime ideal of a Dedekind domain R, then we have shown that $R_{\mathfrak{p}}$ is a DVR.

If R is a DVR, then R is a Dedekind domain, so we can define the $\mathfrak{m}$-adic valuation on R, because every nonzero ideal of R is a product of copies of $\mathfrak{m}$.

Alternatively one defines $v_{\mathfrak{m}}(x)$ as the largest n such that $x \in \mathfrak{m}^n$. One has to check then that

$$\bigcap \mathfrak{m}^n = (0)$$

which can be done. Thus we get our valuation, in either case.

The valuation extends to the field of fractions K, so we get a map

$$K^* \to \mathbb{Z}$$

by defining $v_{\mathfrak{m}}(x/y) = v_{\mathfrak{m}}(x) - v_{\mathfrak{m}}(y)$. It is easy to see that this is well-defined.

Remark. R is precisely the set of elements of K with nonnegative valuation. R^* (the units of R) are precisely the elements with zero valuation. $\mathfrak{m}$ consists of elements with positive valuation.

9.4 Definition. The quotient $R/\mathfrak{m}$ is called the **residue field**.

One can also define a discrete valuation ring by starting with a field with such a valuation $v : K^* \to \mathbb{Z}$. One defines the ring by taking the set of elements with nonnegative valuation.

9.5 Definition. The pair (K, v) for K a field is a **discrete valuation field** if $v : K^* \to \mathbb{Z}$ is a surjective homomorphism satisfying the **ultrametric property**

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

9.6 Exercise. If (K, v) is a discrete valuation field, then the set $R = \{x \in K : v(x) \geq 0\}$ is a discrete valuation ring whose quotient field is K.

9.7 Example. Let $K = \mathbb{C}((t))$ of formal series

$$\sum_{n \geq n_0} a_n t^n, \quad \forall a_n \in \mathbb{C}.$$

This is the field of fractions of the power series ring $\mathbb{C}[[t]]$. Indeed, this is easily seen because the units of the power series ring are precisely the formal power series $\sum_{n \geq 0} a_n t^n$ with $a_0 \neq 0$.

We can define the **t-adic valuation** of $\sum_{n \geq n_0} a_n t^n \in \mathbb{C}[[t]]$ to be n_0 if $a_{n_0} \neq 0$. So the t-adic valuation is the order at zero.

9.8 Theorem. *Suppose R is a noetherian domain such that all the localizations at non-zero primes are DVRs. Then R is a Dedekind domain.*

Interestingly, this result is **false** without noetherian hypothesis.

Proof. We've shown that a Dedekind domain has localizations which are DVRs above. Suppose R is a domain whose localizations $R_{\mathfrak{m}}$ at *maximal* $\mathfrak{m}$ are DVRs; then we show that R is Dedekind.

First, we have assumed that R is noetherian.

It is clear that R has dimension one if all its localizations at maximal ideals have dimension 1.

R is integrally closed because it is the intersection in its quotient field of the integrally closed domains $\bigcap R_{\mathfrak{m}}$. Cf. the lemma below. ▲

9.9 Lemma. *For R any integral domain, we have*

$$R = \bigcap_{\mathfrak{m} \text{ maximal}} R_{\mathfrak{m}}.$$

The intersection is taken inside the field of fractions.

Proof. Exercise to the reader. ▲

There is, incidentally, a harder result:

9.10 Theorem. *R is an integral domain which is integrally closed, then*

$$R = \bigcap_{\mathfrak{p} \text{ height } 1} R_{\mathfrak{p}}.$$

Proof. Omitted. ▲

Let now R be a Dedekind domain. For each localization $R_{\mathfrak{p}}$, we have a valuation $v_{\mathfrak{p}}$ on R. What interaction do these have with each other? Answer: they're basically independent. Let's see what this means.

If I is an ideal of R, we can write $I = \prod \mathfrak{p}_i^{n_i}$ uniquely for each $\mathfrak{p}_i$ prime. We have defined $v_{\mathfrak{p}_i}(I) = n_i$. We also defined $v_{\mathfrak{p}_i}(x)$ by looking at the ideal (x) it generates.

Let us prove the **weak approximation theorem**, which is a generalization of the Chinese remainder theorem.

9.11 Theorem (Weak approximation theorem)**.** *Let R be a Dedekind domain, $\mathfrak{p}_1, \dots, \mathfrak{p}_k$ nonzero prime ideals. Suppose $x_1, \dots, x_k \in K$ and $n_1, \dots, n_k \in \mathbb{Z}$.*

Then there is $x \in K$ such that

$$v_{\mathfrak{p}_i}(x - x_i) \geq n_i$$

and, moreover,

$$v_{\mathfrak{q}}(x) \geq 0$$

for any $\mathfrak{q}$ not among the $\mathfrak{p}_i$.

Proof. First, we assume that each $x_i \in R$ and each $n_i \geq 0$, by multiplying by highly divisible elements. We will in fact take $x \in R$. The two lines below will translate into

$$x - x_i \in \mathfrak{p}_i^{n_i}$$

and

$$x \in R.$$

Now it is just the Chinese remainder theorem, but we sketch a proof anyway.

Consider the ideal

$$\mathfrak{a} = \mathfrak{p}_1^{n_1} + \mathfrak{p}_2^{n_2}\mathfrak{p}_3^{n_3} + \dots \mathfrak{p}_k^{n_k}.$$

Any valuation of this is zero. So this $\mathfrak{a}$ is just (1). We write

$$x_1 = y_1 + z_1,$$

for

$$y_1 \in \mathfrak{p}_1^{n_1}, \quad z_1 \in \mathfrak{p}_2^{n_2} \dots \mathfrak{p}_k^{n_k}.$$

Thus z_1 is very close to 0 at each $\mathfrak{p}_i^{n_i}$ for $i > 1$ and close to x_1 at $\mathfrak{p}$. We can do this for each index. Taking the sum of correspondingly z_i does what we want. ▲

There is a "strong approximation theorem" for number fields where one works with "primes at ∞," i.e. archimedean absolute values; one then has to use adeles or something like that.

A corollary is that:

9.12 Corollary. *Hypotheses as above, we can choose x such that*

$$v_{\mathfrak{p}_i}(x - x_i) = n_i$$

for each i.

So we don't have to settle for inequality.

Proof. Take some $\xi_i \in \mathfrak{p}_i^{n_i} - \mathfrak{p}_i^{n_i+1}$ for each i. We look for x such that

$$x - x_i \equiv \xi_i \text{ mod} \mathfrak{p}_i^{n_i+1}$$

which will do what we want. But we can just invoke the previous theorem for this. ▲

Why is this good? Here is an appplication:

9.13 Theorem. *A Dedekind domain with* Spec*R finite is principal.*

Proof. It is sufficient to show that any prime $\mathfrak{p}$ is principal since R is Dedekind. We apply the weak approximation theorem (more precisely, its corollary) to find an element which is a uniformizer at $\mathfrak{p}$ and units at other primes. Then this element is a generator for $\mathfrak{p}$ because, for any $x \in R$, we have

$$x = \prod_{\mathfrak{q}} \mathfrak{q}^{v_{\mathfrak{q}}(x)}.$$

▲

The converse is obviously false (e.g. $R = \mathbb{Z}$).

Lecture 10
9/20

§1 The adjoint property

Today, we will finish talking about tensor products. Suppose we have a ring-homomorphism $\phi : R \to R'$. In this case, any R'-module can be regarded as an R-module. Let M' be an R'-module and M an R-module; we can talk about

$$\mathrm{Hom}_R(M, M')$$

by thinking of M' as an R-module.

10.1 Proposition. *There is a canonical morphism between*

$$\mathrm{Hom}_R(M, M') \simeq \mathrm{Hom}_{R'}(M \otimes_R R', M').$$

Last time, we mentioned at the very end that if M has an R-module structure, then $M \otimes_R R'$ has an R' module structure where R' acts on the right.

This proposition has a formulation in terms of category theory. If F is the forgetful functor mapping R'-modules to R-modules, namely the procedure of using the morphism $R \to R'$, then this functor has a left-adjoint

$$M \to M \otimes_R R'.$$

Proof. We can describe the bijection explicitly. Given an R'-homomorphism $f : M \otimes_R R' \to M'$, we get a map f_0

$$M \to M'$$

sending

$$m \to m \otimes 1 \to f(m \otimes 1).$$

This is easily seen to be an R-module-homomorphism. Indeed,

$$f_0(ax) = f(ax \otimes 1) = f(\phi(a)(x \otimes 1)) = af(x \otimes 1) = af_0(x)$$

since f is an R'-module homomorphism.

Conversely, if we are given a homomorphism of R-modules

$$f_0 : M \to M'$$

then we can define

$$f : M \otimes_R R' \to M'$$

by sending $m \otimes r' \to r' f_0(m)$, which is a homomorphism of R' modules. This is well-defined because f_0 is a homomorphism of R-modules. We leave some details to the reader. ▲

§2 Tensor products of algebras

There is one other basic property of tensor products to discuss before moving on: namely, what happens when one tensors a ring with another ring. Let R be a commutative ring and suppose we have ring homomorphisms

$$\phi_0 : R \to R_0, \quad \phi_1 : R \to R_1.$$

10.2 Proposition. *Then $R_0 \otimes_R R_1$ has the structure of a commutative ring.*

Proof. Indeed, this multiplication multiplies two typical elements $x \otimes y, x' \otimes y'$ by sending them to $xx' \otimes yy'$. The ring structure is determined by this formula. One ought to check that this approach respects the relations of the tensor product. We will do so in an indirect way.

One can also think of this as follows. Multiplication is the same thing as giving an R-bilinear map

$$(R_0 \otimes_R R_1) \times (R_0 \otimes R_1) \to R_0 \otimes_R R_1,$$

i.e. an R-linear map

$$(R_0 \otimes_R R_1) \otimes_R (R_0 \otimes R_1) \to R_0 \otimes_R R_1.$$

But the left side is isomorphic to $(R_0 \otimes_R R_0) \otimes_R (R_1 \otimes_R R_1)$. Since we have bilinear maps $R_0 \times R_0 \to R_0$ and $R_1 \times R_1 \to R_1$, we get linear maps $R_0 \otimes_R R_0 \to R_0$ and $R_1 \otimes_R R_1 \to R_1$. Tensoring these maps gives the multiplication as a bilinear map. It is easy to see that these two approaches are the same.

We now need to check that this operation is commutative and associative, with $1 \otimes 1$ as a unit; moreover, it distributes over addition. Distributivity over addition is built into the construction (i.e. in view of bilinearity). The rest (commutativity, associativity, units) can be checked directly on the generators, since we have distributivity. ▲

We can in fact describe the tensor product of R-algebras by a universal property. We will describe a commutative diagram:

$$\begin{tikzcd}
 & R \arrow[dl] \arrow[dr] & \\
R_0 \arrow[dr] & & R_1 \arrow[dl] \\
 & R_0 \otimes_R R_1 &
\end{tikzcd}$$

Here $R_0 \to R_0 \otimes_R R_1$ sends $x \to x \otimes 1$; similarly for $R_1 \to R_0 \otimes_R R_1$. These are ring-homomorphisms, and it is easy to see that the above diagram commutes, since $r \otimes 1 = 1 \otimes r = r(1 \otimes 1)$ for $r \in R$.

In fact,

10.3 Proposition. *$R_0 \otimes_R R_1$ is universal with respect to this property: in the language of category theory, the above diagram is a pushout square.*

This means for any commutative ring B, and every pair of maps $u_0 : R_0 \to B$ and $u_1 : R_1 \to B$ such that the pull-backs $R \to R_0 \to B$ and $R \to R_1 \to B$ are the same, then we get a unique map of rings

$$R_0 \otimes_R R_1 \to B$$

which restricts on R_0, R_1 to the morphisms u_0, u_1 that we started with.

Proof. We make B into an R-module by the map $R \to R_0 \to B$ (or $R \to R_1 \to B$, it is the same by assumption). This map $R_0 \otimes_R R_1 \to B$ sends

$$x \otimes y \to u_0(x)u_1(y).$$

It is easy to check that $(x, y) \to u_0(x)u_1(y)$ is R-bilinear (because of the condition that the two pull-backs of u_0, u_1 to R are the same), and that it gives a homomorphism of rings $R_0 \otimes_R R_1 \to B$ which restricts to u_0, u_1 on R_0, R_1. One can check, for instance, that this is a homomorphism of rings by looking at the generators.

It is also clear that $R_0 \otimes_R R_1 \to B$ is unique, because we know that the map on elements of the form $x \otimes 1$ and $1 \otimes y$ is determined by u_0, u_1; these generate $R_0 \otimes_R R_1$, though. ▲

§3 Integrality

We now move to something less formal.

Let us return to the ring $\mathbb{Z}[\sqrt{-5}]$; this is the canonical example of a ring where unique factorization fails. This is because, as we remember,

$$6 = 2 \times 3 = (1 + \sqrt{-5})(1 - \sqrt{-5}).$$

Five is a big number; why did we have to go all the way to five to get this to happen? What about $\mathbb{Z}[\sqrt{-3}]$?

Here we have

$$(1 - \sqrt{-3})(1 + \sqrt{-3}) = 4 = 2 \times 2.$$

These elements can be factored no more, and $1 - \sqrt{-3}$ and 2 are not associates (they differ by something which isn't a unit). So in this ring, we have a failure of unique factorization. For some reason, this doesn't bother people as much.

The reason this doesn't bother people is that $\mathbb{Z}[\sqrt{-3}]$ is contained in the larger ring

$$\mathbb{Z}[\frac{1 + \sqrt{-3}}{2}],$$

which does have unique factorization.

In fact, $\mathbb{Z}[\sqrt{-3}]$ is an index two subgroup of the larger ring. The reason is that the larger ring $\mathbb{Z}[\frac{1+\sqrt{-3}}{2}]$ can be described by the set of elements $a + b\sqrt{-3}$ where a, b are either both integers or both integers plus $\frac{1}{2}$, as is easily seen: this set is closed under addition and multiplication. Note that, by contrast, $\mathbb{Z}[\frac{1+\sqrt{-5}}{2}]$ does not contain $\mathbb{Z}[\sqrt{-5}]$ as a finite index subgroup—it can't be slightly enlarged in the same sense. When you enlarge $\mathbb{Z}[\sqrt{-5}]$, you have to add a lot of stuff.

10.4 Definition. Let $R \subset R'$ be an inclusion of integral domains. An element $x \in R'$ is said to be **integral** over R if x satisfies a monic polynomial equation in $R[X]$, say

$$x^n + r_1 x^{n-1} + \cdots + r_n = 0.$$

10.5 Example. $\frac{1+\sqrt{-3}}{2}$ is integral over $\mathbb{Z}$; it is in fact a sixth root of unity.

10.6 Example. $\frac{1+\sqrt{5}}{2}$ is not integral over $\mathbb{Z}$. To explain this, we need to work a bit more.

We pause for a useful definition.

10.7 Definition. An R-module M is **finitely generated** if there exists a surjection $R^n \to M$ for some n. In other words, it has a finite number of elements whose "span" contains M.

Suppose $R \subset R'$ are domains. Let $x \in R'$.

10.8 Proposition. *$x \in R'$ is integral over R if and only if the subalgebra $R[x]$ (generated by R, x) is a finitely generated R-module.*

This for instance lets us show that $\frac{1+\sqrt{-5}}{2}$ is not integral over $\mathbb{Z}$, because when you keep taking powers, you get arbitrarily large denominators: the arbitrarily large denominators imply that it cannot be integral.

Proof. If $x \in R'$ is integral, then x satisfies

$$x^n + r_1 x^{n-1} + \cdots + r_n = 0.$$

Then $R[x]$ is generated as an R-module by $1, x, \dots, x^{n-1}$. This is because the submodule generated by $1, x, \dots, x^{n-1}$ is closed under multiplication by R and by multiplication by x (by the above equation).

Now suppose x generates a subalgebra $R[x] \subset R'$ which is a finitely generated R-module. Then the increasing sequence of R-modules generated by $\{1\}, \{1, x\}, \{1, x, x^2\}, \dots$ must stabilize, since the union is $R[x]$. It follows that some x^n can be expressed as a linear combination of smaller powers of x. ▲

Lecture 11
9/22

§1 Integrality, continued

Last time we talked about integral extensions. If $R \subset R'$, we say that an element $x \in R'$ is **integral** over R if either of the following equivalent conditions are satisfied:

1. There is a monic polynomial in $R[X]$ which vanishes on x.

2. $R[x] \subset R'$ is a finitely generated R-module.

Last time we supposed that R, R' were domains, but this is not really necessary.

The first thing to do is to add a third equivalent condition.

11.1 Proposition. *$x \in R'$ is integral if and only if there exists a finitely generated R-submodule $M \subset R'$ such that $R \subset M$ and $xM \subset M$.*

Proof. It's obvious that the second condition above (equivalent to integrality) implies the condition of this proposition. Indeed, you could just take $M = R[x]$.

Now let us prove that if there exists such an M which is finitely generated, then x is integral. Just because M is finitely generated, the submodule $R[x]$ is not obviously finitely generated. In particular, this implication requires a bit of proof.

We shall prove that the condition of this proposition implies integrality. Suppose $y_1, \dots, y_k \in M$ generate M as R-module. Then multiplication by x gives an R-module map $M \to M$. In particular, we can write

$$xy_i = \sum a_{ij} y_j$$

where each $a_{ij} \in R$. These $\{a_{ij}\}$ may not be unique, but let us make some choices; we get a k-by-k matrix $A \in M_k(R)$. The claim is that x satisfies the characteristic polynomial of A.

Consider the matrix

$$(x1 - A) \in M_n(R').$$

Note that $(x1-A)$ annihilates each y_i, by the choice of A. We can consider the adjoint $B = (x1 - A)^{adj}$. Then

$$B(x1 - A) = \det(x1 - A)1.$$

This product of matrices obviously annihilates each vector y_i. It follows that

$$(\det(x1 - A)y_i = 0, \quad \forall i,$$

which implies that $\det(x1-A)$ kills M. This implies that $\det(x1-A) = 0$ since $R \subset M$.

As a result, x satisfies the chaacteristic polynomial. ▲

We proved this to show that the set of integral elements is well behaved.

11.2 Theorem. *Let $R \subset R'$. Let $S = \{x \in R' : x \text{ is integral over } R\}$. Then S is a subring of R'. In particular, it is closed under addition and multiplication.*

Proof. Suppose $x, y \in S$. We can consider the finitely generated modules $R[x], R[y] \subset R'$ generated (as algebras) by x over R. By assumption, these are finitely generated R-modules. In particular, the tensor product

$$R[x] \otimes_R R[y]$$

is a finitely generated R-module. Indeed:

11.3 Lemma. *If M, N are finitely generated, then $M \otimes_R N$ is finitely generated.*

Proof. Indeed, if we have surjections $R^m \to M, R^n \to N$, we can tensor them; we get a surjection since the tensor product is right-exact. So have a surjection $R^{mn} = R^m \otimes_R R^n \to M \otimes_R N$. ▲

Back to the main proof. As stated, $R[x] \otimes_R R[y]$ is finitely generated as an R-module. We have a ring-homomorphism $R[x] \otimes_R R[y] \to R'$ which comes from the inclusions $R[x], R[y] \rightarrowtail R'$.

Let M be the image of $R[x] \otimes_R R[y]$ in R'. Then M is an R-submodule of R', indeed an R-subalgebra containing x, y. Also, M is finitely generated. Since $x + y, xy \in M$ and M is a subalgebra, it follows that

$$(x+y)M \subset M, \quad xyM \subset M.$$

Thus $x + y, xy$ are integral over R. ▲

§2 Integral closure

11.4 Definition. If $R \subset R'$, then the set $S = \{x \in R' : x \text{ is integral}\}$ is called the **integral closure** of R in R'. We say that R is **integrally closed in** R' if $S = R'$.

When R is a domain, and K is the quotient field $R_{(0)}$, we shall simply say that R is **integrally closed** if it is integrally closed in K. Alternatively, some people say that R is **normal** in this case.

11.5 Example. The integers $\mathbb{Z} \subset \mathbb{C}$ have as integral closure the set of complex numbers x satisfying a monic polynomial with integral coefficients. This set is called the set of **algebraic integers**.

11.6 Example. i is an algebraic integer because it satisfies the equation $X^2 + 1 = 0$. $\frac{1-\sqrt{-3}}{2}$ is an algebraic integer, as we talked about last time; it is a sixth root of unity. On the other hand, $\frac{1+\sqrt{-5}}{2}$ is not an algebraic integer.

11.7 Example. Take $\mathbb{Z} \subset \mathbb{Q}$. The claim is that $\mathbb{Z}$ is integrally closed in $\mathbb{Q}$, or simply—integrally closed.

Proof. We will build on this proof on Friday. Here is the point. Suppose $\frac{a}{b} \in \mathbb{Q}$ satisfying an equation

$$p(a/b) = 0, \quad p(t) = t^n + c_1 t^{n-1} + \cdots + c_0, \ \forall c_i \in \mathbb{Z}.$$

Assume that a, b have no common factors; we must prove that b has no prime factors, so is ± 1. If b had a prime factor, say q, then we must obtain a contradiction.

We interrupt with a fancy definition.

11.8 Definition. The **valuation at** q (or q**-adic valuation**) is the map $v_q : \mathbb{Q}^* \to \mathbb{Z}$ is the function sending $q^k(a/b)$ to k if $q \nmid a, b$. We extend this to all rational numbers via $v(0) = \infty$.

In general, this just counts the number of factors of q in the expression.

Note the general property that

$$v_q(x+y) \geq \min(v_q(x), v_q(y)).$$

If x, y are both divisible by some power of q, so is $x + y$; this is the statement above. We also have the useful property

$$v_q(xy) = v_q(x) + v_q(y).$$

Now return to the proof that $\mathbb{Z}$ is normal. We would like to show that

$$v_q(a/b) \geq 0.$$

This will prove that b is not divisible by q.

We are assuming that $p(a/b) = 0$. In particular,

$$\left(\frac{a}{b}\right)^n = -c_1\left(\frac{a}{b}\right)^{n-1} - \cdots - c_0.$$

Apply v_q to both sides:

$$nv_q(a/b) \geq \min_i v_q(c_i(a/b)^{n-i}).$$

Since the $c_i \in \mathbb{Z}$, their valuations are nonnegative. In particular, the right hand side is at least

$$\min_i (n-i)v_q(a/b).$$

This cannot happen if $v_q(a/b) < 0$, because $n - i < n$ for each i. ▲

This argument applies more generally. If $R \subset K$ is a subring "defined by valuations," then R is integrally closed in K. We will talk more about this, and about valuation rings, next time. $\mathbb{Z}$ is defined by valuations in the sense that it consists of the elements of $\mathbb{Q}$ which have all nonnegative valuations.

We will finish this lecture by discussing what it means to be integrally closed geometrically.

11.9 Example. Here is a ring which is not integrally closed. Take $\mathbb{C}[x,y]/(x^2 - y^3)$.

In the complex plane, $\mathbb{C}^2$, this corresponds to the subvariety $C \subset \mathbb{C}^2$ defined by $x^2 = y^3$. In $\mathbb{R}^2$, this can be drawn: it has a singularity at $(x,y) = 0$.

Note that $x^2 = y^3$ if and only if there is a complex number z such that $x = z^3, y = z^2$. This complex number z can be recovered via x/y when $x, y \neq 0$. In particular, there is a map $\mathbb{C} \to C$ which sends $z \to (z^3, z^2)$. At every point other than the origin, the inverse can be recovered using rational functions. But this does not work at the origin.

We can think of $\mathbb{C}[x,y]/(x^2-y^3)$ as the subring R' of $\mathbb{C}[z]$ generated by $\{z^n, n \neq 1\}$. There is a map from $\mathbb{C}[x,y]/(x^2-y^3)$ sending $x \to z^3, y \to z^2$. Since these two domains are isomorphic, and R' is not integrally closed, it follows that $\mathbb{C}[x,y]/(x^2-y^3)$ is not integrally closed. The element z can be thought of as an element of the fraction field of R' or of $\mathbb{C}[x,y]/(x^2-y^3)$. It is integral, though.

The failure of integrally closedness has to do with the singularity at the origin.

We now give a generalization of the above example.

11.10 Example. This example is outside the scope of the present course. Say that $X \subset \mathbb{C}^n$ is given as the zero locus of some holomorphic functions $\{f_i : \mathbb{C}^n \to \mathbb{C}\}$. We just gave an example when $n = 2$. Assume that $0 \in X$, i.e. each f_i vanishes at the origin.

Let R be the ring of germs of holomorphic functions 0, in other words holomorphic functions from small open neighborhoods of zero. Each of these f_i becomes an element of R. The ring

$$R/(\{f_i\})$$

is called the ring of germs of holomorphic functions on X at zero.

Assume that R is a domain. This assumption, geometrically, means that near the point zero in X, X can't be broken into two smaller closed analytic pieces. The fraction field of R is to be thought of as the ring of germs of meromorphic functions on X at zero.

We state the following without proof:

11.11 Theorem. *Let g/g' be an element of the fraction field, i.e. $g, g' \in R$. Then g/g' is integral over R if and only if g/g' is bounded near zero.*

In the previous example of X defined by $x^2 = y^3$, the function x/y (defined near the origin on the curve) is bounded near the origin, so it is integral over the ring of germs of regular functions. The reason it is not defined near the origin is *not* that it blows up. In fact, it extends continuously, but not holomorphically, to the rest of the variety X.

Lecture 12
9/24

§1 Valuation rings

Today, we will talk about the notion of a "valuation ring."

12.1 Definition. A **valuation ring** is a domain R such that for every pair of elements $a, b \in R$, either $a \mid b$ or $b \mid a$.

12.2 Example. $\mathbb{Z}$ is not a valuation ring. Neither 2 divides 3 nor 3 divides 2.

12.3 Example. $\mathbb{Z}_{(p)}$, which is the set of all fractions of the form $a/b \in \mathbb{Q}$ where $p \nmid b$, is a valuation ring. To check whether a/b divides a'/b' or vice versa, you just have to check which is divisible by the larger power of p.

Remark. Let R be a valuation ring. Let K be the fraction field of R. Then for all $x \in K^*$, either x or x^{-1} belongs to R. Indeed, if $x = a/b$, $a, b \in R$, then either $a \mid b$ or $b \mid a$, so either x or $x^{-1} \in R$. This condition is equivalent to R's being a valuation ring.

Why are these called valuation rings? Well,

12.4 Definition. Let K be a field. A **valuation** on K is a map $v : K^* \to A$ for A is a totally ordered abelian group satisfying:

1. $v(xy) = v(x) + v(y)$. I.e., v is a homomorphism.

2. $v(x+y) \geq \min v(x), v(y)$. (We define $v(0) = \infty$ by convention; this is a formal constant bigger than everything in A.)

Suppose that K is a field and $v : K \to A \cup \{\infty\}$ is a valuation (i.e. $v(0) = \infty$). Define $R = \{x \in K : v(x) \geq 0\}$.

12.5 Proposition. *R as just defined is a valuation ring.*

Proof. First, we prove that R is a ring. R is closed under addition and multiplication by the two conditions

$$v(xy) = v(x) + v(y)$$

and

$$v(x+y) \geq \min v(x), v(y),$$

so if $x, y \in R$, then $x+y, xy$ have nonnegative valuations.

Note that $0 \in R$ because $v(0) = \infty$. Also $v(1) = 0$ since $v : K^* \to A$ is a homomorphism. So $1 \in R$ too. Finally, $-1 \in R$ because $v(-1) = 0$ since A is totally ordered. It follows that R is also a group.

Let us now show that R is a valuation ring. If $x \in K^*$, either $v(x) \geq 0$ or $v(x^{-1}) \geq 0$ since A is totally ordered.[8] So either $x, x^{-1} \in R$. ▲

In particular, the set of elements with nonnegative valuation is a valuation ring. The converse also holds. Whenever you have a valuation ring, it comes about in this manner.

12.6 Proposition. *Let R be a valuation ring with quotient field K. There is an ordered abelian group A and a valuation $v : K^* \to A$ such that R is the set of elements with nonnegative valuation.*

Proof. First, we construct A. In fact, it is the quotient of K^* by the subgroup of units R^* of R. We define an ordering by saying that $x \leq y$ if $y/x \in R$—this doesn't depend on the representatives in K^* chosen. Note that either $x \leq y$ or $y \leq x$ must hold, since R is a valuation ring. The combination of $x \leq y$ and $y \leq x$ implies that x, y are equivalent classes. The nonnegative elements in this group are those whose representatives in K^* belong to R.

It is easy to see that K^*/R^* in this way is a totally ordered abelian group with the image of 1 as the unit. The reduction map $K^* \to K^*/R^*$ defines a valuation whose corresponding ring is just R. We have omitted some details; for instance, it should be checked that the valuation of $x+y$ is at least the minimum of $v(x), v(y)$. ▲

To summarize:

> Every valuation ring R determines a valuation v from the fraction field of R into $A \cup \{\infty\}$ for A a totally ordered abelian group such that R is just the set of elements of K with nonnegative valuation. As long as we require that $v : K^* \to A$ is surjective, then A is uniquely determined as well.

12.7 Definition. A valuation ring R is **discrete** if we can choose A to be $\mathbb{Z}$.

12.8 Example. $\mathbb{Z}_{(p)}$ is a discrete valuation ring.

The notion of a valuation ring is a useful one.

[8] Otherwise $0 = v(x) + v(x^{-1}) < 0$, contradiction.

§2 General remarks

Let R be a commutative ring. Then Spec$R$ is the set of primes of R, equipped with a certain topology. The space Spec$R$ is almost never Hausdorff. It is almost always a bad idea to apply the familiar ideas from elementary topology (e.g. the fundamental group) to Spec$R$. Nonetheless, it has some other nice features that substitute for its non-Hausdorffness.

For instance, if $R = \mathbb{C}[x, y]$, then Spec$R$ corresponds to $\mathbb{C}^2$ with some additional nonclosed points. The injection of $\mathbb{C}^2$ with its usual topology into Spec$R$ is continuous. While in Spec$R$ you don't want to think of continuous paths, you can in $\mathbb{C}^2$.

Suppose you had two points $x, y \in \mathbb{C}^2$ and their images in Spec$R$. Algebraically, you can still think about algebraic curves passing through x, y. This is a subset of x, y defined by a single polynomial equation. This curve will have what's called a "generic point," since the ideal generated by this curve will be a prime ideal. The closure of this generic point will be precisely this algebraic curve—including x, y.

Remark. If $\mathfrak{p}, \mathfrak{p}' \in$ Spec$R$, then

$$\mathfrak{p}' \in \overline{\{\mathfrak{p}\}}$$

iff

$$\mathfrak{p}' \supset \mathfrak{p}.$$

Why is this? Well, the closure of $\{\mathfrak{p}\}$ is just $V(\mathfrak{p})$, since this is the smallest closed subset of Spec$R$ containing $\mathfrak{p}$.

The point of this discussion is that instead of paths, one can transmit information from point to point in Spec$R$ by having one point be in a closure of another. However, we will show that this relation is contained by the theory of valuation rings.

12.9 Theorem. *Let R be a domain containing a prime ideal $\mathfrak{p}$. Let K be the fraction field of R.*

Then there is a valuation v on K defining a valuation ring $R' \subset K$ such that

1. $R \subset R'$.
2. $\mathfrak{p} = \{x \in R : v(x) > 0\}$.

Let us motivate this by the remark:

Remark. A valuation ring is automatically a local ring. A local ring is a ring where either $x, 1 - x$ is invertible for all x in the ring. Let us show that this is true for a valuation ring.

If x belongs to a valuation ring R with valuation v, it is invertible if $v(x) = 0$. So if $x, 1 - x$ were both noninvertible, then both would have positive valuation. However, that would imply that $v(1) \geq \min v(x), v(1 - x)$ is positive, contradiction.

> If R' is any valuation ring (say defined by a valuation v), then R' is local with maximal ideal consisting of elements with positive valuation.

The theorem above says that there's a good supply of valuation rings. In particular, if R is any domain, $\mathfrak{p} \subset R$ a prime ideal, then we can choose a valuation ring $R' \supset R$ such that $\mathfrak{p}$ is the intersection of the maximal ideal of R' intersected with R. So the map $\mathrm{Spec} R' \to \mathrm{Spec} R$ contains $\mathfrak{p}$.

Proof. Without loss of generality, replace R by $R_{\mathfrak{p}}$, which is a local ring with maximal ideal $\mathfrak{p}R_{\mathfrak{p}}$. The maximal ideal intersects R only in $\mathfrak{p}$.

So, we can assume without loss of generality that

1. R is local.

2. $\mathfrak{p}$ is maximal.

Let P be the collection of all subrings $R' \subset K$ such that $R' \supset R$ but $\mathfrak{p}R' \neq R'$. Then P is a poset under inclusion. The poset is nonempty, since $R \in P$. Every totally ordered chain in P has an upper bound. If you have a totally ordered subring of elements in P, then you can take the union. We invoke:

12.10 Lemma. *Let R_α be a chain in P and $R' = \bigcup R_\alpha$. Then $R' \in P$.*

Proof. Indeed, it is easy to see that this is a subalgebra of K containing R. The thing to observe is that

$$\mathfrak{p}R' = \bigcup_\alpha \mathfrak{p}R_\alpha;$$

since by assumption, $1 \notin \mathfrak{p}R_\alpha$ (because each $R_\alpha \in P$), $1 \notin \mathfrak{p}R'$. In particular, $R' \notin P$. ▲

By the lemma, Zorn's lemma to the poset P. In particular, P has a maximal element R'. By construction, R' is some subalgebra of K and $\mathfrak{p}R' \neq R'$. Also, R' is maximal with respect to these properties.

We show first that R' is local, with maximal ideal $\mathfrak{m}$ satisfying

$$\mathfrak{m} \cap R = \mathfrak{p}.$$

The second part is evident from locality of R', since $\mathfrak{m}$ must contain the proper ideal $\mathfrak{p}R'$, and $\mathfrak{p} \subset R$ is a maximal ideal.

Suppose that $x \in R'$; we show that either $x, 1-x$ belongs to R'^* (i.e. is invertible). Take the ring $R'[x^{-1}]$. If x is noninvertible, this properly contains R'. By maximality, it follows that $\mathfrak{p}R'[x^{-1}] = R'[x^{-1}]$.

And we're out of time. We'll pick this up on Monday.

▲

Lecture 13
[Section] 9/26

The next few section lectures will focus on Fitting ideals.

We need to review Nakayama's lemma.

§1 Nakayama's lemma

13.1 Lemma (Nakayama)**.** *Let R be a local ring, $\mathfrak{p}$ the maximal ideal, M a finitely generated R-module.*

Then if $M = \mathfrak{p}M$, we have $M = 0$.

Moreover, any lift of a $R/\mathfrak{p}$-basis of $M/\mathfrak{p}M$ to M generates M.

Proof. Omitted for now. Probably, it will be covered in class. ▲

§2 Complexes

We now review a little homological algebra.

13.2 Definition. A **complex** of R-modules is a sequence of R-modules

$$\to F_n \xrightarrow{d} F_{n-1} \to \dots \to F_1 \to F_0 \to \dots$$

such that the composite of two consecutive differentials is zero.

13.3 Definition. The n-th **homology** of the complex, denoted $H_n(F)$, is defined as $\ker(F_n \to F_{n-1})/\mathrm{Im}(F_{n+1} \to F_n)$. The complex is **acyclic** if it has trivial homology.

Note that we can add complexes. If F, G are complexes, then $F \oplus G$ is a complex whose n-th term is $F_n \oplus G_n$. Then

$$H_n(F \oplus G) = H_n(F) \oplus H_n(G).$$

13.4 Definition. A complex is called **flat** (resp. **free, projective**) if each module in question is flat (resp. free, projective).

13.5 Example. The complex

$$0 \to R \xrightarrow{1} R \to 0.$$

is acyclic and has trivial homology. A direct sum of these is called a **trivial complex**.

13.6 Lemma. *If R is local, then an acyclic free complex with a right endpoint (i.e. of the form $\dots \to F_1 \to F_0 \to 0$) is a direct sum of trivial complexes.*

Proof. This is an easy exercise following from the fact that any projective module over a local ring is free. ▲

Suppose R is noetherian. Then M has a resolution by finitely generated free modules. Indeed, start by taking a surjection $R^{n_0} \twoheadrightarrow M$; the kernel M_1 is finitely generated since R is noetherian, so there is an surjection $R^{n_1} \twoheadrightarrow M_1$. There is an exact sequence

$$R^{n_1} \to R^{n_0} \to M \to 0$$

which we can continue indefinitely to the left. In this way, we get a **free resolution** of M.

Free resolutions are not unique, because you can add trivial complexes.

Let now R be a local noetherian ring, $\mathfrak{p}$ local, $k = R/\mathfrak{p}$. Let $m_1, \dots, m_{n_0} \in M$ be a lifting of a k-basis for $M \otimes_R k$. Then we have a surjection

$$R^{n_0} \to M \to 0$$

in view of Nakayama. We can take the kernel M_1 and lift a k-basis for $M_1 \otimes_R k$ to get a surjection into M_1, and repeat this. So we get a free resolution

$$\cdots \to R^{n_1} \to R^{n_0} \to M \to 0.$$

Note that the image of the first differential d_1 lies in $\mathfrak{p}R^{n_0}$. This is true more generally: the image of d_i is contained in $\mathfrak{p}R^{n_i}$. The reason is simply that we lifted *bases* over the reductions mod k.

13.7 Definition. A **minimal free resolution** over a local ring R is a free resolution

$$\cdots \to F_1 \to F_0 \to 0$$

such that $\operatorname{Im}(d_n) \subset \mathfrak{p}F_{n-1}$.

We know that a minimal free resolution always exists by the above discussion.

Why is this interesting?

13.8 Theorem. *Let F be a minimal free resolution of M. If $\cdots \to G_1 \to G_0 \to M$ is another finitely generated free resolution of M, then G is a direct sum of F and a trivial complex.*

13.9 Corollary. *A minimal free resolution is unique.*

Proof of the theorem. We need to find a split injection from $F \to G$. The cokernel will be an acyclic projective, hence free, complex; this will imply by the earlier lemma that G is trivial.

We now need a lemma in homological algebra:

13.10 Lemma. *Let R be any ring. Suppose given two complexes of R-modules*

$$F : \cdots \to F_1 \to F_0 \to M \to 0$$

and

$$G : \cdots \to G_1 \to G_0 \to N \to 0.$$

Suppose F is projective and G acyclic. Then any $M \to N$ extends to a map of complexes.

Any two such liftings differ by a chain homotopy.[9]

Proof. Since $F_0 \to M \to N$ is defined, we can lift $F_0 \to G_0$ since G_0 is projective. Now $F_1 \to F_0 \to G_0$ lands in the image of $G_1 \to G_0$ since it is killed when you go to N. Thus $F_1 \to G_0$ can be lifted to $F_1 \to G_1$. Inductively, you keep going.

The proof of the chain homotopy fact can be proved similarly. (This is a loose sketch.) ▲

[9] Recall that this means that for each n, ther is a map $h : F_n \to G_{n+1}$ such that the difference between the two liftings $F \to G$ is $dh + hd$.

In our case, we have two free resolutions of the same module M; both are projective and acyclic. There is thus a map $\alpha : F \to G$ extending the identity $M \to M$. Similarly, we get a map of complexes $\beta : G \to F$ extending the identity. Since $\alpha \circ \beta, \beta \circ \alpha$ are maps $G \to G, F \to F$ extending the identity, $\alpha \circ \beta$ and $\beta \circ \alpha$ are chain homotopic to the identity. In particular, we can find maps $h_n : F_n \to F_{n+1}$ such that

$$(1 - \beta_n \alpha_n) = d_{n+1} h_n + h_{n-1} d_n.$$

But the d_n have images in $\mathfrak{p} F_n$. This is because F is minimal free.

Therefore, the matrix representative of $\beta_n \alpha_n$ of the form

$$I + \begin{bmatrix} \mathfrak{p} & \mathfrak{p} & \mathfrak{p} \\ \mathfrak{p} & & \end{bmatrix}$$

In particular, the determinant of $\beta_n \alpha_n : F_n \to F_n$ is equal to one modulo $\mathfrak{p}$, in particular it is invertible. So $\beta_n \alpha_n$ is invertible since its determinant is invertible. It follows that α_n must therefore be a split injection because its inverse is $(\beta_n \alpha_n)^{-1} \beta_n$. ▲

§3 Fitting ideals

Let R be a general ring. If $\phi : F \to G$ is a map between finitely generated free modules, then in a basis $\{f_1, \dots, f_m\}$ for F and a basis $\{g_1, \dots, g_n\}$ for G, we have

$$\phi(f_i) = \sum a_{ij} g_j$$

for some $a_{ij} \in R$. Then we have represented ϕ as a matrix

$$\begin{bmatrix} a_{11} & a_{21} & \dots \\ a_{12} & \dots & \\ \vdots & & \end{bmatrix}$$

Now consider the map

$$\wedge^l \phi : \wedge^l F \to \wedge^l G.$$

You can convince yourself that this sends $f_{i_1} \wedge \dots f_{i_l}$ of suitable sums of l-by-l minors. Namely,

$$(\wedge^l \phi)(f_{i_1} \wedge \dots f_{i_l}) = \sum \det \begin{bmatrix} a_{i_1 j_1} & \dots & a_{i_l j_1} \\ \vdots & & \vdots \\ a_{i_1 j_l} & \dots & a_{i_l j_l} \end{bmatrix} g_{j_1} \wedge \dots \wedge g_{j_l}$$

13.11 Definition. Define $I_l \phi$ as the image of $\wedge^l F \otimes (\wedge^l G)^* \to R$, which is the ideal generated by the l-by-l minors of ϕ.

13.12 Definition. Let M be of **finite presentation**, i.e. one with a resolution $F \xrightarrow{\phi} G \to M \to 0$ where F, G are finite free. Let G have rank r. Then we call $I_{r-i}(\phi)$ the i**th Fitting ideal.**

Let us show that these are unique and depend only on M.

Proof. Suppose given two free resolutions

$$F \xrightarrow{\phi} G \to M \to 0$$

and

$$F' \xrightarrow{\phi'} G' \to M \to 0.$$

Suppose G has rank r and G' rank r'. We will show that $I_{r-i}(\phi) = I_{r'-i}(\phi')$.

Suppose, without loss of generality, that R is local. To show that two ideals are equal, it is sufficient to show that their localizations are, so this is acceptable. Then we can assume that one of them is a minimal resolution and the other a sum of the minimal one and a trivial complex. Then ϕ' is of the form $\phi \oplus 1_{R^t}$, so the second resolution is just the first with $0 \to R^t \to R^t \to 0$ added to it. Any nonzero $k+t$ by $k+t$ minor of ϕ' comes from a k by k minor of ϕ and a t by t minor of 1_t. From this it can be seen that the two Fitting ideals are the same.

▲

13.13 Definition. So it makes sense to define

$$\mathrm{Fitt}_k(M)$$

as the k-th **Fitting ideal** of M (i.e. the Fitting ideal of any finite free resolution, which is well defined by the argument above).

Remark. By cofactor expansion,

$$I_{l+1}(\phi) = I_l(\phi).$$

Remark. $I_k(\phi \oplus \phi') = \sum_{i+j=k} I_i \phi I_j \phi'$. This follows by the definitions. This implies a formula for the Fitting ideals. In particular,

$$\mathrm{Fitt}_k(M_1 \oplus M_2) = \sum_{i+j=k} \mathrm{Fitt}_i(M_1)\mathrm{Fitt}_j(M_2).$$

We can define the "polynomial series"

$$\mathrm{Fitt}_M(t) = \sum_n \mathrm{Fitt}_n(M) t^n,$$

which is a formal power series whose coefficients are ideals of R.

§4 Examples

These notes are a bit sketchy because I'm having trouble following the lecture.

13.14 Example. Let us compute the Fitting ideals for the R-module R/I. Then a generator is 1. Then we have an exact sequence

$$I \rightarrowtail R \twoheadrightarrow R/I$$

so if we pick a finite generating set $(a_1, \dots, a_n)$ in I, we have a resolution

$$R^n \overset{\phi}{\to} R \twoheadrightarrow R/I.$$

Here ϕ sends a vector to its dot product with $(a_1, \dots, a_n)$. The matrix representing ϕ is just

$$(a_1, \dots, a_n).$$

In particular, the zeroth Fitting ideal or $I_1(\phi)$ is the ideal generated by the 1-by-1 minors, i.e. I itself. The first Fitting ideal is $I_0(\phi)$, which is by convention R. The Fitting polynomial is then

$$I + Rt + Rt^2 + \dots.$$

13.15 Example. Let us compute the Fitting ideal for the R-module R^k. Then the resolution

$$0 \overset{\phi=0}{\to} R^k \to R^k \to 0$$

works, where $\phi = 0$. The Fitting ideals are just zero and R. One can check that the Fitting polynomial is

$$Rt^k + Rt^{k+1} + \dots.$$

In general, $\mathrm{Fitt}_j(M)$ should be thought of as the obstruction to M being generated by j elements. If M is generated by j elements, then its jth Fitting ideal is M. Nonetheless, it is possible that the Fitting ideal is R but the module is not generated by j elements.

13.16 Example. Take $R = \mathbb{Z}[\sqrt{-5}]$ and $M = (2, 1 + \sqrt{-5})$. It can be checked that $\mathrm{Fitt}_1(M) = R$, but the ideal M is not principal.

13.17 Proposition. *If R is local and $\mathrm{Fitt}_j(M) = R$, then M is generated by j elements.*

Proof. Next time. ▲

So the correct statement over every ring is that $\mathrm{Fitt}_j = R$ if and only if M is *locally* j-generated.

Remark. Fitting ideals behave well under base change. In particular, if $R \to S$ is a morphism of rings, then

$$\mathrm{Fitt}_j(M) \otimes_R S = \mathrm{Fitt}_j(M \otimes_R S).$$

It is possible to use the Fitting polynomial to characterize modules over PIDs.

13.18 Theorem. *Over a PID, the Fitting ideal generates the (finitely generated) module.*

This is also true over Dedekind domains to a limited extent:

13.19 Theorem. *Over a Dedekind domain, the Fitting polynomial determines the torsion part of a module and the rank of the projective part.*

We will probably go over the classification of modules over a Dedekind domain. Note that the Fitting ideals can't tell you more about the projective module because those are always degenerate.

13.20 Theorem. *Let R be any noetherian ring. M is projective of constant rank*[10] *r if and only if*

$$\mathrm{Fitt}_M(t) = Rt^r + Rt^{r+1} + \dots.$$

Lecture 14
9/27

§1 Valuation rings, continued

Let us set a goal for today.

First, recall the notion introduced last time. A **valuation ring** is a domain R where for all x in the fraction field of R, either x or x^{-1} lies in R. We saw that if R is a valuation ring, then R is local. That is, there is a unique maximal ideal $\mathfrak{m} \subset R$, automatically prime. Moreover, the zero ideal (0) is prime, as R is a domain. So if you look at the spectrum $\mathrm{Spec} R$ of a valuation ring R, there is a unique closed point $\mathfrak{m}$, and a unique generic point (0). There might be some other prime ideals in $\mathrm{Spec} R$; this depends on where the additional valuation lives.

14.1 Example. Suppose the valuation defining the valuation ring R takes values in $\mathbb{R}$. Then the only primes are $\mathfrak{m}$ and zero.

Let R now be any ring, with $\mathrm{Spec} R$ containing prime ideals $\mathfrak{p} \subset \mathfrak{q}$. In particular, $\mathfrak{q}$ lies in the closure of $\mathfrak{p}$. As we will see, this implies that there is a map

$$\phi : R \to R'$$

such that $\mathfrak{p} = \phi^{-1}(0)$ and $\mathfrak{q} = \phi^{-1}(\mathfrak{m})$, where $\mathfrak{m}$ is the maximal ideal of R'. This statement says that the relation of closure in $\mathrm{Spec} R$ is always controlled by valuation rings. In yet another phrasing, in the map

$$\mathrm{Spec} R' \to \mathrm{Spec} R$$

the closed point goes to $\mathfrak{q}$ and the generic point to $\mathfrak{p}$. This is our eventual goal.

To carry out this goal, we need some more elementary facts. Let us discuss things that don't have any obvious relation to it.

§2 Some useful tools

We will need:

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

[10] I.e. the ranks at all localizations are r.

Note that $\mathfrak{m}M$ is the submodule generated by products of elements of $\mathfrak{m}$ and M.

Remark. This states that if M is finitely generated, then

$$M \otimes_R R/\mathfrak{m} = M/\mathfrak{m}M \neq 0.$$

So to prove that a finitely generated module over a local ring is zero, you can reduce to studying the reduction to $R/\mathfrak{m}$. This is thus a very useful criterion.

Proof. Suppose M is generated by $\{x_1, \dots, x_n\} \subset M$. This means that every element of M is a linear combination of elements of x_i. However, each $x_i \in \mathfrak{m}M$ by assumption. In particular, each x_i can be written as

$$x_i = \sum a_{ij} x_j, \text{ where } a_{ij} \in \mathfrak{m}.$$

If we let A be the matrix $\{a_{ij}\}$, then A sends the vector of the $\{x_i\}$ into itself. In particular, $(I - A)$ kills the vectors x_i.

Now $I - A$ is an n-by-n matrix in the ring R. We could, of course, reduce everything modulo $\mathfrak{m}$ to get the identity; this is because A consists of elements of $\mathfrak{m}$. It follows that the determinant must be congruent to 1 modulo $\mathfrak{m}$.

In particular, $\det(I - A)$ is invertible, since R is local. It follows that $I - A$ is itself invertible. This, however, is a contradiction, since it kills the vector $\{x_i\}$, unless all the x_i are zero. ▲

Nakayama's lemma highlights why it is so useful to work over a local ring. Thus, it is useful to reduce questions about general rings to questions about local rings.

OK. Let us recall:

14.3 Definition. A map of rings $\phi : R \to R'$ is **integral** if ϕ is injective and each element $x \in R'$ is integral over R (i.e. the image $\phi(R)$), or satisfies a monic polynomial whose coefficients lie in the image of the homomorphism ϕ.

We now interpret integrality in terms of the geometry of Spec.

14.4 Proposition (Lying over). *If $\phi : R \to R'$ is an integral extension, then the induced map*

$$\mathrm{Spec} R' \to \mathrm{Spec} R$$

is surjective.

Another way to state this, without mentioning $\mathrm{Spec} R'$, is that if $\mathfrak{p} \subset R$ is prime, then there exists $\mathfrak{q} \subset R'$ such that $\mathfrak{p}$ is the inverse image $\phi^{-1}(\mathfrak{q})$.

Proof. First, let us reduce to the case of a local ring. We replace R with $R_{\mathfrak{p}}$. We get a map

$$\phi_{\mathfrak{p}} : R_{\mathfrak{p}} \to (R - \mathfrak{p})^{-1} R'$$

which is injective if ϕ is, since localization is an exact functor. Here we have localized both R, R' at the multiplicative subset $(R - \mathfrak{p})$.

Note that $\phi_{\mathfrak{p}}$ is an integral extension too, i.e. every x/s with $x \in R', s \in R - \mathfrak{p}$ satisfies a monic polynomial with coefficients in $R_{\mathfrak{p}}$. To see this, note that x is integral over R, so there is a monic polynomial

$$x^n + a_1 x^{n-1} + \cdots + a_0 = 0, \quad \forall a_i \in R \ (= \phi(R)).$$

We can divide this by s^n:

$$(\frac{x}{s})^n + \frac{a_1}{s}(\frac{x}{s})^{n-1} + \cdots + \frac{a_0}{s^n} = 0,$$

where each fraction in the coefficient is in the image of $\phi_{\mathfrak{p}}$. That proves that $\phi_{\mathfrak{p}}$ is also integral.

We will prove the result for $\phi_{\mathfrak{p}}$. In particular, we will show that there is a prime ideal of $(R-\mathfrak{p})^{-1}R'$ that pulls back to $\mathfrak{p}R_{\mathfrak{p}}$. These will imply that if we pull this prime ideal back to R', it will pull back to $\mathfrak{p}$ in R. So it is sufficient for the proposition to handle the case of R local.

Upshot: we can assume R is local with maximal ideal $\mathfrak{p}$. We assume this now. So, we want to find a prime ideal $\mathfrak{q} \subset R'$ such that $\mathfrak{p} = \phi^{-1}(\mathfrak{q})$. Since $\mathfrak{p}$ is already maximal, it will suffice to show that $\mathfrak{p} \subset \phi^{-1}(\mathfrak{q})$. In particular, we need to show that there is a prime ideal $\mathfrak{q}$ such that

$$\mathfrak{p}R' \subset \mathfrak{q}.$$

The pull-back of this will be $\mathfrak{p}$.

If $\mathfrak{p}R' \neq R'$, then $\mathfrak{q}$ exists, since every proper ideal of a ring is contained in a maximal ideal. In particular, we need to show that

$$\mathfrak{p}R' \neq R',$$

or that $\mathfrak{p}$ doesn't generate the unit ideal in R'. Suppose the contrary. Then $1 \in \mathfrak{p}R'$ and we can write

$$1 = \sum x_i \phi(y_i)$$

where $x_i \in R', y_i \in \mathfrak{p}$.

Let R'' be the subalgebra of R' generated by $\phi(R)$ and the x_i. Then $R'' \subset R'$ and is finitely generated over R, because it is generated by the x_i. However, R'' is actually finitely generated as an R-module too, because each x_i satisfies a monic polynomial with coefficients in R. This is where integrality comes in.

So we have that R'' is a finitely generated R-module. Also, the expression $1 = \sum x_i \phi(y_i)$ shows that $\mathfrak{p}R'' = R''$. However, this contradicts Nakayama's lemma. That brings the contradiction, showing that $\mathfrak{p}$ cannot generate (1) in R', proving the lying over theorem.

▲

§3 Back to the goal

Now we return to the goal of the lecture. Again, R was any ring, and we had primes $\mathfrak{p} \subset \mathfrak{q} \subset R$. We wanted a valuation ring R' and a map $\phi : R \to R'$ such that zero pulled back to $\mathfrak{p}$ and the maximal ideal pulled back to $\mathfrak{q}$.

What does it mean for $\mathfrak{p}$ to be the inverse image of $(0) \subset R'$? This means that $\mathfrak{p} = \ker \phi$. So we get an injection

$$R/\mathfrak{p} \rightarrowtail R'.$$

We will let R' be a subring of the quotient field K of the domain $R/\mathfrak{p}$. Of course, this subring will contain $R/\mathfrak{p}$.

In this case, we will get a map $R \to R'$ such that the pull-back of zero is $\mathfrak{p}$. What we want, further, to be true is that R' is a valuation ring and the pull-back of the maximal ideal is $\mathfrak{q}$.

This is starting to look at the problem we discussed last time. Namely, let's throw out R, and replace it with $R/\mathfrak{p}$. Moreover, we can replace R with $R_{\mathfrak{q}}$ and assume that R is local with maximal ideal $\mathfrak{q}$. What we need to show is that a valuation ring R' contained in the fraction field of R, containing R, such that the intersection of the maximal ideal of R' with R is equal to $\mathfrak{q} \subset R$. If we do this, then we will have accomplished our goal.

14.5 Lemma. *Let R be a local domain. Then there is a valuation subring R' of the quotient field of R that* dominates *R, i.e .the map $R \to R'$ is a* local *homomorphism.*

Let's find R' now.

Choose R' maximal such that $\mathfrak{q}R' \neq R'$. Such a ring exists, by Zorn's lemma. We gave this argument at the end last time.

14.6 Lemma. *R' as described is local.*

Proof. Look at $\mathfrak{q}R' \subset R'$; it is a proper subset, too, by assumption. In particular, $\mathfrak{q}R'$ is contained in some maximal ideal $\mathfrak{m} \subset R'$. Replace R' by $R'' = R'_{\mathfrak{m}}$. Note that

$$R' \subset R''$$

and

$$\mathfrak{q}R'' \neq R''$$

because $\mathfrak{m}R'' \neq R''$. But R' is maximal, so $R' = R''$, and R'' is a local ring. So R' is a local ring. ▲

Let $\mathfrak{m}$ be the maximal ideal of R'. Then $\mathfrak{m} \supset \mathfrak{q}R$, so $\mathfrak{m} \cap R = \mathfrak{q}$. All that is left to prove now is that R' is a valuation ring.

14.7 Lemma. *R' is integrally closed.*

Proof. Let R'' be its integral closure. Then $\mathfrak{m}R'' \neq R''$ by lying over, since $\mathfrak{m}$ (the maximal ideal of R') lifts up to R''. So R'' satisfies

$$\mathfrak{q}R'' \neq R''$$

and by maximality, we have $R'' = R'$. ▲

To summarize, we know that R' is a local, integrally closed subring of the quotient field of R, such that the maximal ideal of R' pulls back to $\mathfrak{q}$ in R. All we now need is:

14.8 Lemma. *R' is a valuation ring.*

Proof. Let x lie in the fraction field. We must show that either x or $x^{-1} \in R'$. Say $x \notin R'$. This means by maximality of R' that $R'' = R'[x]$ satisfies

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

In particular, we can write

$$1 = \sum q_i x^i, \quad q_i \in \mathfrak{q}R' \subset R'.$$

This implies that

$$(1 - q_0) + \sum_{i>0} -q_i x^i = 0.$$

But $1 - q_0$ is invertible in R', since R' is local. We can divide by the highest power of x:

$$x^{-N} + \sum_{i>0} \frac{-q_i}{1 - q_0} x^{-N+i} = 0.$$

In particular, $1/x$ is integral over R'; this implies that $1/x \in R'$ since R' is integrally closed and q_0 is a nonunit. So R' is a valuation ring. ▲

We can state the result formally.

14.9 Theorem. *Let R be a ring, $\mathfrak{p} \subset \mathfrak{q}$ prime ideals. Then there is a homomorphism $\phi : R \to R'$ into a valuation ring R' with maximal ideal $\mathfrak{m}$ such that*

$$\phi^{-1}(0) = \mathfrak{p}$$

and

$$\phi^{-1}(\mathfrak{m}) = \mathfrak{q}.$$

There is a related fact which we now state.

14.10 Theorem. *Let R be any domain. Then the integral closure of R in the quotient field K is the intersection*

$$\bigcap R_\alpha$$

of all valuation rings $R_\alpha \subset K$ containing R.

So an element of the quotient field is integral over R if and only if its valuation is nonnegative at every valuation which is nonnegative on R.

Proof. The $\subset$ argument is easy, because one can check that a valuation ring is integrally closed. (Exercise.) The interesting direction is to assume that $v(x) \geq 0$ for all v nonnegative on R.

Let us suppose x is nonintegral. Suppose $R' = R[1/x]$ and I be the ideal $(x^{-1}) \subset R'$. There are two cases:

1. $I = R'$. Then in the ring R', x^{-1} is invertible. In particular, $x^{-1}P(x^{-1}) = 1$. Multiplying by a high power of x shows that x is integral over R. Contradiction.

2. Suppose $I \subsetneq R'$. Then I is contained in a maximal ideal $\mathfrak{q} \subset R'$. There is a valuation subring $R'' \subset K$, containing R', such that the corresponding valuation is positive on $\mathfrak{q}$. In particular, this valuation is positive on x^{-1}, so it is negative on x, contradiction.

▲

So the integral closure has this nice characterization via valuation rings. In some sense, the proof that $\mathbb{Z}$ is integrally closed has the property that every integrally closed ring is integrally closed for that reason: it's the common nonnegative locus for some valuations.

Lecture 15
9/29

§1 Noetherian rings and modules

The finiteness condition of a noetherian ring makes commutative algebra much nicer.

15.1 Definition. Let R be a commutative ring and M an R-module. We say that M is **noetherian** if every submodule of M is finitely generated.

15.2 Definition. R is **noetherian** if R is noetherian as an R-module. In particular, this says that all of its ideals are finitely generated.

15.3 Example. 1. Any field is noetherian. There are two ideals: (1) and (0).

2. Any PID is noetherian: any ideal is generated by one element. So $\mathbb{Z}$ is noetherian.

First, let's just think about the condition of modules. Here is a convenient reformulation of it.

15.4 Proposition. *M is a module over R. The following are equivalent:*

1. *M is noetherian.*
2. *Every chain of submodules of M, $M_0 \subset M_1 \subset \dots$, eventually stabilizes at some M_N. (Ascending chain condition.)*

Proof. Say M is noetherian and we have such a chain

$$M_0 \subset M_1 \subset \dots .$$

Write

$$M' = \bigcup M_i \subset M,$$

which is finitely generated since M is noetherian. Let it be generated by $x_1, \dots, x_n$. Each of these finitely many elements is in the union, so they are all contained in some M_N. This means that

$$M' \subset M_N, \quad \text{so} \quad M_N = M'$$

and the chain stabilizes.

For the converse, assume the ACC. Let $M' \subset M$ be any submodule. Define a chain of submodules $M_0 \subset M_1 \subset \cdots \subset M'$ as follows. First, just take $M_0 = \{0\}$. Take M_{n+1} to be M_n plus the submodule generated by some $x \in M' - M_n$, if this is possible. So M_0 is zero, M_1 is generated by some nonzero element of M', M_2 is M_1 together with some element of M' not in M_1. By construction, we have an ascending chain, so it stabilizes at some finite place. This means at some point, it is impossible to choose something in M' that does not belong to some M_N. In particular, M' is generated by N elements, since M_N is. ▲

15.5 Proposition. *If*

$$M' \rightarrowtail M \twoheadrightarrow M''$$

is an exact sequence of modules, then M is noetherian if and only if M', M'' are.

One direction says that noetherianness is preserved under subobjects and quotients.

Proof. If M is noetherian, then every submodule of M' is a submodule of M, so is finitely generated. So M' is noetherian too. Now we show that M'' is noetherian. Let $N \subset M''$ and let $\widetilde{N} \subset M$ the inverse image. Then $\widetilde{N}$ is finitely generated, so N—as the homomorphic image of $\widetilde{N}$—is finitely generated So M'' is noetherian.

Suppose M', M'' noetherian. We prove M noetherian. Let's verify the ascending chain condition. Consider

$$M_1 \subset M_2 \subset \cdots \subset M.$$

Let M_i'' denote the image of M_i in M'' and let M_i' be the intersection of M_i with M'. Here we think of M' as a submodule of M. These are ascending chains of submodules of M', M'', respectively, so they stabilize by noetherianness. So for some N, we have that $n \geq N$ implies

$$M_n' = M_{n+1}', \quad M_n'' = M_{n+1}''.$$

We claim that this implies, for such n,

$$M_n = M_{n+1}.$$

Why? Say $x \in M_{n+1} \subset M$. Then x maps into something in $M_{n+1}'' = M_n''$. So there is something in M_n, call it y, such that x, y go to the same thing in M''. In particular,

$$x - y \in M_{n+1}$$

goes to zero in M'', so $x - y \in M'$. Thus $x - y \in M_{n+1}' = M_n'$. In particular,

$$x = (x - y) + y \in M_n' + M_n = M_n.$$

So $x \in M_n$, and

$$M_n = M_{n+1}.$$

This proves the result. ▲

The class of noetherian modules is thus "robust." We can get from that the following.

15.6 Proposition. *If $\phi : A \to B$ is a surjection of commutative rings and A is noetherian, then B is noetherian too.*

Proof. Indeed, B is noetherian as an A-module; indeed, it is the quotient of a noetherian A-module (namely, A). However, it is easy to see that the A-submodules of B are just the B-modules in B, so B is noetherian as a B-module too. So B is noetherian. ▲

Another easy stability property:

15.7 Proposition. *Let R be a commutative ring, $S \subset R$ a multiplicatively closed subset. If R is noetherian, then $S^{-1}R$ is noetherian.*

I.e., the class of noetherian rings is closed under localization.

Proof. Say $\phi : R \to S^{-1}R$ is the canonical map. Let $I \subset S^{-1}R$ be an ideal. Then $\phi^{-1}(I) \subset R$ is an ideal, so finitely generated. It follows that

$$\phi^{-1}(I)(S^{-1}R) \subset S^{-1}R$$

is finitely generated as an ideal in $S^{-1}R$; the generators are the images of the generators of $\phi^{-1}(I)$.

Now we claim that

$$\phi^{-1}(I)(S^{-1}R) = I.$$

The inclusion $\subset$ is trivial. For the latter inclusion, if $x/s \in I$, then $x \in \phi^{-1}(I)$, so

$$x = (1/s)x \in (S^{-1}R)\phi^{-1}(I).$$

This proves the claim and implies that I is finitely generated. ▲

§2 The basis theorem

Let us now prove something a little less formal.

15.8 Theorem (Hilbert basis theorem)**.** *If R is a noetherian ring, then the polynomial ring $R[X]$ is noetherian.*

Proof. Let $I \subset R[X]$ be an ideal. We prove that it is finitely generated. For each $m \in \mathbb{Z}_{\geq 0}$, let $I(n)$ be the collection of elements $a \in R$ consisting of the coefficients of x^n of elements of I of degree $\leq n$. This is an ideal, as is easily seen.

In fact, we claim that

$$I(1) \subset I(2) \subset \dots$$

which follows because if $a \in I(1)$, there is an element $aX + \dots$ in I. Thus $X(aX + \dots) = aX^2 + \dots \in I$, so $a \in I(2)$. And so on.

Since R is noetherian, this chain stabilizes at some $I(N)$. Also, because R is noetherian, each $I(n)$ is generated by finitely many elements $a_{n,1}, \dots, a_{n,m_n} \in I(n)$. All of these come from polynomials $P_{n,i} \in I$ such that $P_{n,i} = a_{n,i}X^n + \dots$.

The claim is that the $P_{n,i}$ for $n \leq N$ and $i \leq m_n$ generate I. This is a finite set of polynomials, so if we prove the claim, we will have proved the basis theorem. Let J be the ideal generated by $\{P_{n,i}, n \leq N, i \leq m_n\}$. We know $J \subset I$. We must prove $I \subset J$.

We will show that any element $P(X) \in I$ of degree n belongs to J by induction on n. The degree is the largest nonzero coefficient. In particular, the zero polynomial does not have a degree, but the zero polynomial is obviously in J.

There are two cases. In the first case, $n \geq N$. Then we write

$$P(X) = aX^n + \dots.$$

By definition $a \in I(n) = I(N)$ since the chain of ideals $I(n)$ stabilized. Thus we can write a in terms of the generators: $a = \sum a_{N,i}\lambda_i$ for some $\lambda_i \in R$. Define the polynomial

$$Q = \sum \lambda_i P_{N,i} x^{n-N} \in J.$$

Then Q has degree n and the leading term is just a. In particular,

$$P - Q$$

is in I and has degree less than n. By the inductive hypothesis, this belongs to J, and since $Q \in J$, it follows that $P \in J$.

Now consider the case of $n < N$. Again, we write $P(X) = aX^n + \dots.$ Then $a \in I(n)$. We can write

$$a = \sum a_{n,i}\lambda_i, \quad \lambda_i \in R.$$

But the $a_{n,i} \in I(n)$. The polynomial

$$Q = \sum \lambda_i P_{n,i}$$

belongs to J since $n < N$. In the same way, $P - Q \in I$ has a lower degree. Induction as before implies that $P \in J$. ▲

15.9 Example. Let k be a field. Then $k[x_1, \dots, x_n]$ is noetherian for any n, by the Hilbert basis theorem and induction on n.

15.10 Example. Any finitely generated commutative ring R is noetherian. Indeed, then there is a surjection

$$\mathbb{Z}[x_1, \dots, x_n] \twoheadrightarrow R$$

where the x_i get mapped onto generators in R. The former is noetherian by the basis theorem, and R is as a quotient noetherian.

15.11 Corollary. *Any ring R can be obtained as a filtered direct limit of noetherian rings.*

Proof. Indeed, R is the filtered direct limit of its finitely generated subrings. ▲

This observation is sometimes useful in commutative algebra and algebraic geometry, in order to reduce questions about arbitrary commutative rings to noetherian rings. Noetherian rings have strong finiteness hypotheses that let you get numerical invariants that may be useful. For instance, we can do things like inducting on the dimension for noetherian local rings.

15.12 Example. Take $R = \mathbb{C}[x_1, \dots, x_n]$. For any algebraic variety V defined by polynomial equations, we know that V is the vanishing locus of some ideal $I \subset R$. Using the Hilbert basis theorem, we have shown that I is finitely generated. This implies that V can be described by *finitely* many polynomial equations.

Lecture 16
10/1

§1 More on noetherian rings

Let R be a noetherian ring.

16.1 Proposition. *An R-module M is noetherian if and only if M is finitely generated.*

Proof. The only if direction is obvious. A module is noetherian if and only if every submodule is finitely generated.

For the if direction, if M is finitely generated, then there is a surjection of R-modules

$$R^n \to M$$

where R is noetherian. So R^n is noetherian because it is a successive extension of copies of R and an extension of two noetherian modules is also noetherian. So M is a quotient of a noetherian module and is noetherian.

▲

Today, we will continue with the structure theory for noetherian modules.

The first piece of intuition to have is the following. Let R be noetherian; consider Spec$R$. An R-module M is supposed to be thought of as somehow spread out over Spec$R$. If $\mathfrak{p} \in \mathrm{Spec}R$, then

$$\kappa(\mathfrak{p}) = \text{fr. field } R/\mathfrak{p}$$

which is the residue field of $R_{\mathfrak{p}}$. If M is any R-module, we can consider $M \otimes_R \kappa(\mathfrak{p})$ for each $\mathfrak{p}$; it is a vector space over $\kappa(\mathfrak{p})$. If M is finitely generated, then $M \otimes_R \kappa(\mathfrak{p})$ is a finite-dimensional vector space.

16.2 Definition. Let M be a finitely generated R-module. Then supp$M$ is defined to be the set of primes $\mathfrak{p} \in \mathrm{Spec}R$ such that

$$M \otimes_R \kappa(\mathfrak{p}) \neq 0.$$

You're supposed to think of a module M as something like a vector bundle over Spec$R$. At each $\mathfrak{p} \in \mathrm{Spec}R$, we associate the vector space $M \otimes_R \kappa(\mathfrak{p})$. It's not really a vector bundle, since the fibers don't have to have the same dimension. For instance, the support of the $\mathbb{Z}$-module $\mathbb{Z}/p$ just consists of the prime (p). The fibers don't have the same dimension.

Nonetheless, we can talk about the support, i.e. the set of spaces where the vector space is not zero.

Remark. $\mathfrak{p} \in \mathrm{supp}M$ if and only if $M_{\mathfrak{p}} \neq 0$. This is because

$$(M \otimes_R R_{\mathfrak{p}})/\mathfrak{p}R_{\mathfrak{p}}(M \otimes_R R_{\mathfrak{p}}) = M_{\mathfrak{p}} \otimes_{R_{\mathfrak{p}}} \kappa(\mathfrak{p})$$

and we can use Nakayama's lemma over the local ring $R_{\mathfrak{p}}$. (We are using the fact that M is finitely generated.)

Remark. $M = 0$ if and only if supp$M = \emptyset$. This is because $M = 0$ if and only if $M_{\mathfrak{p}} = 0$ for all localizations. We saw this earlier.

We will see soon that that supp$M$ is closed in Spec$R$. You imagine that M lives on this closed subset supp$M$, in some sense.

§2 Associated primes

Throughout, R is noetherian.

16.3 Definition. Let M be a finitely generated R-module. The prime ideal $\mathfrak{p}$ is said to be **associated** to M if there exists an element $x \in M$ such that $\mathfrak{p}$ is the annihilator of x. The set of associated primes is $\mathrm{Ass}(M)$.

Note that the annihilator of an element $x \in M$ is not necessarily prime, but it is possible that the annihilator might be prime, in which case it is associated.

The first claim is that there are some.

16.4 Proposition. *If $M \neq 0$, then there is an associated prime.*

Proof. Let I be a maximal element among the annihilators of nonzero elements $x \in M$. Then $1 \notin I$ because the annihilator of a nonzero element is not the full ring. The existence of I is guaranteed thanks to the noetherianness of R.[11]

So I is the annihilator $\mathrm{Ann}(x)$ of some $x \in M - \{0\}$. I claim that I is prime, hence an associated prime. Indeed, suppose $ab \in I$ where $a, b \in R$. This means that

$$(ab)x \neq 0.$$

Consider the annihilator of bx. This contains the annihilator of x, so I; it also contains a. Maximality tells us that either $bx = 0$ (in which case $b \in I$) or $\mathrm{Ann}(bx) = I$ and then $a \in \mathrm{Ann}(bx) = I$. So either $a, b \in I$. And I is prime. ▲

16.5 Proposition. *Any finitely generated R-module has only finitely many associated primes.*

The idea is going to be to use the fact that M is finitely generated to build M out of finitely many pieces, and use that to bound the number of associated primes to each piece.

16.6 Lemma. *Suppose we have an exact sequence of finitely generated R-modules*

$$0 \to M' \to M \to M'' \to 0.$$

Then

$$\mathrm{Ass}(M') \subset \mathrm{Ass}(M) \subset \mathrm{Ass}(M') \cup \mathrm{Ass}(M'')$$

Proof. The first claim is obvious. If $\mathfrak{p}$ is the annihilator of something in M', it is an annihilator of something in M (namely its image), because $M' \to M$ is injective.

The hard direction is the other direction. Suppose $\mathfrak{p} \in \mathrm{Ass}(M)$. Then there is $x \in M$ such that

$$\mathfrak{p} = \mathrm{Ann}(x).$$

Consider the submodule $Rx \subset M$. If $Rx \cap M' \neq 0$, then we can choose $y \in Rx \cap M' - \{0\}$. I claim that $\mathrm{Ann}(y) = \mathfrak{p}$ and so $\mathfrak{p} \in \mathrm{Ass}(M')$.

[11] It is a well-known argument that in a noetherian ring, any subset of ideals contains a maximal element.

Now $y = ax$ for some $a \in R$. The annihilator of y is the set of elements $b \in R$ such that

$$abx = 0$$

or $ab \in \mathfrak{p}$. But $y = ax \neq 0$, so $a \notin \mathfrak{p}$. As a result, the condition $b \in \mathrm{Ann}(y)$ is the same as $b \in \mathfrak{p}$. In other words,

$$\mathrm{Ann}(y) = \mathfrak{p}$$

which proves the claim.

What if the intersection $Rx \cap M' = 0$. Let $\phi : M \twoheadrightarrow M''$ be the surjection. I claim that $\mathfrak{p} = \mathrm{Ann}(\phi(x))$ and $\mathfrak{p} \in \mathrm{Ass}(M'')$. The proof is as follows. Clearly $\mathfrak{p}$ annihilates $\phi(x)$ as it annihilates x. Suppose $a \in \mathrm{Ann}(\phi(x))$. This means that $\phi(ax) = 0$, so $ax \in \ker \phi$; but $\ker \phi \cap Rx = 0$. So $ax = 0$ and $a \in \mathfrak{p}$. So $\mathrm{Ann}(\phi(x)) = \mathfrak{p}$. ▲

16.7 Lemma. *For any finitely generated R-module M, there exists a finite filtration*

$$0 = M_0 \subset M_1 \subset \cdots \subset M_k = M$$

such that the quotients are isomorphic to various $R/\mathfrak{p}_i$.

Proof. Let $M' \subset M$ be maximal among submodules for which such a filtration exists. What we'd like to show is that $M' = M$, but a priori we don't know this. Now M' is well-defined since 0 has a filtration and M is noetherian. There is a filtration

$$0 = M_0 \subset M_1 \subset \cdots \subset M_l = M' \subset M.$$

Now what can we say? If $M' = M$, we're done, as we said. Otherwise, look at the quotient $M/M' \neq 0$. There is an associated prime of M/M'. So there is a prime $\mathfrak{p}$ which is the annihilator of $x \in M/M'$. This means that there is an injection

$$R/\mathfrak{p} \to M/M'.$$

Now, we just make M' bigger by taking M_{l+1} as the inverse image in M of $R/\mathfrak{p} \subset M/M'$. We have thus extended this filtration one step further since $M_{l+1}/M_l \simeq R/\mathfrak{p}$, a contradiction since M' was maximal. ▲

Now we are in a position to meet the goal.

Pf of Proposition 16.5. Suppose M is finitely generated Take our filtration

$$0 = M_0 \subset M_1 \subset \cdots \subset M_k = M.$$

By induction, we show that $\mathrm{Ass}(M_i)$ is finite for each i. It is obviously true for $i = 0$. In general, we have an exact sequence

$$0 \to M_i \to M_{i+1} \to R/\mathfrak{p}_i \to 0$$

which implies that

$$\mathrm{Ass}(M_{i+1}) \subset \mathrm{Ass}(M_i) \cup \mathrm{Ass}(R/\mathfrak{p}_i) = \mathrm{Ass}(M_i) \cup \{\mathfrak{p}_i\}.$$

This proves the claim and the proposition; it also shows that the number of associated primes is at most the length of the filtration.

▲

Let us first describe how associated primes localize.

16.8 Proposition. *Let R noetherian, M finitely generated and $S \subset R$ multiplicatively closed. Then*

$$\mathrm{Ass}(S^{-1}M) = \left\{S^{-1}\mathfrak{p} : \mathfrak{p} \in \mathrm{Ass}(M), \mathfrak{p} \cap S = \emptyset\right\}.$$

Here $S^{-1}M$ is considered as an $S^{-1}R$-module.

We've seen that prime ideals in $S^{-1}R$ can be identified as a subset of Spec$R$. This shows that this notion is compatible with localization.

Proof. We prove the easy direction. Suppose $\mathfrak{p} \in \mathrm{Ass}(M)$ and $\mathfrak{p} \cap S = \emptyset$. Then $\mathfrak{p} = \mathrm{Ann}(x)$ for some $x \in M$. Then the annihilator of $x/1$ is just $S^{-1}\mathfrak{p}$, as one easily sees. Thus $S^{-1}\mathfrak{p} \in \mathrm{Ass}(S^{-1}M)$.

The harder direction is left as an exercise. ▲

The next claim is that the support and the associated primes are related.

16.9 Proposition. *The support is the closure of the associated primes:*

$$\mathrm{supp}M = \bigcup_{\mathfrak{q} \in \mathrm{Ass}(M)} \overline{\{\mathfrak{q}\}}$$

16.10 Corollary. supp(M) *is closed.*

Proof. Indeed, the above result says that

$$\mathrm{supp}M = \bigcup_{\mathfrak{q} \in \mathrm{Ass}(M)} \overline{\{\mathfrak{q}\}}.$$

▲

16.11 Corollary. *The ring R has finitely many minimal prime ideals.*

Proof. Indeed, every minimal prime ideal is an associated prime for the R-module R itself. Why is this? Well, supp$R$ = Spec$R$. Thus every prime ideal of R contains an associated prime. And R has finitely many associated primes. ▲

Remark. So Spec$R$ is the finite union of irreducible pieces $\overline{\mathfrak{q}}$ if R is noetherian.

Let us prove the proposition.

Proof. First, the easy direction. We show that supp(M) contains the set of primes $\mathfrak{p}$ containing an associated prime. So let $\mathfrak{q}$ be an associated prime and $\mathfrak{p} \supset \mathfrak{q}$. We show that

$$\mathfrak{p} \in \mathrm{supp}M, \ \textit{i.e.}\ M_{\mathfrak{p}} \neq 0.$$

But there is an injective map

$$R/\mathfrak{q} \to M$$

so an injective map

$$(R/\mathfrak{q})_{\mathfrak{p}} \to M_{\mathfrak{p}}$$

where the first thing is nonzero since nothing nonzero in $R/\mathfrak{q}$ can be annihilated by something not in $\mathfrak{p}$. So $M_{\mathfrak{p}} \neq 0$.

The hard direction is the converse. Say that $\mathfrak{p} \in \mathrm{supp} M$. We have to show that $\mathfrak{p}$ contains an associated prime. Now $M_{\mathfrak{p}} \neq 0$ and it is a finitely generated $R_{\mathfrak{p}}$-module, where $R_{\mathfrak{p}}$ is noetherian. So this has an associated prime.

$$\mathrm{Ass}(M_{\mathfrak{p}}) \neq \emptyset$$

and we can find an element $\mathfrak{q}_{\mathfrak{p}} \subset R_{\mathfrak{p}}$ in there, where $\mathfrak{q}$ is a prime of R contained in $\mathfrak{p}$. But by the above fact about localization and associated primes, we have that

$$\mathfrak{q} \in \mathrm{Ass}(M)$$

and we have already seen that $\mathfrak{q} \subset \mathfrak{p}$. This proves the other inclusion and establishes the result. ▲

We have just seen that $\mathrm{supp} M$ is a closed subset of $\mathrm{Spec} R$ and is a union of finitely many irreducible subsets. More precisely,

$$\mathrm{supp} M = \bigcup_{\mathfrak{q} \in \mathrm{Ass}(M)} \overline{\{\mathfrak{q}\}}$$

though there might be some redundancy in this expression. Some associated prime might be contained in others.

16.12 Definition. A prime $\mathfrak{p} \in \mathrm{Ass}(M)$ is an **isolated** associated prime of M if it is minimal (with respect to the ordering on $\mathrm{Ass}(M)$); it is **embedded** otherwise.

So the embedded primes are not needed to describe the support of M.

§3 The case of one associated prime

16.13 Proposition. *Let M be a finitely generated R-module. Then*

$$\mathrm{supp} M = \{\mathfrak{p} \in \mathrm{Spec} R : \mathfrak{p} \text{ contains an associated prime}\}.$$

16.14 Definition. A finitely generated R-module M is **$\mathfrak{p}$-primary** if

$$\mathrm{Ass}(M) = \{\mathfrak{p}\}.$$

If $\mathrm{Ass}(M)$ consists of a point, we call M **primary**.

Lecture 17
10/4

For the remainder of this lecture, R is a noetherian ring, and M a finitely generated R-module. $S \subset R$ is a multiplicatively closed subset.

§1 A loose end

Let us start with an assertion we made last time, but we didn't prove. Namely, that

$$\mathrm{Ass}(S^{-1}M) = \left\{S^{-1}\mathfrak{p}, \mathfrak{p} \in \mathrm{Ass}(M), \mathfrak{p} \cap S = \emptyset\right\}.$$

We proved the easy direction, that if $\mathfrak{p} \in \mathrm{Ass}(M)$ and does not intersect S, then $S^{-1}\mathfrak{p}$ is an associated prime of $S^{-1}M$.

17.1 Proposition. *The reverse inclusion also holds.*

Proof. Let $\mathfrak{q} \in \mathrm{Ass}(S^{-1}M)$. This means that $\mathfrak{q} = \mathrm{Ann}(x/s)$ for some $x \in M$, $s \in S$.

Call the map $R \to S^{-1}R$ to be ϕ. Then $\phi^{-1}(\mathfrak{q})$ is the set of elements $a \in R$ such that

$$\frac{ax}{s} = 0 \in S^{-1}M.$$

In other words, by definition of the localization, this is

$$\bigcup_{t \in S} \{a \in R : atx = 0 \in M\} = \bigcup \mathrm{Ann}(tx) \subset R.$$

We know, however, that among elements of the form $\mathrm{Ann}(tx)$, there is a *maximal* element $I = \mathrm{Ann}(t_0x)$ for some $t_0 \in S$. Indeed, R is noetherian. Then if you think about any other annihilator $I' = \mathrm{Ann}(tx)$, then I', I are both contained in $\mathrm{Ann}(t_0tx)$. However,

$$I \subset \mathrm{Ann}(t_0x)$$

and I is maximal, so $I = \mathrm{Ann}(t_0tx)$ and

$$I' \subset I.$$

That is I contains all these other annihilators. In particular, the big union above, i.e. $\phi^{-1}(\mathfrak{q})$, is just

$$I = \mathrm{Ann}(t_0x).$$

It follows that $\phi^{-1}(\mathfrak{q})$ is the annihilator of $\mathrm{Ann}(t_0x)$, so this is an associated prime of M. This means that every associated prime of $S^{-1}M$ comes from an associated prime of M. That completes the proof. ▲

§2 Primary modules

17.2 Definition. Let $\mathfrak{p} \subset R$ be prime, M a finitely generated R-module. Then M is **$\mathfrak{p}$-primary** if

$$\mathrm{Ass}(M) = \{\mathfrak{p}\}.$$

Let's say that the zero module is not primary.

A module is **primary** if it is $\mathfrak{p}$-primary for some $\mathfrak{p}$, i.e. has precisely one associated prime.

17.3 Proposition. *Let M be a finitely generated R-module. Then M is $\mathfrak{p}$-primary if and only if, for every $m \in M - \{0\}$, the annihilator $\mathrm{Ann}(m)$ has radical $\mathfrak{p}$.*

Proof. We first need a small observation.

17.4 Lemma. *If M is $\mathfrak{p}$-primary, so is any nonzero submodule of M is $\mathfrak{p}$-primary.*

Proof. Indeed, any associated prime of the submodule is an associated prime of M. Note that the submodule, if it is nonzero, it has an associated prime. That has to be $\mathfrak{p}$. ▲

Assume first M to be $\mathfrak{p}$-primary. Let $x \in M$, $x \neq 0$. Let $I = \mathrm{Ann}(x)$. So by definition there is an injection

$$R/I \to M$$

sending $1 \to x$. As a result, R/I is $\mathfrak{p}$-primary by the above lemma. We want to know that $\mathfrak{p} = \mathrm{Rad}(I)$. We saw that the support $\mathrm{supp} R/I = \{\mathfrak{q} : \mathfrak{q} \supset I\}$ is the union of the closures of the associated primes. In this case,

$$\mathrm{supp}(R/I) = \{\mathfrak{q} : \mathfrak{q} \supset \mathfrak{p}\}.$$

But we know that $\mathrm{Rad}(I) = \bigcap_{\mathfrak{q} \supset I} \mathfrak{q}$, which by the above is just $\mathfrak{p}$. This proves that $\mathrm{Rad}(I) = \mathfrak{p}$. We have shown that if R/I is primary, then I has radical $\mathfrak{p}$.

The converse is easy. Suppose the condition holds and $\mathfrak{q} \in \mathrm{Ass}(M)$, so $\mathfrak{q} = \mathrm{Ann}(x)$ for $x \neq 0$. But then $\mathrm{Rad}(\mathfrak{q}) = \mathfrak{p}$, so

$$\mathfrak{q} = \mathfrak{p}$$

and $\mathrm{Ass}(M) = \{\mathfrak{p}\}$. ▲

We have another characterization.

17.5 Proposition. *Let $M \neq 0$ be a finitely generated R-module. Then M is primary iff for each $a \in R$, either multiplication $a : M \to M$ is injective or nilpotent.*

Proof. Suppose M to be $\mathfrak{p}$-primary. Then multiplication by anything in $\mathfrak{p}$ is nilpotent because the annihilator of everything nonzero has radical $\mathfrak{p}$. But if $a \notin \mathfrak{p}$, then $\mathrm{Ann}(x)$ for $x \in M - \{0\}$ has radical $\mathfrak{p}$ and cannot contain a.

Other direction, now. Assume that every element of a acts either injectively or nilpotently on M. Let $I \subset R$ be the collection of elements $a \in R$ such that $a^n M = 0$ for n large. Then I is an ideal; it is closed under addition by the binomial formula. If $a, b \in I$ and a^n, b^n act by zero, then $(a+b)^{2n}$ acts by zero as well.

I claim that I is actually prime. If $a, b \notin I$, then a, b act by multiplication injectively on I. So $a : M \to M, b : M \to M$ are injective. However, a composition of injections is injective, so ab acts injectively and $ab \notin I$. So I is prime.

We need now to check that if $x \in M$ is nonzero, then $\mathrm{Ann}(x)$ has radical I. This is because something $a \in R$ has a power that kills x, multiplication $M \overset{a}{\to} M$ can't be injective, so it must be nilpotent. Conversely, if $a \in I$, then a power of a is nilpotent, so it must kill x. ▲

So we have this notion of a primary module. The idea is that all the torsion is somehow concentrated in some prime.

§3 Primary decomposition

This is the structure theorem for modules over a noetherian ring, in some sense.

17.6 Definition. Let M be a finitely generated R-module. A submodule $N \subset M$ is **$\mathfrak{p}$-coprimary** if M/N is $\mathfrak{p}$-primary.

Similarly, we can say that $N \subset M$ is **coprimary**.

17.7 Definition. $N \subsetneq M$ is **irreducible** if whenever $N = N_1 \cap N_2$ for $N_1, N_2 \subset M$, then either one of N_1, N_2 equals N. It is not nontrivially the intersection of larger submodules.

17.8 Proposition. *An irreducible submodule $N \subset M$ is coprimary.*

Proof. Say $a \in R$. We'd like to show that

$$M/N \overset{a}{\to} M/N$$

is either injective or nilpotent. Consider the following submodule of M/N:

$$K(n) = \{x \in M/N : a^n x = 0\}.$$

Then $K(0) \subset K(1) \subset \dots$; this chain stops by noetherianness as the quotient module is noetherian. In particular, $K(n) = K(2n)$ for large n.

In particular, if $x \in M/N$ is divisible by a^n (n large) and nonzero, then $a^n x$ is also nonzero. Indeed, say $x = a^n y$; then $y \notin K(n)$, so $a^n x = a^{2n} y \neq 0$ or we would have $y \in K(2n) = K(n)$. In M/N, the submodules

$$a^n(M/N) \cap \ker(a^n)$$

are equal to zero for large n. But our assumption was that N is irreducible. So one of these submodules of M/N is zero. I.e., either $a^n(M/N) = 0$ or $\ker a^n = 0$. We get either injectivity or nilpotence on M/N. This proves the result. ▲

17.9 Proposition. *M has an irreducible decomposition. There exist finitely many irreducible submodules $N_1, \dots, N_k$ with*

$$N_1 \cap \dots \cap N_k = 0.$$

In other words,

$$M \to \bigoplus M/N_i$$

is injective. So a finitely generated module over a noetherian ring can be imbedded in a direct sum of primary modules.

Proof. Let $M' \subset M$ be a maximal submodule of M such that M' cannot be written as an intersection of finitely many irreducible submodules. If no such M' exists, then we're done, because then 0 can be written as an intersection of finitely many irreducible submodules.

Now M' is not irreducible, or it would be the intersection of one irreducible submodule. Then M' can be written as $M_1' \cap M_2'$ for two strictly larger submodules of M. But M_1', M_2' admit decompositions as intersections of irreducibles. So M' does as well, contradiction. ▲

For any M, we have an **irreducible decomposition**

$$0 = \bigcap N_i$$

for the N_i a finite set of irreducible (and thus coprimary) submodules. This decomposition here is highly non-unique and non-canonical. Let's try to pare it down to something which is a lot more canonical.

The first claim is that we can collect together modules which are coprimary for some prime.

17.10 Lemma. *Let $N_1, N_2 \subset M$ be $\mathfrak{p}$-coprimary submodules. Then $N_1 \cap N_2$ is also $\mathfrak{p}$-coprimary.*

Proof. We have to show that $M/N_1 \cap N_2$ is $\mathfrak{p}$-primary. Indeed, we have an injection

$$M/N_1 \cap N_2 \rightarrowtail M/N_1 \oplus M/N_2$$

which implies that $\mathrm{Ass}(M/N_1 \cap N_2) \subset \mathrm{Ass}(M/N_1) \cup \mathrm{Ass}(M/N_2) = \{\mathfrak{p}\}$. So we're done. ▲

In particular, if we don't want irreducibility but only primariness in the decomposition

$$0 = \bigcap N_i,$$

we can assume that each N_i is $\mathfrak{p}_i$ coprimary for some prime $\mathfrak{p}_i$ with the $\mathfrak{p}_i$ distinct.

17.11 Definition. Such a decomposition of zero is called a **primary decomposition**.

We can further assume that

$$N_i \not\supset \bigcap_{j \neq i} N_j$$

or we could omit one of the N_i. Let's assume that the decomposition is minimal. Then the decomposition is called a **reduced primary decomposition**.

Again, what this tells us is that $M \rightarrowtail \bigoplus M/N_i$. What we have shown is that M can be imbedded in a sum of pieces, each of which is $\mathfrak{p}$-primary for some prime, and the different primes are distinct.

This is **not** unique. However,

17.12 Proposition. *The primes $\mathfrak{p}_i$ that appear in a reduced primary decomposition of zero are uniquely determined. They are the associated primes of M.*

Proof. All the associated primes of M have to be there, because we have the injection

$$M \rightarrowtail \bigoplus M/N_i$$

so the associated primes of M are among those of M/N_i (i.e. the $\mathfrak{p}_i$).

The hard direction is to see that each $\mathfrak{p}_i$ is an associated prime. I.e. if M/N_i is $\mathfrak{p}_i$-primary, then $\mathfrak{p}_i \in \mathrm{Ass}(M)$; we don't need to use primary modules except for primes in the associated primes. Here we need to use the fact that our decomposition has no redundancy. Without loss of generality, it suffices to show that $\mathfrak{p}_1$, for instance, belongs to $\mathrm{Ass}(M)$. We will use the fact that

$$N_1 \not\supset N_2 \cap \dots .$$

So this tells us that $N_2 \cap N_3 \cap \dots$ is not equal to zero, or we would have a containment. We have a map

$$N_2 \cap \dots \cap N_k \to M/N_1;$$

it is injective, since the kernel is $N_1 \cap N_2 \cap \dots \cap N_k = 0$ as this is a decomposition. However, M/N_1 is $\mathfrak{p}_1$-primary, so $N_2 \cap \dots \cap N_k$ is $\mathfrak{p}_1$-primary. In particular, $\mathfrak{p}_1$ is an associated prime of $N_2 \cap \dots \cap N_k$, hence of M. ▲

The primes are determined. The factors are not. However, in some cases they are.

17.13 Proposition. *Let $\mathfrak{p}_i$ be a minimal associated prime of M, i.e. not containing any smaller associated prime. Then the submodule N_i corresponding to $\mathfrak{p}_i$ in the reduced primary decomposition is uniquely determined: it is the kernel of*

$$M \to M_{\mathfrak{p}_i}.$$

Proof. We have that $\bigcap N_j = \{0\} \subset M$. When we localize at $\mathfrak{p}_i$, we find that

$$(\bigcap N_j)_{\mathfrak{p}_i} = \bigcap (N_j)_{\mathfrak{p}_i} = 0$$

as localization is an exact functor. If $j \neq i$, then M/N_j is $\mathfrak{p}_j$ primary, and has only $\mathfrak{p}_j$ as an associated prime. It follows that $(M/N_j)_{\mathfrak{p}_i}$ has no associated primes, since the only associated prime could be $\mathfrak{p}_j$, and that's not contained in $\mathfrak{p}_j$. In particular, $(N_j)_{\mathfrak{p}_i} = M_{\mathfrak{p}_i}$.

Thus, when we localize the primary decomposition at $\mathfrak{p}_i$, we get a trivial primary decomposition: most of the factors are the full $M_{\mathfrak{p}_i}$. It follows that $(N_i)_{\mathfrak{p}_i} = 0$. When we draw a commutative diagram

$$\begin{tikzcd}
N_i \arrow[r] \arrow[d] & (N_i)_{\mathfrak{p}_i} = 0 \arrow[d] \\
M \arrow[r] & M_{\mathfrak{p}_i}.
\end{tikzcd}$$

we find that N_i goes to zero in the localization.

Now if $x \in \ker(M \to M_{\mathfrak{p}_i}$, then $sx = 0$ for some $s \notin \mathfrak{p}_i$. When we take the map $M \to M/N_i$, sx maps to zero; but s acts injectively on M/N_i, so x maps to zero in M/N_i, i.e. is zero in N_i. ▲

This has been abstract, so:

17.14 Example. Let $R = \mathbb{Z}$. Let $M = \mathbb{Z} \oplus \mathbb{Z}/p$. Then zero can be written as

$$\mathbb{Z} \cap \mathbb{Z}/p$$

as submodules of M. But $\mathbb{Z}$ is $\mathfrak{p}$-coprimary, while $\mathbb{Z}/p$ is (0)-coprimary.

This is not unique. We could have considered

$$\{(n,n), n \in \mathbb{Z}\} \subset M.$$

However, the zero-coprimary part has to be the p-torsion. This is because (0) is the minimal ideal.

The decomposition is always unique, in general, if we have no inclusions among the prime ideals. For $\mathbb{Z}$-modules, this means that primary decomposition is unique for torsion modules. Any torsion group is a direct sum of the p-power torsion over all primes p.

Lecture 18
10/6

Today, we will talk about unique factorization.

§1 Unique factorization

Let R be a domain.

18.1 Definition. A nonzero element $x \in R$ is **prime** if (x) is a prime ideal.

In other words, x is not a unit, and if $x \mid ab$, then either $x \mid a$ or $x \mid b$.

18.2 Definition. A domain R is **factorial** if every nonzero noninvertible element $x \in R$ factors as a product $x_1 \dots x_n$ where each x_i is prime.

A simple observation:

18.3 Proposition. *This factorization is essentially unique, that is up to multiplication by units.*

Proof. Let $x \in R$ be a nonunit. Say $x = x_1 \dots x_n = y_1 \dots y_m$ were two different prime factorizations. Then $m, n > 0$.

We have that $x_1 \mid y_1 \dots y_m$, so $x_1 \mid y_i$ for some i. But y_i is prime. So x_1 and y_i differ by a unit. By removing each of these, we can get a smaller set of nonunique factorizations. Namely, we find that

$$x_2 \dots x_n = y_1 \dots \hat{y_i} \dots y_m$$

and then we can induct on the number of factors. ▲

The motivating example is of course:

18.4 Example. $\mathbb{Z}$ is factorial. This is the fundamental theorem of arithmetic.

§2 A ring-theoretic criterion

18.5 Definition. Let R be a domain. A prime ideal $\mathfrak{p} \subset R$ is said to be of **height one** if $\mathfrak{p}$ is minimal among ideals containing x for some nonzero $x \in R$.

So a prime of height one is not the zero prime, but it is as close to zero as possible, in some sense. When we later talk about dimension theory, we will talk about primes of any height. In a sense, $\mathfrak{p}$ is "almost" generated by one element.

18.6 Theorem. *Let R be a noetherian domain. The following are equivalent:*

1. *R is factorial.*
2. *Every height one prime is principal.*

Proof. Let's first show 1) implies 2). Assume R is factorial and $\mathfrak{p}$ is height one, minimal containing (x) for some $x \neq 0 \in R$. Then x is a nonunit, and it is nonzero, so it has a prime factorization

$$x = x_1 \dots x_n, \quad \text{each } x_i \text{ prime.}$$

Some $x_i \in \mathfrak{p}$ because $\mathfrak{p}$ is prime. In particular,

$$\mathfrak{p} \supset (x_i) \supset (x).$$

But (x_i) is prime itself, and it contains (x). The minimality of $\mathfrak{p}$ says that $\mathfrak{p} = (x_i)$.

Conversely, suppose every height one prime is principal. Let $x \in R$ be nonzero and a nonunit. We want to factor x as a product of primes. Consider the ideal $(x) \subsetneq R$. As a result, (x) is contained in a prime ideal. Since R is noetherian, there is a minimal prime ideal $\mathfrak{p}$ containing (x). Then $\mathfrak{p}$, being a height one prime, is principal—say $\mathfrak{p} = (x_1)$. It follows that $x_1 \mid x$ and x_1 is prime. Say

$$x = x_1 x_1'.$$

If x_1' is a nonunit, repeat this process to get $x_1' = x_2 x_2'$ with x_2 a prime element. Keep going; inductively we have

$$x_k = x_{k+1} x_{k+1}'.$$

If this process stops, with one of the x_k' a unit, we get a prime factorization of x. Suppose the process continues forever. Then we would have

$$(x) \subsetneq (x_1') \subsetneq (x_2') \subsetneq (x_3') \subsetneq \dots,$$

which is impossible by noetherianness. ▲

We have seen that unique factorization can be formulated in terms of prime ideals.

§3 Locally factorial domains

18.7 Definition. A noetherian domain R is said to be **locally factorial** if $R_{\mathfrak{p}}$ is factorial for each $\mathfrak{p}$ prime.

18.8 Example. The coordinate ring $\mathbb{C}[x_1, \dots, x_n/I$ of an algebraic variety is locally factorial if the variety is smooth. We may talk about this later.

18.9 Example (Nonexample)**.** Let R be $\mathbb{C}[A, B, C, D]/(AD - BC)$. The spectrum of R has maximal ideals consisting of 2-by-2 matrices of determinant zero. This variety is very singular at the origin. It is not even locally factorial at the origin.

The failure of unique factorization comes from the fact that

$$AD = BC$$

in this ring R. This is a protypical example of a ring without unique factorization. The reason has to do with the fact that the variety has a singularity at the origin.

§4 The Picard group

18.10 Definition. Let R be a commutative ring. An R-module I is **invertible** if there exists J such that

$$I \otimes_R J \simeq R.$$

Invertibility is with respect to the tensor product.

Remark. You're supposed to think of a module as giving something like a vector bundle on Spec$R$. An invertible module looks like a line bundle on Spec$R$.

There are many equivalent characterizations.

18.11 Proposition. *Let R be a ring, I an R-module. TFAE:*

1. *I is invertible.*
2. *I is finitely generated and $I_{\mathfrak{p}} \simeq R_{\mathfrak{p}}$ for all primes $\mathfrak{p} \subset R$.*
3. *I is finitely generated and there exist $a_1, \dots, a_n \in R$ which generate (1) in R such that*
$$I[a_i^{-1}] \simeq R[a_i^{-1}].$$

Proof. First, we show that if I is invertible, then I is finitely generated Suppose $I \otimes_R J \simeq R$. This means that $1 \in R$ corresponds to an element

$$\sum i_k \otimes j_k \in I \otimes_R J.$$

Thus, there exists a finitely generated submodule $I_0 \subset I$ such that the map $I_0 \otimes J \to I \otimes J$ is surjective. Tensor this with I, so we get a surjection

$$I_0 \simeq I_0 \otimes J \otimes I \to I \otimes J \otimes I \simeq I$$

which leads to a surjection $I_0 \twoheadrightarrow I$. This implies that I is finitely generated

We now show 1 implies 2. Note that if I is invertible, then $I \otimes_R R'$ is an invertible R' module for any R-algebra R'; to get an inverse, tensor the inverse of I with R'. In particular, $I_{\mathfrak{p}}$ is an invertible $R_{\mathfrak{p}}$-module for each $\mathfrak{p}$. As a result,

$$I_{\mathfrak{p}}/\mathfrak{p}I_{\mathfrak{p}}$$

is invertible over $R_{\mathfrak{p}}/\mathfrak{p}R_{\mathfrak{p}}$. This means that $I_{\mathfrak{p}}/\mathfrak{p}I_{\mathfrak{p}}$ is a one-dimensional vector space over the residue field. (The invertible modules over a vector space are the one-dimensional spaces.) Choose an element $x \in I_{\mathfrak{p}}$ which generates $I_{\mathfrak{p}}/\mathfrak{p}I_{\mathfrak{p}}$. Since $I_{\mathfrak{p}}$ is finitely generated, this shows that x generates $I_{\mathfrak{p}}$.

We get a surjection $\alpha : R_{\mathfrak{p}} \twoheadrightarrow I_{\mathfrak{p}}$ carrying $1 \to x$. I claim that:

> This map is injective.

This will imply that $I_{\mathfrak{p}}$ is free of rank 1. Well, let J be an inverse of I in R-modules; the same argument provides a surjection $\beta : R_{\mathfrak{p}} \to J_{\mathfrak{p}}$. We get a map

$$R_{\mathfrak{p}} \overset{\alpha}{\twoheadrightarrow} I_{\mathfrak{p}} \overset{\beta'}{\twoheadrightarrow} R_{\mathfrak{p}}$$

(where $\beta = \beta \otimes 1_{I_{\mathfrak{p}}}$) whose composite must be multiplication by a unit, since the ring is local. Thus the composite is injective and α is injective.

Now we show 2 implies 3. Suppose I is finitely generated and $I_{\mathfrak{p}} \simeq R_{\mathfrak{p}}$ for all $\mathfrak{p}$. I claim that for each $\mathfrak{p}$, we can choose an element x of $I_{\mathfrak{p}}$ generating $I_{\mathfrak{p}}$. By multiplying by the denominator, we can assume that $x \in I$. Then if $\{x_1, \dots, x_n\} \subset I$ generates I, then we have equalities

$$s_i x_i = a_i x \in R$$

for some $s_i \notin \mathfrak{p}$ as x generates $I_{\mathfrak{p}}$. This means that x generates I after inverting the s_i. It follows that $I[1/a] = R[1/a]$ where $a = \prod s_i \notin \mathfrak{p}$. In particular, we find that there is an open covering $\{\mathrm{Spec} R[1/a_{\mathfrak{p}}]\}$ of $\mathrm{Spec} R$ (where $a_{\mathfrak{p}} \notin \mathfrak{p}$) on which I is isomorphic to R. To say that these cover $\mathrm{Spec} R$ is to say that the $a_{\mathfrak{p}}$ generate 1.

Finally, let's do the implication 3 implies 1. Assume that we have the situation of $I[1/a_i] \simeq R[1/a_i]$. We want to show that I is invertible. We start by showing that I is **finitely presented**. This means that there is an exact sequence

$$R^m \to R^n \to I \to 0,$$

i.e. I is the cokernel of a map between free modules of finite rank. To see this, first, we've assumed that I is finitely generated. So there is a surjection

$$R^n \twoheadrightarrow I$$

with a kernel $K \rightarrowtail R^n$. We must show that K is finitely generated. Localization is an exact functor, so $K[1/a_i]$ is the kernel of $R[1/a_i]^n \to I[1/a_i]$. However, we have an exact sequence

$$K[1/a_i] \rightarrowtail R[1/a_i]^n \twoheadrightarrow R[1/a_i]$$

by the assumed isomorphism $I[1/a_i] \simeq R[1/a_i]$. But since a free module is projective, this sequence splits and we find that $K[1/a_i]$ is finitely generated. If it's finitely generated, it's generated by finitely many elements in K. As a result, we find that there is a map

$$R^N \to K$$

such that the localization to Spec$R[1/a_i]$ is surjective. This implies by the homework that $R^N \to K$ is surjective.[12] Thus K is finitely generated.

In any case, we have shown that the module I is finitely presented. **Define** $J = \mathrm{Hom}_R(I, R)$ as the candidate for its dual. This construction is compatible with localization. We can choose a finite presentation $R^m \to R^n \to I \to 0$, which leads to a sequence

$$0 \to J \to \mathrm{Hom}(R^n, R) \to \mathrm{Hom}(R^m, R).$$

It follows that the formation of J commutes with localization. In particular, this argument shows that

$$J[1/a] = \mathrm{Hom}_{R[1/a]}(I[1/a], R[1/a]).$$

One can check this by using the description of J. By construction, there is a canonical map $I \otimes J \to R$. I claim that this map is invertible.

For the proof, we use the fact that one can check for an isomorphism locally. It suffices to show that

$$I[1/a] \otimes J[1/a] \to R[1/a]$$

is an isomorphism for some collection of a's that generate the unit ideal. However, we have $a_1, \dots, a_n$ that generate the unit ideal such that $I[1/a_i]$ is free of rank 1, hence so is $J[1/a_i]$. It thus follows that $I[1/a_i] \otimes J[1/a_i]$ is an isomorphism. ▲

18.12 Definition. Let R be a commutative ring. We define the **Picard group** Pic(R) to be the set of isomorphism classes of invertible R-modules. This is an abelian group under the tensor product; the identity element is given by R.

Next time, we will continue talking about the Picard group and how it controls the failure of unique factorization.

Lecture 19
10/8

Last time, for a commutative ring R, we defined the **Picard group** Pic(R) as the set of isomorphism classes of invertible R-modules. The group structure is given by the tensor product.

[12] To check that a map is surjective, just check at the localizations at any maximal ideal.

§1 Cartier divisors

Assume furthermore that R is a domain. We now introduce:

19.1 Definition. A **Cartier divisor** for R is a submodule $M \subset K(R)$ such that M is invertible.

In other words, a Cartier divisor is an invertible fractional ideal. Alternatively, it is an invertible R-module M with a nonzero map $M \to K(R)$. **Once this map is nonzero, it is automatically injective,** since injectivity can be checked at the localizations, and any module-homomorphism from a domain into its quotient field is either zero or injective (because it is multiplication by some element).

We now make this into a group.

19.2 Definition. Given $(M, a : M \hookrightarrow K(R))$ and $(N, b : N \hookrightarrow K(R))$, we define the sum to be

$$(M \otimes N, a \otimes b : M \otimes N \hookrightarrow K(R)).$$

The map $a \otimes b$ is nonzero, so by what was said above, it is an injection. Thus the Cartier divisors from an abelian group $\mathrm{Cart}(R)$.

By assumption, there is a homomorphism

$$\mathrm{Cart}(R) \to \mathrm{Pic}(R)$$

mapping $(M, M \hookrightarrow K(R)) \to M$.

19.3 Proposition. *The map* $\mathrm{Cart}(R) \to \mathrm{Pic}(R)$ *is surjective. In other words, any invertible R-module can be embedded in $K(R)$.*

Proof. Let M be an invertible R-module. Indeed, we know that $M_{(0)} = M \otimes_R K(R)$ is an invertible $K(R)$-module, so a one-dimensional vector space over $K(R)$. In particular, $M_{(0)} \simeq K(R)$. There is a nonzero homomorphic map

$$M \to M_{(0)} \simeq K(R),$$

which is automatically injective by the discussion above. ▲

What is the kernel of $\mathrm{Cart}(R) \to \mathrm{Pic}(R)$? This is the set of Cartier divisors which are isomorphic to R itself. In other words, it is the set of $(R, R \hookrightarrow K(R))$. This data is the same thing as the data of a nonzero element of $K(R)$. So the kernel of

$$\mathrm{Cart}(R) \to \mathrm{Pic}(R)$$

has kernel isomorphic to $K(R)^*$. We have a short exact sequence

$$K(R)^* \to \mathrm{Cart}(R) \to \mathrm{Pic}(R) \to 0.$$

§2 Weil divisors and Cartier divisors

Now, we want to assume $\mathrm{Cart}(R)$ if R is "good." The "goodness" in question is to assume that R is locally factorial, i.e. that $R_{\mathfrak{p}}$ is factorial for each $\mathfrak{p}$. This is true, for instance, if R is the coordinate ring of a smooth algebraic variety.

19.4 Proposition. *If R is locally factorial and noetherian, then the group $\mathrm{Cart}(R)$ is a free abelian group. The generators are in bijection with the height one primes of R.*

We start by discussing Weil divisors.

19.5 Definition. A **Weil divisor** for R is a formal linear combination $\sum n_i[\mathfrak{p}_i]$ where the $\mathfrak{p}_i$ range over height one primes of R. So the group of Weil divisors is the free abelian group on the height one primes of R. We denote this group by $\mathrm{Weil}(R)$.

Now assume that R is a locally factorial, noetherian domain. We shall produce an isomorphism

$$\mathrm{Weil}(R) \simeq \mathrm{Cart}(R)$$

that sends $[\mathfrak{p}_i]$ to that height one prime $\mathfrak{p}_i$ together with the imbedding $\mathfrak{p}_i \hookrightarrow R \to K(R)$.

We first check that this is well-defined. Since $\mathrm{Weil}(R)$ is free, all we have to do is check that each $\mathfrak{p}_i$ is a legitimate Cartier divisor. In other words, we need to show that:

19.6 Proposition. *If $\mathfrak{p} \subset R$ is a height one prime and R locally factorial, then $\mathfrak{p}$ is invertible.*

Proof. In the last lecture, we gave a criterion for invertibility: namely, being locally trivial. We have to show that for any prime $\mathfrak{q}$, we have that $\mathfrak{p}_{\mathfrak{q}}$ is isomorphic to $R_{\mathfrak{q}}$. If $\mathfrak{p} \not\subset \mathfrak{q}$, then $\mathfrak{p}_{\mathfrak{q}}$ is the entire ring $R_{\mathfrak{q}}$, so this is obvious. Conversely, suppose $\mathfrak{p} \subset \mathfrak{q}$. Then $\mathfrak{p}_{\mathfrak{q}}$ is a height one prime of $R_{\mathfrak{q}}$: it is minimal over some element in $R_{\mathfrak{q}}$.

Thus $\mathfrak{p}_{\mathfrak{q}}$ is principal, in particular free of rank one, since $R_{\mathfrak{q}}$ is factorial. We saw last time that being factorial is equivalent to the principalness of height one primes. ▲

We need to define the inverse map

$$\mathrm{Cart}(R) \to \mathrm{Weil}(R).$$

In order to do this, start with a Cartier divisor $(M, M \hookrightarrow K(R))$. We then have to describe which coefficient to assign a height one prime. To do this, we use a local criterion.

Let's first digress a bit. Consider a locally factorial domain R and a prime $\mathfrak{p}$ of height one. Then $R_{\mathfrak{p}}$ is factorial. In particular, its maximal ideal $\mathfrak{p}R_{\mathfrak{p}}$ is height one, so principal. It is the principal ideal generated by some $t \in R_{\mathfrak{p}}$. Now we show:

19.7 Proposition. *Every nonzero ideal in $R_{\mathfrak{p}}$ is of the form (t^n) for some unique $n \geq 0$.*

Proof. Let $I_0 \subset R_{\mathfrak{p}}$ be nonzero. If $I_0 = R_{\mathfrak{p}}$, then we're done—it's generated by t^0. Otherwise, $I_0 \subsetneq R_{\mathfrak{p}}$, so contained in $\mathfrak{p}R_{\mathfrak{p}} = (t)$. So let $I_1 = \{x \in R_{\mathfrak{p}} : tx \in I_0\}$. Thus

$$I_1 = t^{-1}I_0.$$

I claim now that $I_1 \neq I_0$, i.e. that there exists $x \in R_{\mathfrak{p}}$ such that $x \notin I_0$ but $tx \in I_0$. The proof comes from the theory of associated primes. Look at $R_{\mathfrak{p}}/I_0$; it has at least one associated prime as it is nonzero.

Since it is a torsion module, this associated prime must be $\mathfrak{p}R_{\mathfrak{p}}$ since the only primes in $R_{\mathfrak{p}}$ are (0) and (t), **which we have not yet shown**. So there exists an element in the quotient R/I_0 whose annihilator is precisely (t). Lifting this gives an element in R which when multiplied by (t) is in I_0 but which is not in I_0. So $I_0 \subsetneq I_1$.

Proceed as before now. Define $I_2 = \{x \in R_{\mathfrak{p}} : tx \in I_1\}$. This process must halt since we have assumed noetherianness. We must have $I_m = I_{m+1}$ for some m, which would imply that some $I_m = R_{\mathfrak{p}}$ by the above argument. It then follows that $I_0 = (t^m)$ since each I_i is just tI_{i+1}. ▲

We thus have a good structure theory for ideals in R localized at a height one prime. Let us make a more general claim.

19.8 Proposition. *Every nonzero finitely generated $R_{\mathfrak{p}}$-submodule of the fraction field $K(R)$ is of the form (t^n) for some $n \in \mathbb{Z}$.*

Proof. Say that $M \subset K(R)$ is such a submodule. Let $I = \{x \in R_{\mathfrak{p}}, xM \subset R_{\mathfrak{p}}\}$. Then $I \neq 0$ as M is finitely generated M is generated over $R_{\mathfrak{p}}$ by a finite number of fractions $a_i/b_i, b_i \in R$. Then the product $b = \prod b_i$ brings M into $R_{\mathfrak{p}}$.

We know that $I = (t^m)$ for some m. In particular, t^mM is an ideal in R. In particular,

$$t^mM = t^pR$$

for some p, in particular $M = t^{p-m}R$.

▲

Now let's go back to the main discussion. R is a noetherian locally factorial domain; we want to construct a map

$$\mathrm{Cart}(R) \to \mathrm{Weil}(R).$$

Given $(M, M \hookrightarrow K(R))$ with M invertible, we want to define a formal sum $\sum n_i[\mathfrak{p}_i]$. For every height one prime $\mathfrak{p}$, let us look at the local ring $R_{\mathfrak{p}}$ with maximal ideal generated by some $t_{\mathfrak{p}} \in R_{\mathfrak{p}}$. Now $M_{\mathfrak{p}} \subset K(R)$ is a finitely generated $R_{\mathfrak{p}}$-submodule, so generated by some $t_{\mathfrak{p}}^{n_{\mathfrak{p}}}$. So we map $(M, M \hookrightarrow K(R))$ to

$$\sum_{\mathfrak{p}} n_{\mathfrak{p}}[\mathfrak{p}].$$

First, we have to check that this is well-defined. In particular, we have to show:

19.9 Proposition. *For almost all height one $\mathfrak{p}$, we have $M_{\mathfrak{p}} = R_{\mathfrak{p}}$. In other words, the integers $n_{\mathfrak{p}}$ are almost all zero.*

Proof. We can always assume that M is actually an ideal. Indeed, choose $a \in R$ with $aM = I \subset R$. As Cartier divisors, we have $M = I - (a)$. If we prove the result for I and (a), then we will have proved it for M (note that the $n_{\mathfrak{p}}$'s are additive invariants[13]). So because of this additivity, it is sufficient to prove the proposition for actual (i.e. nonfractional) ideals.

Assume thus that $M \subset R$. All of these $n_{\mathfrak{p}}$ associated to M are at least zero because M is actually an ideal. What we want is that $n_{\mathfrak{p}} \leq 0$ for almost all $\mathfrak{p}$. In other words, we must show that

$$M_{\mathfrak{p}} \supset R_{\mathfrak{p}} \quad \text{almost all } \mathfrak{p}.$$

To do this, just choose any $x \in M - 0$. There are finitely many minimal primes containing (x) (by primary decomposition applied to $R/(x)$). Every other height one prime $\mathfrak{q}$ does not contain (x).[14] This states that $M_{\mathfrak{q}} \supset x/x = 1$, so $M_{\mathfrak{q}} \supset R_{\mathfrak{q}}$.

The key claim we've used in this proof is the following. If $\mathfrak{q}$ is a height one prime in a domain R containing some nonzero element (x), then $\mathfrak{q}$ is minimal among primes containing (x). In other words, we can test the height one condition at any nonzero element in that prime. Alternatively:

19.10 Lemma. *There are no nontrivial containments among height one primes.*

▲

Anyway, we have constructed maps between $\mathrm{Cart}(R)$ and $\mathrm{Weil}(R)$. The map $\mathrm{Cart}(R) \to \mathrm{Weil}(R)$ takes $M \to \sum n_{\mathfrak{p}}[\mathfrak{p}]$. The other map $\mathrm{Weil}(R) \to \mathrm{Cart}(R)$ takes $[\mathfrak{p}] \to \mathfrak{p} \subset K(R)$. The composition $\mathrm{Weil}(R) \to \mathrm{Weil}(R)$ is the identity. Why is that? Start with a prime $\mathfrak{p}$; that goes to the Cartier divisor $\mathfrak{p}$. Then we need to finitely generatedre the multiplicities at other height one primes. But if $\mathfrak{p}$ is height one and $\mathfrak{q}$ is a height one prime, then if $\mathfrak{p} \neq \mathfrak{q}$ the lack of nontrivial containment relations implies that the multiplicity of $\mathfrak{p}$ at $\mathfrak{q}$ is zero. We have shown that

$$\mathrm{Weil}(R) \to \mathrm{Cart}(R) \to \mathrm{Weil}(R)$$

is the identity.

Now we have to show that $\mathrm{Cart}(R) \to \mathrm{Weil}(R)$ is injective. Say we have a Cartier divisor $(M, M \hookrightarrow K(R))$ that maps to zero in $\mathrm{Weil}(R)$, i.e. all its multiplicities $n_{\mathfrak{p}}$ are zero at height one primes. We show that $M = R$.

First, assume $M \subset R$. It is sufficient to show that at any maximal ideal $\mathfrak{m} \subset R$, we have

$$M_{\mathfrak{m}} = R_{\mathfrak{m}}.$$

What can we say? Well, $M_{\mathfrak{m}}$ is principal as M is invertible, being a Cartier divisor. Let it be generated by $x \in R_{\mathfrak{m}}$; suppose x is a nonunit (or we're already done). But $R_{\mathfrak{m}}$ is factorial, so $x = x_1 \dots x_n$ for each x_i prime. If $n > 0$, then however M has nonzero multiplicity at the prime ideal $(x_i) \subset R_{\mathfrak{m}}$. This is a contradiction.

The general case of M not really a subset of R can be handled similarly: then the generating element x might lie in the fraction field. So x, if it is not a unit in R, is a

[13] To see this, localize at $\mathfrak{p}$—then if M is generated by t^a, N generated by t^b, then $M \otimes N$ is generated by t^{a+b}.

[14] Again, we're using something about height one primes not proved yet.

product of some primes in the numerator and some primes in the denominator. The nonzero primes that occur lead to nonzero multiplicities.

Lecture 20
10/13

§1 Recap and a loose end

Last time, it was claimed that if R is a locally factorial domain, and $\mathfrak{p} \subset R$ is of height one, then every prime ideal of $R_{\mathfrak{p}}$ is either maximal or zero. This follows from general dimension theory. This is equivalent to the following general claim about height one primes:

> There are no nontrivial inclusions among height one primes for R a locally factorial domain.

Proof. Suppose $\mathfrak{q} \subsetneq \mathfrak{p}$ is an inclusion of height one primes.

Replace R by $R_{\mathfrak{p}}$. Then R is local with some maximal ideal $\mathfrak{m}$, which is principal with some generator x. Then we have an inclusion

$$0 \subset \mathfrak{q} \subset \mathfrak{m}.$$

This inclusion is proper. However, $\mathfrak{q}$ is principal since it is height one in the factorial ring $R_{\mathfrak{p}}$. This cannot be since every element is a power of x times a unit. (Alright, this wasn't live TEXed well.) ▲

Last time, we were talking about Weil(R) and Cart(R) for R a locally factorial noetherian domain.

1. Weil(R) is free on the height one primes.

2. Cart(R) is the group of invertible submodules of $K(R)$.

We produced an isomorphism

$$\mathrm{Weil}(R) \simeq \mathrm{Cart}(R).$$

Remark. Geometrically, what is this? Suppose $R = \mathbb{C}[X_1, \dots, X_n]/I$ for some ideal I. Then the maximal ideals, or closed points in Spec$R$, are certain points in $\mathbb{C}^n$; they form an irreducible variety if R is a domain. The locally factorial condition is satisfied, for instance, if the variety is *smooth.* In this case, the Weil divisors correspond to sums of irreducible varieties of codimension one—which correspond to the primes of height one. The Weil divisors are free on the set of irreducible varieties of codimension one.

The Cartier divisors can be thought of as "linear combinations" of subvarieties which are locally defined by one equation. It is natural to assume that the condition of being defined by one equation corresponds to being codimension one. This is true by the condition of R locally factorial.

In general, we can always construct a map

$$\mathrm{Cart}(R) \to \mathrm{Weil}(R),$$

but it is not necessarily an isomorphism.

§2 Further remarks on Weil(R) and Cart(R)

Recall that the Cartier group fits in an exact sequence:

$$K(R)^* \to \mathrm{Cart}(R) \to \mathrm{Pic}(R) \to 0,$$

because every element of $\mathrm{Cart}(R)$ determines its isomorphism class, and every element of $K(R)^*$ determines a free module of rank one. Contrary to what was stated last time, it is **not true** that exactness holds on the right. In fact, the kernel is the group R^* of units of R. So the exact sequence runs

$$0 \to R^* \to K(R)^* \to \mathrm{Cart}(R) \to \mathrm{Pic}(R) \to 0.$$

This is true for *any* domain R. For R locally factorial and noetherian, we know that $\mathrm{Cart}(R) \simeq \mathrm{Weil}(R)$, though.

We can think of this as a generalization of unique factorization.

20.1 Proposition. *R is factorial if and only if R is locally factorial and* $\mathrm{Pic}(R) = 0$*.*

Proof. Assume R is locally factorial and $\mathrm{Pic}(R) = 0$. Then every prime ideal of height one (an element of $\mathrm{Weil}(R)$, hence of $\mathrm{Cart}(R)$) is principal, which implies that R is factorial. And conversely. ▲

In general, we can think of the exact sequence above as a form of unique factorization for a locally factorial domain: any invertible fractional ideal is a product of height one prime ideals.

Let us now give an example.

§3 Discrete valuation rings and Dedekind rings

20.2 Example. Let R be a noetherian local domain whose prime ideals are (0) and the maximal ideal $\mathfrak{m} \neq 0$. In this condition, I claim:

20.3 Proposition. *TFAE:*

1. *R is factorial.*

2. *$\mathfrak{m}$ is principal.*

3. *R is integrally closed.*

4. *R is a valuation ring with value group $\mathbb{Z}$.*

20.4 Definition. A ring satisfying these conditions is called a **discrete valuation ring** (**DVR**). A discrete valuation ring necessarily has only two prime ideals. In fact, a valuation ring with value group $\mathbb{Z}$ satisfies all the above conditions.

Proof. Suppose R is factorial. Then every prime ideal of height one is principal. But $\mathfrak{m}$ is the only prime that can be height one (it's minimal over any nonzero nonunit of R. Thus 1 implies 2, and similarly 2 implies 1.

1 implies 3 is true for any R: factorialness implies integrally closedness. This is either either homework on the problem set or an easy exercise one can do for yourself.

4 implies 2 because one chooses an element $x \in R$ such that the valuation of x is one. Then, it is easy to see that x generates $\mathfrak{m}$: if $y \in \mathfrak{m}$, then the valuation of y is at least one, so $y/x \in R$ and $y = (y/x)x \in (x)$.

The implication 2 implies 4 was essentially done last time. Suppose $\mathfrak{m}$ is principal, generated by t. Last time, we saw that *all* nonzero ideals of R have the form (t^n) for some $n > 0$. If $x \in R$, we define the valuation of x to be n if $(x) = (t^n)$. One can easily check that this is a valuation on R which extends to the quotient field by additivity.

The interesting part of the argument is the claim that 3 implies 2. Suppose R is integrally closed; I claim that $\mathfrak{m}$ is principal. Choose $x \in \mathfrak{m} - \{0\}$. If $(x) = \mathfrak{m}$, we're done. Otherwise, we can look at $\mathfrak{m}/(x) \neq 0$. We have a finitely generated module over a noetherian ring which is nonzero, so it has an associated prime. That associated prime is either zero or $\mathfrak{m}$. But 0 is not an associated prime because every element in the module is killed by x. So $\mathfrak{m}$ is an associated prime.

Thus, there is $y \in \mathfrak{m}$ such that $y \notin (x)$ and $\mathfrak{m}y \subset (x)$. In particular, $y/x \in K(R) - R$ but

$$(y/x)\mathfrak{m} \subset R.$$

There are two cases:

1. Suppose $(y/x)\mathfrak{m} = R$. Then we can write $\mathfrak{m} = R(x/y)$. So $\mathfrak{m}$ is principal. (This argument shows that $x/y \in R$.)

2. The other possibility is that $y/x\mathfrak{m} \subsetneq R$. In this case, this is an ideal, so

$$(y/x)\mathfrak{m} \subset \mathfrak{m}.$$

   In particular, multiplication by y/x carries $\mathfrak{m}$ to itself. So multiplication by y/x stabilizes the finitely generated module $\mathfrak{m}$. By the usual characteristic polynomial argument, we see that y/x is integral over R. In particular, $y/x \in R$, as R was integrally closed, a contradiction as $y \notin (x)$.

▲

We now introduce a closely related notion.

20.5 Definition. A **Dedekind ring** is a noetherian domain R such that

1. R is integrally closed.

2. Every nonzero prime ideal of R is maximal.

Remark. If R is Dedekind, then any nonzero element is height one. This is evident since every nonzero prime is maximal.

If R is Dedekind, then R is locally factorial. In fact, the localization of R at a nonzero prime $\mathfrak{p}$ is a DVR.

Proof. $R_{\mathfrak{p}}$ has precisely two prime ideals: (0) and $\mathfrak{p}R_{\mathfrak{p}}$. As a localization of an integrally closed domain, it is integrally closed. So $R_{\mathfrak{p}}$ is a DVR by the above result (hence factorial). ▲

Assume R is Dedekind now. We have an exact sequence

$$0 \to R^* \to K(R)^* \to \mathrm{Cart}(R) \to \mathrm{Pic}(R) \to 0.$$

Here $\mathrm{Cart}(R) \simeq \mathrm{Weil}(R)$. But $\mathrm{Weil}(R)$ is free on the nonzero primes, or equivalently maximal ideals, R being Dedekind. In fact, however, $\mathrm{Cart}(R)$ has a simpler description.

20.6 Proposition. *Suppose R is Dedekind. Then* $\mathrm{Cart}(R)$ *consists of all nonzero finitely generated submodules of $K(R)$ (i.e.* ***fractional ideals****).*

This is the same thing as saying as every nonzero finitely generated submodule of $K(R)$ is invertible.

Proof. Suppose $M \subset K(R)$ is nonzero and finitely generated It suffices to check that M is invertible after localizing at every prime, i.e. that $M_{\mathfrak{p}}$ is an invertible—or equivalently, trivial, $R_{\mathfrak{p}}$-module. At the zero prime, there is nothing to check. We might as well assume that $\mathfrak{p}$ is maximal. Then $R_{\mathfrak{p}}$ is a DVR and $M_{\mathfrak{p}}$ is a finitely generated submodule of $K(R_{\mathfrak{p}}) = K(R)$.

Let S be the set of integers n such that there exists $x \in M_{\mathfrak{p}}$ with $v(x) = n$, for v the valuation of $R_{\mathfrak{p}}$. By finite generation of M, S is bounded below. Thus S has a least element k. There is an element of $M_{\mathfrak{p}}$, call it x, with valuation k.

It is easy to check that $M_{\mathfrak{p}}$ is generated by x, and is in fact free with generator x. The reason is simply that x has the smallest valuation of anything in $M_{\mathfrak{p}}$. ▲

What's the upshot of this?

20.7 Theorem. *If R is a Dedekind ring, then any nonzero ideal $I \subset R$ is invertible, and therefore uniquely described as a product of powers of (nonzero) prime ideals, $I = \prod \mathfrak{p}_i^{n_i}$.*

Proof. This is simply because I is in $\mathrm{Cart}(R) = \mathrm{Weil}(R)$ by the above result. ▲

This is Dedekind's generalization of unique factorization.

We now give the standard examples:

20.8 Example.

1. Any PID is Dedekind.
2. If K is a finite extension of $\mathbb{Q}$, and set R to be the integral closure of $\mathbb{Z}$ in K, then R is a Dedekind ring. The ring of integers in any number field is a Dedekind ring.
3. If R is the coordinate ring of an algebraic variety which is smooth and irreducible of dimension one, then R is Dedekind.
4. Let X be a compact Riemann surface, and let $S \subset X$ be a nonempty finite subset. Then the ring of meromorphic functions on X with poles only in S is Dedekind. The maximal ideals in this ring are precisely those corresponding to points of $X - S$.

Lecture 21
10/15

Today, we want to start heading towards Serre's criterion for normality. The first we need to talk about is the theory of Artinian rings.

§1 Artinian rings

21.1 Definition. A commutative ring R is **Artinian** every descending chain of ideals $I_0 \supset I_1 \supset I_2 \supset \dots$ stabilizes.

Remark. The same definition makes sense for modules. We can define an R-module M to be **Artinian** if every descending chain of submodules stabilizes.

Remark. If $0 \to M' \to M \to M'' \to 0$ is an exact sequence, then M is Artinian iff M', M'' are. This is proved in the same way as for noetherianness.

This definition is obviously dual to the notion of noetherianness, but it is much more restrictive. Our first goal for today is to prove:

21.2 Theorem. *A commutative ring R is artinian iff:*

1. *R is noetherian.*
2. *Every prime ideal of R is maximal.*[15]

So artinian rings are very simple—small in some sense.

Proof. Let's warm up to this by first proving 2. Let R be artinian; we prove that:

21.3 Lemma. *Every prime $\mathfrak{p} \subset R$ is maximal.*

Proof. Indeed, $R/\mathfrak{p}$ is artinian. We want to show that this is a field, which is the same thing as saying that $\mathfrak{p}$ is maximal. Let $x \in R/\mathfrak{p}$ be nonzero. We have a descending chain

$$R/\mathfrak{p} \supset (x) \supset (x^2) \dots$$

which necessarily stabilizes. Then we have $(x^n) = (x^{n+1})$ for some n. In particular, we have $x^n = yx^{n+1}$ for some $y \in R/\mathfrak{p}$. But x is a nonzerodivisor, and we find

$$1 = xy$$

so x is invertible. Thus $R/\mathfrak{p}$ is a field. ▲

Next, we claim there aren't many primes:

21.4 Lemma. *If R is artinian, there are only finitely many maximal ideals.*

[15] This is much different from the Dedekind ring condition—there, zero is not maximal. An artinian domain is necessarily a field, in fact.

Proof. Assume otherwise. Then we have an infinite sequence

$$\mathfrak{m}_1, \dots, \mathfrak{m}_2, \dots$$

of distinct maximal ideals. Then we have the descending chain

$$R \supset \mathfrak{m}_1 \supset \mathfrak{m}_1 \cap \mathfrak{m}_2 \supset \dots .$$

This stabilizes. So for some n, we have that $\mathfrak{m}_1 \cap \dots \cap \mathfrak{m}_n \subset \mathfrak{m}_{n+1}$. However, this means that $\mathfrak{m}_{n+1}$ contains one of the $\mathfrak{m}_1, \dots, \mathfrak{m}_n$ since these are prime ideals (a familiar argument). Maximality and distinctness of the $\mathfrak{m}_i$ give a contradiction. ▲

In particular, we see that Spec$R$ for an artinian ring is just a finite set. In fact, since each point is closed, as each prime is maximal, the set has the *discrete topology.*

This means that R factors as a product of rings. Whenever Spec$R$ can be written as a disjoint union of components, you get a factoring of R into a product (this was on the homework). So $R = \prod R_i$ where each R_i has only one maximal ideal. We find, as a result,

21.5 Proposition. *Any artinian ring is a finite product of local artinian rings.*

Now, let us continue our analysis. We may as well assume that we are working with *local* artinian rings R in the future. In particular, R has a unique prime $\mathfrak{m}$, which must be the radical of R as the radical is the intersection of all primes. In particular, $\mathfrak{m}$ consists of nilpotent elements.

I claim now that:

21.6 Lemma. *Let $(R, \mathfrak{m})$ be a local artinian ring. Then $\mathfrak{m}$ is nilpotent. In particular, there is n such that $\mathfrak{m}^n = (0)$.*

Proof. We have the chain of ideals

$$\mathfrak{m} \supset \mathfrak{m}^2 \supset \dots ,$$

which stabilizes, so there is a large n with $\mathfrak{m}^n = \mathfrak{m}^{n+1} = \dots$. Let us call this stable ideal I. We want to show that $I = 0$.

Assume not. Consider all ideals J such that $IJ \neq 0$. This is nonempty (as $I = I(1) \neq 0$). There is a minimal such ideal J. That's what the condition of artinianness buys us—any nonempty collection of ideals in an artinian ring has a minimal element.

First, I claim that J is principal. Indeed, there is $x \in J$ with $xI \neq 0$; thus $(x)I \neq 0$, and minimality implies that $J = (x)$.

I now claim that $x \in \mathfrak{m}$. If otherwise, then x would be invertible, so $J = R$. In particular, no nontrivial ideals J satisfy $JI = 0$. But $\mathfrak{m}I = I$ by construction of I. So x is a nonunit.

Consider ideals I' such that $xI' \neq 0$. There is at least one, namely I. So there is a minimal one.

OK, we messed up. Let's assume this. ▲

Finally, we may prove:

21.7 Lemma. *A local artinian ring R is noetherian.*

Proof. We have the filtration $R \supset \mathfrak{m} \supset \mathfrak{m}^2 \supset \dots$. This eventually stabilizes at zero—that's the previous statement. I claim that R is noetherian as an R-module. To prove this, it suffices to show that $\mathfrak{m}^k/\mathfrak{m}^{k+1}$ is noetherian as an R-module. But of course, this is annihilated by $\mathfrak{m}$, so it is really a vector space over the field $R/\mathfrak{m}$. But $\mathfrak{m}^k/\mathfrak{m}^{k+1}$ is a subquotient of an artinian module so is artinian itself. We have to show that it is noetherian. It suffices to show now that if k is a field, and V a k-vector space, then TFAE:

1. V is artinian.
2. V is noetherian.
3. V is finite-dimensional.

This is evident by linear algebra. ▲

Now, finally, we have shown that an artinian ring is noetherian. We have to discuss the converse. Let us assume now that R is noetherian and has only maximal prime ideals. We show that R is artinian. Let us consider Spec$R$; there are only finitely many minimal primes by the theory of associated primes. Every prime ideal is minimal in this case. Once again, we learn that Spec$R$ is finite and has the discrete topology. This means that R is a product of factors $\prod R_i$ where each R_i is a local noetherian ring with a unique prime ideal. We might as well now prove:

21.8 Lemma. *Let $(R, \mathfrak{m})$ be a local noetherian ring with one prime ideal. Then R is artinian.*

Proof. We know that $\mathfrak{m} = \mathrm{rad}(R)$. So $\mathfrak{m}$ consists of nilpotent elements, so by finite generatedness it is nilpotent. Then we have a finite filtration

$$R \supset \mathfrak{m} \supset \dots \supset \mathfrak{m}^k = 0.$$

Each of the quotients are finite-dimensional vector spaces, so artinian—this implies that R itself is artinian.

▲

▲

The theory of artinian rings is thus a special case of the theory of noetherian rings.

§2 Reducedness

Recall:

21.9 Definition. A ring R is **reduced** if it has no nonzero nilpotents.

21.10 Proposition. *If R is noetherian, then R is reduced if and only if it satisfies the following conditions:*

1. *Every associated prime of R is minimal (no embedded primes).*
2. *If $\mathfrak{p}$ is minimal, then $R_{\mathfrak{p}}$ is a field.*

Proof. First, assume R reduced. What can we say? Say $\mathfrak{p}$ is a minimal prime; then $R_{\mathfrak{p}}$ has precisely one prime ideal (namely, $\mathfrak{m} = \mathfrak{p}R_{\mathfrak{p}}$). It is in fact a local artinian ring, though we don't need that fact. The radical of $R_{\mathfrak{p}}$ is just $\mathfrak{m}$. But R was reduced, so $R_{\mathfrak{p}}$ was reduced; it's an easy argument that localization preserves reducedness. So $\mathfrak{m} = 0$. The fact that 0 is a maximal ideal in $R_{\mathfrak{p}}$ says that it is a field.

On the other hand, we still have to do part 1. R is reduced, so $\mathrm{Rad}(R) = \bigcap_{\mathfrak{p} \in \mathrm{Spec} R} \mathfrak{p} = 0$. In particular,

$$\bigcap_{\mathfrak{p} \text{ minimal}} \mathfrak{p} = 0.$$

The map

$$R \to \prod_{\mathfrak{p} \text{ minimal}} R/\mathfrak{p}$$

is injective. The associated primes of the product, however, are just the minimal primes. So $\mathrm{Ass}(R)$ can contain only minimal primes.

That's one direction of the proposition. Let us prove the converse now. Assume R satisfies the two conditions listed. In other words, $\mathrm{Ass}(R)$ consists of minimal primes, and each $R_{\mathfrak{p}}$ for $\mathfrak{p} \in \mathrm{Ass}(R)$ is a field. We would like to show that R is reduced. Primary decomposition tells us that there is an injection

$$R \hookrightarrow \prod_{\mathfrak{p}_i \text{ minimal}} M_i, \quad M_i \ \ \mathfrak{p}_i - \text{primary}.$$

In this case, each M_i is primary with respect to a minimal prime. We have a map

$$R \hookrightarrow \prod M_i \to \prod (M_i)_{\mathfrak{p}_i},$$

which is injective, because when you localize a primary module at its associated prime, you don't kill anything by definition of primariness. Since we can draw a diagram

$$\begin{tikzcd}
R \arrow[r] \arrow[d] & \prod M_i \arrow[d] \\
\prod R_{\mathfrak{p}_i} \arrow[r] & \prod (M_i)_{\mathfrak{p}_i}
\end{tikzcd}$$

and the map $R \to \prod (M_i)_{\mathfrak{p}_i}$ is injective, the downward arrow on the right injective. Thus R can be embedded in a product of the fields $\prod R_{\mathfrak{p}_i}$, so is reduced. ▲

This proof actually shows:

21.11 Proposition (Scholism)**.** *A noetherian ring R is reduced iff it injects into a product of fields. We can take the fields to be the localizations at the minimal primes.*

21.12 Example. Let $R = k[X]$ be the coordinate ring of a variety X in $\mathbb{C}^n$. Assume X is reduced. Then $\mathrm{MaxSpec} R$ is a union of irreducible components X_i, which are the closures of the minimal primes of R. The fields you get by localizing at minimal primes depend only on the irreducible components, and in fact are the rings of meromorphic functions on X_i. Indeed, we have a map

$$k[X] \to \prod k[X_i] \to \prod k(X_i).$$

If we don't assume that R is radical, this is **not** true.

There is a stronger condition than being reduced we could impose. We could say:

21.13 Proposition. *If R is a noetherian ring, then R is a domain iff*

1. *R is reduced.*
2. *R has a unique minimal prime.*

Proof. One direction is obvious. A domain is reduced and (0) is the minimal prime.

The other direction is proved as follows. Assume 1 and 2. Let $\mathfrak{p}$ be the unique minimal prime of R. Then $\mathrm{Rad}(R) = 0 = \mathfrak{p}$ as every prime ideal contains $\mathfrak{p}$. As (0) is a prime ideal, R is a domain. ▲

We close by making some remarks about this embedding of R into a product of fields.

21.14 Definition. Let R be any ring, not necessarily a domain. Let $K(R)$ be the localized ring $S^{-1}R$ where S is the multiplicatively closed set of nonzerodivisors in R. $K(R)$ is called the **total ring of fractions** of R.

When R is a field, this is the quotient field.

First, to get a feeling for this, we show:

21.15 Proposition. *Let R be noetherian. The set of nonzerodivisors S can be described by $S = R - \bigcup_{\mathfrak{p} \in \mathrm{Ass}(R)} \mathfrak{p}$.*

Proof. If $x \in \mathfrak{p} \in \mathrm{Ass}(R)$, then x must kill something in R as it is in an associated prime. So x is a zerodivisor.

Conversely, suppose x is a zerodivisor, say $xy = 0$ for some $y \in R - \{0\}$. In particular, $x \in \mathrm{Ann}(y)$. We have an injection $R/\mathrm{Ann}(y) \hookrightarrow R$ sending 1 to y. But $R/\mathrm{Ann}(y)$ is nonzero, so it has an associated prime $\mathfrak{p}$ of $R/\mathrm{Ann}(y)$, which contains $\mathrm{Ann}(y)$ and thus x. But $\mathrm{Ass}(R/\mathrm{Ann}(y)) \subset \mathrm{Ass}(R)$. So x is contained in a prime in $\mathrm{Ass}(R)$. ▲

Assume now that R is reduced. Then $K(R) = S^{-1}R$ where S is the complement of the union of the minimal primes. At least, we can claim:

21.16 Proposition. *Let R be reduced and noetherian. Then $K(R) = \prod_{\mathfrak{p}_i \text{ minimal}} R_{\mathfrak{p}_i}$.*

So $K(R)$ is the product of fields into which R embeds. We will give a proof of this next time.

Lecture 22
10/18

§1 A loose end

Let us start with a little IOU from last time. We were talking about the theory of artinian rings. We asserted the following without proof.

22.1 Lemma. *If R is artinian, then* $\mathrm{Rad}(R)$ *is nilpotent.*

Proof. Call $J = \mathrm{Rad}(R)$. Consider the decreasing filtration

$$R \supset J \supset J^2 \supset J^3 \supset \dots.$$

We want to show that this stabilizes at zero. A priori, we know that it stabilizes *somewhere*. For some n, we have

$$J^n = J^{n'}, \quad n' \geq n.$$

Call the eventual stabilization of these ideals I. Consider ideals I' such that

$$II' \neq 0.$$

1. There aren't any such I'. Then $I = 0$, and we're done.

2. Otherwise, there is one, namely the unit ideal (1). So there is a minimal such I' as this is an artinian ring. What can we say about I'? Necessarily it is nonzero, and furthermore there is $x \in I'$ with $xI \neq 0$. It follows by minimality that

   $$I' = (x)$$

   so I' is principal, generated by some $x \in I'$. Then $xI \neq 0$; observe that this is also $(xI)I$ as $I^2 = I$ from the definition of I. Since $(xI)I \neq 0$, it follows again by minimality that

   $$xI = (x).$$

   This means that there is $y \in I$ such that $xy = x$; but now, by construction $I \subset J = \mathrm{Rad}(R)$, implying that y is nilpotent. It follows that

   $$x = xy = xy^2 = \dots = 0$$

   as y is nilpotent. However, $x \neq 0$ as $xI \neq 0$.

▲

This finishes the IOU.

§2 Total rings of fractions

We now continue the discussion begun last time. Let R be noetherian and M a finitely generated R-module. We would like to understand very rough features of M. We can embed M into a larger R-module. Here are two possible approaches.

1. $S^{-1}M$, where S is a large multiplicatively closed subset of M. Let us take S to be the set of all $a \in R$ such that $M \overset{a}{\to} M$ is injective, i.e. a is not a zerodivisor on M. Then the map
$$M \to S^{-1}M$$
is an injection. Note that S is the complement of the union of $\mathrm{Ass}(R)$.

2. Another approach would be to use a *primary decomposition*
$$M \hookrightarrow \prod M_i,$$
where each M_i is $\mathfrak{p}_i$-primary for some prime $\mathfrak{p}_i$ (and these primes range over $\mathrm{Ass}(M)$). In this case, it is clear that anything not in each $\mathfrak{p}_i$ acts injectively. So we can draw a commutative diagram
$$\begin{tikzcd} M \arrow[r] \arrow[d] & \prod M_i \arrow[d] \\ \prod M_{\mathfrak{p}_i} \arrow[r] & \prod (M_i)_{\mathfrak{p}_i} \end{tikzcd} .$$
The map going right and down is injective. It follows that M injects into the product of its localizations at associated primes.

The claim is that these constructions agree if M has no embedded primes. I.e., if there are no nontrivial containments among the associated primes of M, then $S^{-1}M$ (for $S = R - \bigcup_{\mathfrak{p} \in \mathrm{Ass}(M)} \mathfrak{p}$) is just $\prod M_{\mathfrak{p}}$. To see this, note that any element of S must act invertibly on $\prod M_{\mathfrak{p}}$. We thus see that there is always a map
$$S^{-1}M \to \prod_{\mathfrak{p} \in \mathrm{Ass}(M)} M_{\mathfrak{p}}.$$

22.2 Proposition. *This is an isomorphism if M has no embedded primes.*

Proof. Let us go through a series of reductions. Let $I = \mathrm{Ann}(M) = \{a : aM = 0\}$. Wlog, we can replace R by R/I. This plays nice with the associated primes.

The assumption is now that $\mathrm{Ass}(M)$ consists of the minimal primes of R.

Without loss of generality, we can next replace R by $S^{-1}R$ and M by $S^{-1}M$, because that doesn't affect the conclusion; localization plays nice with associated primes.

Now, however, R is artinian: i.e., all primes of R are minimal (or maximal). Why is this? Let R be *any* noetherian ring and $S = R - \bigcup_{\mathfrak{p} \text{ minimal}} \mathfrak{p}$. Then I claim that $S^{-1}R$ is artinian. We'll prove this in a moment.

So R is artinian, hence a product $\prod R_i$ where each R_i is local artinian. Without loss of generality, we can replace R by R_i by taking products. The condition we are trying to prove is now that

$$S^{-1}M \to M_{\mathfrak{m}}$$

for $\mathfrak{m} \subset R$ the maximal ideal. But S is the complement of the union of the minimal primes, so it is $R - \mathfrak{m}$ as R has one minimal (and maximal) ideal. This is obviously an isomorphism: indeed, both are M. ▲

Let us return to the claim. It is called **prime avoidance**. We start by proving:

22.3 Proposition. *Let $\mathfrak{p}_1, \mathfrak{p}_2, \dots, \mathfrak{p}_n$ be a finite set of primes of R. Suppose $I \subset R$ is not contained in any $\mathfrak{p}_i$. Then there is $x \in I$ such that x is not contained in any $\mathfrak{p}_i$.*

This implies the claim made earlier. In a noetherian ring, a nonminimal prime will contain an element which does not belong to any minimal prime. It follows that if $S = R - \bigcup_{\mathfrak{p} \text{ minimal}} \mathfrak{p}$, then S contains an element of each nonminimal prime. So $S^{-1}R$ has only minimal primes.

Proof. Induction on n.

When $n = 1$, this is obvious.

Suppose $n > 1$ and the result is true for $n - 1$. The inductive hypothesis states that for each $i \in [1, n]$, there is $x_i \in I$ which fails to lie in $\mathfrak{p}_i$ for $i \neq j$. If there is i such that $x_i \notin \mathfrak{p}_i$, then we're done—take $x = x_i$. Assume otherwise, so each $x_i \in \mathfrak{p}_i$.

We now take

$$x = \sum_i \prod_{j \neq i} x_j.$$

Then evidently $x \in I$, I being an ideal. We now show that $x \notin \mathfrak{p}_i$ for each i. The reason is that there is one term in the sum which doesn't include the factor x_i, but is the product of the $x_j, j \neq i$; this doesn't belong to $\mathfrak{p}_i$ then. All the other terms in the sum include the factor x_i so do belong to $\mathfrak{p}_i$. When we add up a bunch of things such that one doesn't belongs $\mathfrak{p}_i$ and the others do, the sum isn't in $\mathfrak{p}_i$. This establishes prime avoidance. ▲

22.4 Corollary. *Let R be a noetherian ring with no embedded primes (i.e.* $\mathrm{Ass}(R)$ *consists of minimal primes). Then $K(R) = \prod_{\mathfrak{p}_i \text{ minimal}} R_{\mathfrak{p}_i}$.*

If R is reduced, we get the statement made last time: there are no embedded primes, and $K(R)$ is a product of fields.

§3 The image of $M \to S^{-1}M$

Let's ask now the following question. Let R be a noetherian ring, M a finitely generated R-module, and S the set of nonzerodivisors on M, i.e. $R - \bigcup_{\mathfrak{p} \in \mathrm{Ass}(M)} \mathfrak{p}$. We have seen that there is an imbedding

$$\phi : M \hookrightarrow S^{-1}M.$$

What is the image? Given $x \in S^{-1}M$, when does it belong to the imbedding above.

To answer such a question, it suffices to check locally. In particular:

22.5 Proposition. *x belongs to the image of M in $S^{-1}M$ iff for every $\mathfrak{p} \in \mathrm{Spec}R$, the image of x in $(S^{-1}M)_{\mathfrak{p}}$ lies inside $M_{\mathfrak{p}}$.*

This isn't all that interesting. However, it turns out that you can check this at a smaller set of primes.

22.6 Proposition. *In fact, it suffices to show that x is in the image of $\phi_{\mathfrak{p}}$ for every $\mathfrak{p} \in \mathrm{Ass}(M/sM)$ where $s \in S$.*

This is a little opaque; soon we'll see what it actually means. The proof is very simple.

Proof. Remember that $x \in S^{-1}M$. In particular, we can write $x = y/s$ where $y \in M, s \in S$. What we'd like to prove that $x \in M$, or equivalently that $y \in sM$.[16] In particular, we want to know that y maps to zero in M/sM. If not, there exists an associated prime $\mathfrak{p} \in \mathrm{Ass}(M/sM)$ such that y does not get killed in $(M/sM)_{\mathfrak{p}}$. We have assumed, however, for every associated prime $\mathfrak{p} \in \mathrm{Ass}(M)$, $x \in (S^{-1}M)_{\mathfrak{p}}$ lies in the image of $M_{\mathfrak{p}}$. This states that the image of y in this quotient $(M/sM)_{\mathfrak{p}}$ is zero, or that y is divisible by s in this localization. ▲

The case we actually care about is the following:

Take R as a noetherian domain and $M = R$. Then $S = R - \{0\}$ and $S^{-1}M$ is just the fraction field $K(R)$. The goal is to describe R as a subset of $K(R)$. What we have proven is that R is the intersection in the fraction field

$$\boxed{R = \bigcap_{\mathfrak{p} \in \mathrm{Ass}(R/s), s \in R-0} R_{\mathfrak{p}}.}$$

So to check that something belongs to R, we just have to check that in a *certain set of localizations.*

Let us state this as a result:

22.7 Theorem (Krull intersection theorem, preliminary version)**.** *If R is a noetherian domain*

$$R = \bigcap_{\mathfrak{p} \in \mathrm{Ass}(R/s), s \in R-0} R_{\mathfrak{p}}$$

§4 Serre's criterion

We can now state a result.

22.8 Theorem (Serre)**.** *Let R be a noetherian domain. Then R is integrally closed iff it satisfies*

1. *For any $\mathfrak{p} \subset R$ of height one, $R_{\mathfrak{p}}$ is a DVR.*
2. *For any $s \neq 0$, R/s has no embedded primes (i.e. all the associated primes of R/s are height one).*

[16] In general, this would be equivalent to $ty \in tsM$ for some $t \in S$; but S consists of nonzerodivisors on M.

Here is the non-preliminary version of the Krull theorem.

22.9 Theorem (Krull)**.** *Let R be a noetherian integrally closed ring. Then*

$$R = \bigcap_{\mathfrak{p} \text{ height one}} R_{\mathfrak{p}},$$

where each $R_{\mathfrak{p}}$ is a DVR.

Proof. Now evident from the earlier Krull theorem and Serre's criterion. ▲

Earlier in the class, we proved that a domain was integrally closed if and only if it could be described as an intersection of valuation rings. We have now shown that when R is noetherian, we can take *discrete* valuation rings.

Remark. In algebraic geometry, say $R = \mathbb{C}[x_1, \dots, x_n]/I$. Its maximal spectrum is a subset of $\mathbb{C}^n$. If I is prime, and R a domain, this variety is irreducible. We are trying to describe R inside its field of fractions.

The field of fractions are like the "meromorphic functions"; R is like the holomorphic functions. Geometrically, this states to check that a meromorphic function is holomorphic, you can just check this by computing the "poleness" along each codimension one subvariety. If the function doesn't blow up on each of the codimension one subvarieties, and R is normal, then you can extend it globally.

This is an algebraic version of Hartog's theorem: this states that a holomorphic function on $\mathbb{C}^2 - (0, 0)$ extends over the origin, because this has codimension > 1.

All the obstructions of extending a function to all of $\mathrm{Spec} R$ are in codimension one.

Now, we prove Serre's criterion.

Proof. Let us first prove that R is integrally closed if 1 and 2 occur. We know that

$$R = \bigcap_{\mathfrak{p} \in \mathrm{Ass}(R/x), x \neq 0} R_{\mathfrak{p}};$$

by condition 1, each such $\mathfrak{p}$ is of height one, and $R_{\mathfrak{p}}$ is a DVR. So R is the intersection of DVRs and thus integrally closed.

The hard part is going in the other direction. Assume R is integrally closed. We want to prove the two conditions. In R, consider the following conditions on a prime ideal $\mathfrak{p}$:

1. $\mathfrak{p}$ is an associated prime of R/x for some $x \neq 0$.

2. $\mathfrak{p}$ is height one.

3. $\mathfrak{p}_{\mathfrak{p}}$ is principal in $R_{\mathfrak{p}}$.

First, 3 implies 2 implies 1. 3 implies that $\mathfrak{p}$ contains an element x which generates $\mathfrak{p}$ after localizing. It follows that there can be no prime between (x) and $\mathfrak{p}$ because that would be preserved under localization. Similarly, 2 implies 1 is easy. If $\mathfrak{p}$ is minimal over (x), then $\mathfrak{p} \in \mathrm{Ass} R/(x)$ since the minimal primes in the support are always associated.

We are trying to prove the inverse implications. In that case, the claims of the theorem will be proved. We have to show that 1 implies 3. This is an argument we really saw last time, but let's see it again. Say $\mathfrak{p} \in \mathrm{Ass}(R/x)$. We can replace R by $R_\mathfrak{p}$ so that we can assume that $\mathfrak{p}$ is maximal. We want to show that $\mathfrak{p}$ is generated by one element.

What does the condition $\mathfrak{p} \in \mathrm{Ass}(R/x)$ buy us? It tells us that there is $\overline{y} \in R/x$ such that $\mathrm{Ann}(\overline{y}) = \mathfrak{p}$. In particular, there is $y \in R$ such that $\mathfrak{p}y \subset (x)$ and $y \notin (x)$. We have the element $y/x \in K(R)$ which sends $\mathfrak{p}$ into R. That is,

$$(y/x)\mathfrak{p} \subset R.$$

There are two cases to consider, as in last time:

1. $(y/x)\mathfrak{p} = R$. Then $\mathfrak{p} = R(x/y)$ so $\mathfrak{p}$ is principal.
2. $(y/x)\mathfrak{p} \neq R$. In particular, $(y/x)\mathfrak{p} \subset \mathfrak{p}$. Then since $\mathfrak{p}$ is finitely generated, we find that y/x is integral over R, hence in R. This is a contradiction as $y \notin (x)$.

Only the first case is now possible. So $\mathfrak{p}$ is in fact principal. ▲

Lecture 23
10/20

What we'd like to talk about today is something mentioned on the first day, and many times since. Namely, the **Nullstellensatz.**

§1 The Hilbert Nullstellensatz

There are several ways to say it. Let us start with the following.

23.1 Theorem. *All maximal ideals in the polynomial ring $R = \mathbb{C}[x_1, \dots, x_n]$ come from points in $\mathbb{C}^n$.*

The maximal spectrum of $R = \mathbb{C}[x_1, \dots, x_n]$ is thus identified with $\mathbb{C}^n$. This can be thought of in the following way. Let $\mathfrak{m} \subset R$ be a maximal ideal. Then there is a map

$$\mathbb{C} \to R \to R/\mathfrak{m}$$

where $R/\mathfrak{m}$ is thus a finitely generated $\mathbb{C}$-algebra, as R is. We would like to show that $R/\mathfrak{m}$ is a finitely generated $\mathbb{C}$-vector space. This would imply that $R/\mathfrak{m}$ is integral over $\mathbb{C}$, and there are no proper algebraic extensions of $\mathbb{C}$.

The Nullstellensatz in this form would follow from the next claim:

23.2 Proposition. *Let k be a field, L/k an extension of fields. Suppose L is a finitely generated k-algebra. Then L is a finite k-vector space.*

This is what we will prove.

We start with an easy proof in the special case:

23.3 Lemma. *Assume k is uncountable (e.g. $\mathbb{C}$, the original case of interest). Then the above proposition is true.*

Proof. Since L is a finitely generated k-algebra, it suffices to show that L/k is algebraic. If not, there exists $x \in L$ which isn't algebraic over k. So x satisfies no nontrivial polynomials. I claim now that the uncountably many elements $\frac{1}{x-\lambda}, \lambda \in K$ are linearly independent over K. This will be a contradiction as L is a finitely generated k-algebra, hence at most countably dimensional over k. (Note that the polynomial ring is countably dimensional over k, and L is a quotient.)

So let's prove this. Suppose not. Then there is a nontrivial linear dependence

$$\sum \frac{c_i}{x-\lambda_i} = 0, \quad c_i, \lambda_i \in K.$$

Here the λ_j are all distinct to make this nontrivial. Clearing denominators, we find

$$\sum_i c_i \prod_{j \neq i} (x - \lambda_j) = 0.$$

Wlog, $c_1 \neq 0$. This equality was in the field L. But x is transcendental over k. So we can think of this as a polynomial ring relation. Since we can think of this as a relation in the polynomial ring, we see that doing so, all but the $i = 1$ term in the sum is divisible by $x - \lambda_1$ as a polynomial. It follows that, as polynomials in the indeterminate x,

$$x - \lambda_1 \mid c_1 \prod_{j \neq 1} (x - \lambda_j).$$

This is a contradiction since all the λ_i are distinct. ▲

This is kind of a strange proof, as it exploits the fact that $\mathbb{C}$ is uncountable. This shouldn't be relevant.

§2 The normalization lemma

Let's now give a more algebraic proof. We shall exploit the following highly useful fact in commutative algebra:

23.4 Theorem (Noether normalization lemma)**.** *Let k be a field, and $R = k[x_1, \dots, x_n]/\mathfrak{p}$ be a finitely generated domain over k (where $\mathfrak{p}$ is a prime ideal in the polynomial ring).*

Then there exists a polynomial subalgebra $k[y_1, \dots, y_m] \subset R$ such that R is integral over $k[y_1, \dots, y_m]$.

Later we will see that m is the *dimension* of R.

There is a geometric picture here. Then $\mathrm{Spec} R$ is some irreducible algebraic variety in k^n (plus some additional points), with a smaller dimension than n if $\mathfrak{p} \neq 0$. Then there exists a *finite map* to k^m. In particular, we can map surjectively $\mathrm{Spec} R \to k^m$ which is integral. The fibers are in fact finite, because integrality implies finite fibers. (We have not actually proved this yet.)

How do we actually find such a finite projection? In fact, in characteristic zero, we just take a vector space projection $\mathbb{C}^n \to \mathbb{C}^m$. For a "generic" projection onto a subspace of the appropriate dimension, the projection will will do as our finite map. In characteristic p, this may not work.

Proof. First, note that m is uniquely determined as the transcendence degree of the quotient field of R over k.

Among the variables $x_1, \dots, x_n \in R$ (which we think of as in R by an abuse of notation), choose a maximal subset which is algebraically independent. This subset has no nontrivial polynomial relations. In particular, the ring generated by that subset is just the polynomial ring on that subset. We can permute these variables and assume that

$$\{x_1, \dots, x_m\}$$

is the maximal subset. In particular, R contains the *polynomial ring* $k[x_1, \dots, x_m]$ and is generated by the rest of the variables. The rest of the variables are not adjoined freely though.

The strategy is as follows. We will implement finitely many changes of variable so that R becomes integral over $k[x_1, \dots, x_m]$.

The essential case is where $m = n - 1$. Let us handle this. So we have

$$R_0 = k[x_1, \dots, x_m] \subset R = R_0[x_n]/\mathfrak{p}.$$

Since x_n is not algebraically independent, there is a nonzero polynomial $f(x_1, \dots, x_m, x_n) \in \mathfrak{p}$.

We want f to be monic in x_n. This will buy us integrality. A priori, this might not be true. We will modify the coordinate system to arrange that, though. Choose $N \gg 0$. Define for $1 \leq i \leq m$,

$$x_i' = x_i + x_n^{N^i}.$$

Then the equation becomes:

$$0 = f(x_1, \dots, x_m, x_n) = f(\left\{x_i' - x_n^{N^i}\right\}, x_n).$$

Now $f(x_1, \dots, x_n, x_{n+1})$ looks like some sum

$$\sum \lambda_{a_1 \dots b} x_1^{a_1} \dots x_m^{a_m} x_n^b, \quad \lambda_{a_1 \dots b} \in k.$$

But N is really really big. Let us expand this expression in the x_i' and pay attention to the largest power of x_n we see. We find that

$$f(\left\{x_i' - x_n^{N_i}\right\}, x_n)$$

has the largest power of x_n precisely where, in the expression for f, a_m is maximized first, then a_{m-1}, and so on. The largest exponent would have the form

$$x_n^{a_m N^m + a_{m-1} N^{m-1} + \dots + b}.$$

We can't, however, get any exponents of x_n in the expression $f(\left\{x_i' - x_n^{N_i}\right\}, x_n)$ other than these. If N is super large, then all these exponents will be different from each other. In particular, each power of x_n appears precisely once in the expansion of f. We see in particular that x_n is integral over $x_1', \dots, x_n'$. Thus each x_i is as well.

So we find

R is integral over $k[x_1', \dots, x_m']$.

We have thus proved the normalization lemma in the codimension one case. What about the general case? We repeat this. Say we have

$$k[x_1, \dots, x_m] \subset R.$$

Let R' be the subring of R generated by $x_1, \dots, x_m, x_{m+1}$. The argument we just gave implies that we can choose $x_1', \dots, x_m'$ such that R' is integral over $k[x_1', \dots, x_m']$, and the x_i' are algebraically independent. We know in fact that $R' = k[x_1', \dots, x_m', x_{m+1}]$.

Let us try repeating the argument while thinking about x_{m+2}. Let $R'' = k[x_1', \dots, x_m', x_{m+2}]$ modulo whatever relations that x_{m+2} has to satisfy. So this is a subring of R. The same argument shows that we can change variables such that $x_1'', \dots, x_m''$ are algebraically independent and R'' is integral over $k[x_1'', \dots, x_m'']$. We have furthermore that $k[x_1'', \dots, x_m'', x_{m+2}] = R''$.

Having done this, let us give the argument where $m = n - 2$. You will then see how to do the general case. Then I claim that:

R is integral over $k[x_1'', \dots, x_m'']$.

For this, we need to check that x_{m+1}, x_{m+2} are integral (because these together with the x_i'' generate $R''[x_{m+2}][x_{m+2}] = R$. But x_{m+2} is integral over this by construction. The integral closure of $k[x_1'', \dots, x_m'']$ in R thus contains

$$k[x_1'', \dots, x_m'', x_{m+2}] = R''.$$

However, R'' contains the elements $x_1', \dots, x_m'$. But by construction, x_{m+1} is integral over the $x_1', \dots, x_m'$. The integral closure of $k[x_1'', \dots, x_m'']$ must contain x_{m+2}. This completes the proof in the case $m = n - 2$. The general case is similar; we just make several changes of variables, successively.

▲

§3 Back to the Nullstellensatz

Consider a finitely generated k-algebra R which is a field. We need to show that R is a finite k-module. This will prove the proposition. Well, note that R is integral over a polynomial ring $k[x_1, \dots, x_m]$ for some m. If $m > 0$, then this polynomial ring has more than one prime. For instance, (0) and $(x_1, \dots, x_m)$. But these must lift to primes in R. Indeed, we have seen that whenever you have an integral extension, the induced map on spectra is surjective. So

$$\mathrm{Spec} R \to \mathrm{Spec} k[x_1, \dots, x_m]$$

is surjective. If R is a field, this means $\mathrm{Spec} k[x_1, \dots, x_m]$ has one point and $m = 0$. So R is integral over k, thus algebraic. This implies that R is finite as it is finitely generated. This proves one version of the Nullstellensatz.

§4 Another version

Another version of the Nullstellensatz, which is more precise, says:

23.5 Theorem. *Let $I \subset \mathbb{C}[x_1, \dots, x_n]$. Let $V \subset \mathbb{C}^n$ be the subset of $\mathbb{C}^n$ defined by the ideal I (i.e. the zero locus of I).*

Then $\mathrm{Rad}(I)$ *is precisely the collection of f such that $f|_V = 0$. In particular,*

$$\mathrm{Rad}(I) = \bigcap_{\mathfrak{m} \supset I, \mathfrak{m} \text{ maximal}} \mathfrak{m}.$$

In particular, there is a bijection between radical ideals and algebraic subsets of $\mathbb{C}^n$.

The last form of the theorem, which follows from the expression of maximal ideals in the polynomial ring, is very similar to the result

$$\mathrm{Rad}(I) = \bigcap_{\mathfrak{p} \supset I, \mathfrak{p} \text{ prime}} \mathfrak{p},$$

true in any commutative ring. However, this general result is not necessarily true.

23.6 Example. The intersection of all primes in a DVR is zero, but the intersection of all maximals is nonzero.

Proof. It now suffices to show that for every $\mathfrak{p} \subset \mathbb{C}[x_1, \dots, x_n]$ prime, we have

$$\mathfrak{p} = \bigcap_{\mathfrak{m} \supset I \text{ maximal}} \mathfrak{m}$$

since every radical ideal is an intersection of primes.

How can we prove this? Well, let $R = \mathbb{C}[x_1, \dots, x_n]/\mathfrak{p}$. This is a domain finitely generated over $\mathbb{C}$. We want to show that the intersection of maximal ideals in R is zero. This is equivalent to the above displayed equality.

So fix $f \in R - \{0\}$. Let $R' = R[f^{-1}]$. Then R' is also an integral domain, finitely generated over $\mathbb{C}$. R' has a maximal ideal $\mathfrak{m}$ (which a priori could be zero). If we look at the map $R' \to R'/\mathfrak{m}$, we get a map into a field finitely generated over $\mathbb{C}$, which is thus $\mathbb{C}$. The composite map

$$R \to R' \to R'/\mathfrak{m}$$

is just given by an n-tuple of complex numbers, i.e. to a point in $\mathbb{C}^n$ which is even in V as it is a map out of R. This corresponds to a maximal ideal in R. This maximal ideal does not contain f by construction. ▲

Lecture 24
10/22

Today, we will start talking about completions of commutative rings. Let us begin with some motivation.

§1 Motivation

Say you have a commutative ring R. We can draw Spec$R$, a picture whose points are the primes of R. Consider a maximal ideal $\mathfrak{m} \in$ Spec$R$. If you think of Spec$R$ as a space, and R as a collection of functions on that space, then $R_{\mathfrak{m}}$ is the collection of "germs" of functions defined near the point $\mathfrak{m}$.

The Zariski topology is kind of lousy as far as topologies go, and you can't really find small neighborhoods of $\mathfrak{m}$.

24.1 Example. Let X be a compact Riemann surface, and let $x \in X$. Let R be the ring of holomorphic functions on $X - \{x\}$ which are meromorphic at x. In this case, Spec$R$ has the ideal (0) and maximal ideals corresponding to the zero locus at some point in $X - \{x\}$. So Spec$R$ is $X - \{x\}$ together with a "generic" point.

Let's just look at the closed points. If we pick $y \in X - \{x\}$, then we can consider the local ring $R_y = \left\{s^{-1}r, s(y) \neq 0\right\}$. This ring is a direct limit of the rings of holomorphic functions on sets U that extend meromorphically to X, where U ranges over open subsets of X containing y which are the nonzero loci of things in R. However, U really ranges over complements of finite subsets. It does not range over open sets in the *complex* topology.

Near y, X looks like the complex numbers in the complex plane. In the Zariski topology, this isn't the case. Each R_y actually remembers the whole Riemann surface. The reason is that the quotient field of R_y is the rational function field of X, which recovers X. Thus R_y remembers too much.

We would like a variant of localization that would remember much less about the global topology.

§2 Definition

24.2 Definition. Let R be a commutative ring and $I \subset R$ an ideal. Then we define the **completion of R at I**

$$\hat{R}_I = \varprojlim R/I^n.$$

So this is the inverse limit of the quotients R/I^n. There is a tower of commutative rings

$$\cdots \to R/I^3 \to R/I^2 \to R/I$$

whose inverse limit is $R_I^\vee$.

Let us give some examples.

24.3 Example. Let $R = \mathbb{Z}, I = (p)$. Then the completion is denoted $\mathbb{Z}_p$ and is called the ring of **p-adic integers.** This is the inverse limit of the rings $\mathbb{Z}/p^i$.

24.4 Example. Let X be a Riemann surface. Let $x \in X$ be as before, and let R be as before: the ring of meromorphic functions on X with poles only at x. We can complete R at the ideal $\mathfrak{m}_y \subset R$ corresponding to $y \in X - \{x\}$. This is always isomorphic to a power series ring

$$\mathbb{C}[[t]]$$

where t is a holomorphic coordinate at y.

The reason is that if you consider $R/\mathfrak{m}_y^n$, you always get $\mathbb{C}[t]/(t^n)$, where t corresponds to a local coordinate at y. Thus *these* rings don't remember much about the Riemann surface. They're all isomorphic, for instance.

Remark. Usually, we will complete R at *maximal* ideals. If we wanted to study R near a prime $\mathfrak{p} \in \mathrm{Spec} R$, we might first approximate R by $R_{\mathfrak{p}}$, which is a local ring; we might make another approximation by completing $R_{\mathfrak{p}}$. Then we get a *really* local structure.

Remark. There is always a map $R \to \hat{R}_I$ by taking the limit of the maps R/I^i.

A priori, you might think you get a big mess. The amazing thing is that for noetherian rings, you get well-behaved stuff.

§3 Properties of completions

24.5 Proposition. *Let R be noetherian, $I \subset R$ an ideal. Then $\hat{R}_I$ is noetherian.*

Proof. Choose generators $x_1, \dots, x_n \in I$. This can be done as I is finitely generated Consider a power series ring

$$R[[t_1, \dots, t_n]];$$

the claim is that there is a map $R[[t_1 \dots t_n]] \to \hat{R}_I$ sending each t_i to $x_i \in \hat{R}_I$. This is not trivial, since we aren't talking about a polynomial ring, but a power series ring.

To build this map, we want a compatible family of maps

$$R[[t_1, \dots, t_n]] \to R[t_1, \dots, t_n]/(t_1, \dots, t_n)^k \to R/I^k.$$

where the second ring is the polynomial ring where you have killed homogeneous polynomials of degree $\geq k$. There is a map from $R[[t_1, \dots, t_n]]$ to the second ring that kills monomials of degree $\geq k$. The second map $R[t_1, \dots, t_n]/(t_1, \dots, t_n)^k \to R/I^k$ sends $t_i \to x_i$ and is obviously well-defined.

So we get the map

$$\phi : R[[t_1, \dots, t_n]] \to \hat{R}_I,$$

which I claim is surjective. Let us prove this. Suppose $a \in \hat{R}_I$. Then a can be thought of as a collection of elements $(a_k) \in R/I^k$ which are compatible with one another. We can lift each a_k to some $\overline{a_k} \in R$ in a compatible manner, such that

$$\overline{a_{k+1}} = \overline{a_k} + b_k, \quad b_k \in I^k.$$

Since $b_k \in I^k$, we can write it as

$$b_k = f_k(x_1, \dots, x_n)$$

for f_k a polynomial in R of degree k, by definition of the generators in I^k.

I claim now that

$$a = \phi\left(\sum f_k(t_1, \dots, t_n)\right).$$

The proof is just to check modulo I^k for each k. This we do by induction. When you reduce modulo I^k, one checks easily that you get a_k.

As we have seen, $\hat{R}_I$ is the quotient of a power series ring. In the homework, it was seen that $R[[t_1, \dots, t_n]]$ is noetherian; this is a variant of the Hilbert basis theorem proved in class. So $\hat{R}_I$ is noetherian. ▲

We want to think of completion as analogous to localization. We would like to think of it as an inoffensive operation. One way to say this for localization was that localization is an exact functor. This is true for completions too. But first, we need a variant: completions of modules.

24.6 Definition. Let R be a ring, M an R-module, $I \subset R$ an ideal. We define the **completion of** M **at** I as

$$\hat{M}_I = \varprojlim M/I^nM.$$

This is an inverse limit of R-modules, so it is an R-module. Furthermore, it is even an $\hat{R}_I$-module, as one easily checks. It is also functorial.

24.7 Proposition. *If R is noetherian and $I \subset R$ an ideal, then the construction $M \to \hat{M}_I$ is exact when restricted to finitely generated modules.*

Let's be more precise. If M is finitely generated, and $0 \to M' \to M \to M'' \to 0$ is an exact sequence,[17] then

$$0 \to \hat{M'}_I \to \hat{M}_I \to \hat{M''}_I \to 0$$

is also exact.

For a moment, let us step back and think about exact sequences of inverse limits of abelian groups. Say we have a tower of exact sequences of abelian groups

$$\begin{tikzcd}
0 \arrow[r] & \vdots \arrow[r] \arrow[d] & \vdots \arrow[r] \arrow[d] & \vdots \arrow[r] \arrow[d] & 0 . \\
0 \arrow[r] & A_2 \arrow[r] \arrow[d] & B_2 \arrow[r] \arrow[d] & C_2 \arrow[r] \arrow[d] & 0 \\
0 \arrow[r] & A_1 \arrow[r] \arrow[d] & B_1 \arrow[r] \arrow[d] & C_1 \arrow[r] \arrow[d] & 0 \\
0 \arrow[r] & A_0 \arrow[r] & B_0 \arrow[r] & C_0 \arrow[r] & 0
\end{tikzcd}$$

Then we get a sequence

$$0 \to \varprojlim A_n \to \varprojlim B_n \to \varprojlim C_n \to 0.$$

In general, it is *not* exact. But it is left-exact.

24.8 Proposition. *Hypotheses as above,* $0 \to \varprojlim A_n \to \varprojlim B_n \to \varprojlim C_n$ *is exact.*

[17] The ends are finitely generated by noetherianness.

Proof. It is obvious that $\phi \circ \psi = 0$.

Let us first show that $\phi : \varprojlim A_n \to \varprojlim B_n$ is injective. So suppose a is in the projective limit, represented by a compatible sequence of elements $(a_k) \in A_k$. If ϕ maps to zero, all the a_k go to zero in B_k. Injectivity of $A_k \to B_k$ implies that each a_k is zero. This implies ϕ is injective.

Now let us show exactness at the next step. Let $\psi : \varprojlim B_n \to \varprojlim C_n$ and let $b = (b_k)$ be in $\ker \psi$. This means that each b_k gets killed when it maps to C_k. This means that each b_k comes from something in a_k. These a_k are unique by injectivity of $A_k \to B_k$. It follows that the a_k have no choice but to be compatible. Thus (a_k) maps into (b_k). So b is in the image of ϕ. ▲

So far, so good. We get some level of exactness. But the map on the end is not necessarily surjective. Nonetheless:

24.9 Proposition. *$\psi : \varprojlim B_n \to \varprojlim C_n$ is surjective if each $A_{n+1} \to A_n$ is surjective.*

Proof. Say $c \in \varprojlim C_n$, represented by a compatible family (c_k). We have to show that there is a compatible family $(b_k) \in \varprojlim B_n$ which maps into c. It is easy to choose the b_k *individiually* since $B_k \to C_k$ is surjective. The problem is that a priori we may not get something compatible.

We construct b_k by induction on then, therefore. Assume that b_k which lifts c_k has been constructed. We know that c_k receives a map from c_{k+1}.

$$\begin{tikzcd} & c_{k+1} . \arrow[d] \\ b_k \arrow[r] & c_k \end{tikzcd}$$

Choose any $x \in B_{k+1}$ which maps to c_{k+1}. However, x might not map down to b_k, which would screw up the compatibility conditions. Next, we try to adjust x. Consider $x' \in B_k$ to be the image of x under $B_{k+1} \to B_k$. We know that $x' - b_k$ maps to zero in C_k, because c_{k+1} maps to c_k. So $x' - b_k$ comes from something in A_k, call it a.

$$\begin{tikzcd} x \arrow[r] & c_{k+1} . \arrow[d] \\ b_k \arrow[r] & c_k \end{tikzcd}$$

But a comes from some $\overline{a} \in A_{k+1}$. Then we define

$$b_{k+1} = x - \overline{a},$$

which adjustment doesn't change the fact that b_{k+1} maps to c_{k+1}. However, this adjustment makes b_{k+1} compatible with b_k. Then we construct the family b_k by induction. We have seen surjectivity. ▲

Now, let us study the exactness of completions.

Proof of Proposition 24.7. Let us try to apply the general remarks above to studying the sequence

$$0 \to \hat{M'}_I \to \hat{M}_I \to \hat{M''}_I \to 0.$$

Now $\hat{M}_I = \varprojlim M/I^n$. We can construct surjective maps

$$M/I^n \twoheadrightarrow M''/I^n$$

whose inverse limits lead to $\hat{M}_I \to \hat{M''}_I$. The image is $M/(M' + I^n M)$. What is the kernel? Well, it is $M' + I^n M/I^n M$. This is equivalently

$$M'/M' \cap I^n M.$$

So we get an exact sequence

$$0 \to M'/M' \cap I^n M \to M/I^n M \to M''/I^n M'' \to 0.$$

By the above analysis of exactness of inverse limits, we get an exact sequence

$$0 \to \varprojlim M'/(I^n M \cap M') \to \hat{M}_I \to \hat{M''}_I \to 0.$$

We of course have surjective maps $M'/I^n M' \to M'/(I^n M \cap M')$ though these are generally not isomorphisms. Something "divisible by I^n" in M but in M' is generally not divisible by I^n in M'. Anyway, we get a map

$$\varprojlim M'/I^n M' \to \varprojlim M'/I^n M \cap M'$$

where the individual maps are not necessarily isomorphisms. Nonetheless, I claim that the map on inverse limits is an isomorphism. This will imply that completion is indeed an exact functor.

Essentially, to say that this map is an isomorphism is to say that the filtrations $I^n M'$ and $I^n M \cap M'$ on M' are *comparable.* To prove this, and to complete the proof of exactness, it suffices to show:

24.10 Proposition (Artin-Rees lemma)**.** *Let R be noetherian, $I \subset R$ an ideal. Suppose M is a finitely generated R-module and $M' \subset M$ a submodule. Then there is a constant c such that*

$$I^{n+c} M \cap M' \subset I^n M'.$$

So the two filtrations $I^n M \cap M', I^n M'$ on M are equivalent up to a shift.

Proof. Define a new ring $R' = R \oplus It \oplus I^2 t^2 + \dots$, which is a subring of $R[t]$. The coefficient of t^n is required to belong to I^n.

24.11 Lemma. *R' is noetherian.*

Proof. Choose generators $x_1, \dots, x_n \in I$; then there is a map $R[y_1, \dots, y_n] \to R'$ sending $y_i \to x_i t$. This is surjective. Hence by the basis theorem, R' is noetherian. ▲

Let $N = M \oplus IMt \oplus I^2M[t] \oplus \dots \subset M[t] = M \otimes_R R[t]$. Note that N is an R'-module. It is in fact a finitely generated R'-module, hence noetherian, since M was finitely generated over R. Let $N' = N \cap M'[t]$. In particular

$$N' = M' \oplus (M' \cap IM)t \oplus \dots.$$

So $N' \subset N$ is finitely generated. Choose generators for N', and let c be the largest degree (exponent of t) that occurs. I claim that c works. This is easy to check, but we're out of time. We'll talk about this more next week. ▲

▲

Lecture 25
10/25

Last time, we were talking about completions. We showed that if R is noetherian and $I \subset R$ an ideal, an exact sequence

$$0 \to M' \to M \to M \to 0$$

of finitely generated R-modules leads to a sequence

$$0 \to \hat{M'}_I \to \hat{M}_I \to \hat{M};_I \to 0$$

which is also exact. We showed this using the Artin-Rees lemma.

Remark. In particular, completion is an **exact functor**: if $A \to B \to C$ is exact, so is the sequence of completions. This can be seen by drawing in kernels and cokernels, and using the fact that completions preserve short exact sequences.

§1 Completions and flatness

Suppose that M is a finitely generated R-module. Then there is a surjection $R^n \twoheadrightarrow M$, whose kernel is also finitely generated as R is noetherian. It follows that M is finitely presented. In particular, there is a sequence

$$R^m \to R^n \to M \to 0.$$

We get an exact sequence

$$\hat{R}^m \to \hat{R}^n \to \hat{M} \to 0$$

where the second map is just multiplication by the same m-by-n matrix as in the first case.

25.1 Corollary. *If M is finitely generated, there is a canonical isomorphism*

$$\hat{M}_I \simeq M \otimes_R \hat{R}_I.$$

Proof. We know that there is a map $M \to \hat{M}_I$, so the canonical morphism $\phi_M : M \otimes_R \hat{R}_I \to \hat{M}_I$ exists (because this induces a map from $M \otimes_R \hat{R}_I$). We need to check that it is an isomorphism.

If there is an exact sequence $M' \to M \to M'' \to 0$, there is a commutative diagram

$$\begin{tikzcd}
M' \otimes_R \hat{R}_I \arrow[r] \arrow[d, "\phi_{M'}"] & M \otimes_R \hat{R}_I \arrow[r] \arrow[d, "\phi_M"] & M'' \otimes_R \hat{R}_I \arrow[r] \arrow[d] & 0 . \\
\hat{M'}_I \arrow[r] & \hat{M}_I \arrow[r] & \hat{M''}_I \arrow[r] & 0
\end{tikzcd}$$

Exactness of completion and right-exactness of $\otimes$ implies that this diagram is exact. It follows that if $\phi_M, \phi_{M'}$ are isomorphisms, so is $\phi_{M''}$.

But any M'' appears at the end of such a sequence with M', M are free by the finite presentation argument above. So it suffices to prove ϕ an isomorphism for finite frees, which reduces to the case of ϕ_R an isomorphism. That is obvious. ▲

25.2 Corollary. *$\hat{R}_I$ is a flat R-module.*

Proof. Indeed, tensoring with $\hat{R}_I$ is exact (because it is completion, and completion is exact) on the category of finitely generated R-modules. Exactness on the category of all R-modules follows by taking direct limits, since every module is a direct limit of finitely generated modules, and direct limits preserve exactness. ▲

Remark. Warning: $\hat{M}_I$ is, in general, not $M \otimes_R \hat{R}_I$ when M is not finitely generated. One example to think about is $M = \mathbb{Z}[t]$, $R = \mathbb{Z}$. The completion of M at $I = (p)$ is the completion of $\mathbb{Z}[t]$ at $p\mathbb{Z}[t]$, which contains elements like

$$1 + pt + p^2t^2 + \dots,$$

which belong to the completion but not to $\hat{R}_I \otimes M = \mathbb{Z}_p[t]$.

§2 The Krull intersection theorem

We lied earlier. What we called the Krull intersection theorem is not actually called the Krull theorem.

25.3 Theorem (Krull)**.** *Let R be a local noetherian ring with maximal ideal $\mathfrak{m}$.*[18] *Then the map $R \to \hat{R}_{\mathfrak{m}}$ is injective. Alternatively,*

$$\bigcap \mathfrak{m}^i = (0).$$

Proof. Let $I = \ker(R \to \hat{R}_{\mathfrak{m}})$. We have $I \hookrightarrow R$; thus there is a map

$$\hat{I}_{\mathfrak{m}} \hookrightarrow \hat{R}_{\mathfrak{m}}.$$

Now $\hat{I}_{\mathfrak{m}}$ is generated by I as an $R_{\mathfrak{m}}$-module. It follows that the map $\hat{I}_{\mathfrak{m}} \hookrightarrow R_{\mathfrak{m}}$ is the zero map.

So $\hat{I}_{\mathfrak{m}} = 0$. But this is the inverse limit of a tower of abelian groups $I/\mathfrak{m}^i I$ where the maps are surjections; to say that this limit is zero is to say that $I = \mathfrak{m}I$. So $I = 0$ by Nakayama. ▲

[18] This is a favorite time to complete R.

§3 Hensel's lemma

One thing that you might be interested in doing is solving Diophantine equations. Say $R = \mathbb{Z}$; you want to find solutions to a polynomial $f(X) \in \mathbb{Z}[X]$. Generally, it is very hard to find solutions. However, there are easy tests you can do that will tell you if there are no solutions. For instance, reduce mod a prime. One way you can prove that there are no solutions is to show that there are no solutions mod 2.

But there might be solutions mod 2 and yet you might not be sure about solutions in $\mathbb{Z}$. So you might try mod 4, mod 8, and so on—you get a whole tower of problems to consider. If you manage to solve all these equations , you can solve the equations in the 2-adic integers $\mathbb{Z}_2 = \hat{\mathbb{Z}}_{(2)}$.

But the Krull intersection theorem implies that $\mathbb{Z} \to \mathbb{Z}_2$ is injective. So if you expected that there was a unique solution in $\mathbb{Z}$, you might try looking at the solutions in $\mathbb{Z}_2$ to be the solutions in $\mathbb{Z}$.

The moral is that solving an equation over $\mathbb{Z}_2$ is intermediate in difficulty between $\mathbb{Z}/2$ and $\mathbb{Z}$. Nonetheless, it turns out that solving an equation mod $\mathbb{Z}/2$ is very close to solving it over $\mathbb{Z}_2$, thanks to

25.4 Theorem (Hensel's Lemma)**.** *Let R be a noetherian ring, $I \subset R$ an ideal. Let $f(X) \in R[X]$ be a polynomial such that the equation $f(X) = 0$ has a solution $a \in R/I$. Suppose, moreover, that $f'(a)$ is invertible in R/I.*

Then a lifts uniquely to a solution of the equation $f(X) = 0$ in $\hat{R}_I$.

25.5 Example. Let $R = \mathbb{Z}, I = (5)$. Consider the equation $f(x) = x^2 + 1 = 0$ in R. This has a solution modulo five, namely 2. Then $f'(2) = 4$ is invertible in $\mathbb{Z}/5$. So the equation $x^2 + 1 = 0$ has a solution in $\mathbb{Z}_5$. In other words, $\sqrt{-1} \in \mathbb{Z}_5$.

Let's prove Hensel's lemma.

Proof. Now we have $a \in R/I$ such that $f(a) = 0 \in R/I$ and $f'(a)$ is invertible. The claim is going to be that for each $m \geq 1$, there is a *unique* element $a_n \in R/I^n$ such that

$$a_n \to a \ (I), \quad f(a_n) = 0 \in R/I^n.$$

Uniqueness implies that this sequence (a_n) is compatible, and thus gives the required element of the completion. It will be a solution of $f(X) = 0$ since it is a solution at each element of the tower.

Let us now prove the claim. For $n = 1$, $a_1 = a$ necessarily. The proof is induction on n. Assume that a_n exists and is unique. We would like to show that a_{n+1} exists and is unique. Well, if it is going to exist, when we reduce a_{n+1} modulo I^n, we must get a_n or uniqueness at the n-th step would fail.

So let $\overline{a}$ be any lifting of a_n to R/I^{n+1}. Then a_{n+1} is going to be that lifting plus some $\epsilon \in I^n/I^{n+1}$. We want

$$f(\overline{a} + \epsilon) = 0 \in R/I^{n+1}.$$

But this is

$$f(\overline{a}) + \epsilon f'(\overline{a})$$

because $\epsilon^2 = 0 \in R/I^{n+1}$. However, this lets us solve for ϵ, because then necessarily $\epsilon = \frac{-f(\overline{a})}{f'(\overline{a})} \in I^n$. Note that $f'(\overline{a}) \in R/I^{n+1}$ is invertible. If you believe this for a moment, then we have seen that ϵ exists and is unique; note that $\epsilon \in I^n$ because $f(\overline{a}) \in I^n$.

25.6 Lemma. *$f'(\overline{a}) \in R/I^{n+1}$ is invertible.*

Proof. If we reduce this modulo R/I, we get the invertible element $f'(a) \in R/I$. Note also that the I/I^{n+1} is a nilpotent ideal in R/I^{n+1}. So we are reduced to showing, more generally:

25.7 Lemma. *Let A be a ring,*[19] *J a nilpotent ideal.*[20] *Then an element $x \in A$ is invertible if and only if its reduction in A/J is invertible.*

Proof. One direction is obvious. For the converse, say $x \in A$ has an invertible image. This implies that there is $y \in A$ such that $xy \equiv 1 \mod J$. Say

$$xy = 1 + m,$$

where $m \in J$. But $1 + m$ is invertible because

$$\frac{1}{1+m} = 1 - m + m^2 \pm \dots .$$

The expression makes sense as the high powers of m are zero. So this means that $y(1+m)^{-1}$ is the inverse to x. ▲

▲

▲

This was one of many versions of Hensel's lemma. There are many ways you can improve on a statement. The above version says something about "nondegenerate" cases, where the derivative is invertible. There are better versions which handle degenerate cases.

25.8 Example. Consider $x^2 - 1$; let's try to solve this in $\mathbb{Z}_2$. Well, $\mathbb{Z}_2$ is a domain, so the only solutions can be ± 1. But these have the same reduction in $\mathbb{Z}/2$. The lifting of the solution is non-unique.

The reason why Hensel's lemma fails is that $f'(\pm 1) = \pm 2$ is not invertible in $\mathbb{Z}/2$. But it is not far off. If you go to $\mathbb{Z}/4$, we do get two solutions, and the derivative is at least nonzero at those places.

One possible extension of Hensel's lemma is to allow the derivative to be noninvertible, but at least to bound the degree to which it is noninvertible. From this you can get interesting information. But then you may have to look at equations R/I^n instead of just R/I, where n depends on the level of noninvertibility.

Let us describe the multivariable Hensel lemma.

[19] E.g. R/I^{n+1}.

[20] E.g. $J = I/I^{n+1}$.

25.9 Theorem. *Let $f_1, \dots, f_n$ be polynomials in n variables over the ring R. Let J be the Jacobian matrix $(\frac{\partial f_i}{\partial x_j})$. Suppose $\Delta = \det J \in R[x_1, \dots, x_n]$.*

If the system $\{f_i(x) = 0\}$ has a solution $a \in (R/I)^n$ in R/I for some ideal I satisfying the condition that $\Delta(a)$ is invertible, then there is a unique solution of $\{f_i(x) = 0\}$ in $\hat{R}_I^n$ which lifts a.

The proof is the same idea: successive approximation, using the invertibility of Δ.

Lecture 26
10/27

Today, we'd like to start talking about dimension theory. But first we need a little something else.

§1 Some definitions

Let R be a commutative ring, M an R-module.

26.1 Definition. M is **simple** if $M \neq 0$ and M has no nontrivial submodules.

26.2 Definition. M is **finite length** if there is a finite filtration $0 \subset M^0 \subset \cdots \subset M^n = M$ where each M^i/M^{i-1} is simple.

Remark. M is simple iff it is isomorphic $R/\mathfrak{m}$ for $\mathfrak{m} \subset R$ an ideal. Why? Well, it must contain a cyclic submodule generated by $x \in M - \{0\}$. So it must contain a submodule isomorphic to R/I, and simplicity implies that $M \simeq R/I$ for some I. If I is not maximal, then we will get a nontrivial submodule of R/I. Conversely, it's easy to see that $R/\mathfrak{m}$ is simple for $\mathfrak{m}$ maximal.

26.3 Proposition. *M is finite length iff M is both noetherian and artinian.*

Proof. Any simple module is obviously both noetherian and artinian—there are two submodules. So if M is finite length, then the finite filtration with simple quotients implies that M is noetherian and artinian, since these two properties are stable under extensions.

Suppose $M \neq 0$ is noetherian and artinian. Let $M_1 \subset M$ be a minimal nonzero submodule, possible by artinianness. This is necessarily simple. Then we have a filtration

$$0 = M_0 \subset M_1.$$

If $M_1 = M$, then the filtration goes up to M, and we have that M is of finite length. If not, find a minimal M_2 containing M_1; then the quotient M_2/M_1 is simple. We have the filtration

$$0 = M_0 \subset M_1 \subset M_2,$$

which we can keep continuing until at some point we hit M. Note that since M is noetherian, we cannot continue this strictly ascending chain forever. ▲

26.4 Proposition. *In this case, the length of the filtration is well-defined. That is, any two filtrations on M with simple quotients have the same length.*

26.5 Definition. This number is called the **length** of M and is denoted $\ell(M)$.

Proof. Let us introduce a temporary definition: $l(M)$ is the length of the *minimal* filtration on M. A priori, we don't know that $\ell(M)$ makes any sense. **We will show that any filtration is of length $l(M)$.** This is the proposition in another form.

The proof of this claim is by induction on $l(M)$. Suppose we have a filtration

$$0 = M_0 \subset M_1 \subset \cdots \subset M_n = M$$

with simple quotients. We'd like to show that $n = l(M)$. By definition of $l(M)$, there is another filtration

$$0 = N_0 \subset \cdots \subset N_{l(M)} = M.$$

If $l(M) = 0, 1$, then M is zero or simple, which will imply that $n = 0, 1$ respectively. So we can assume $l(M) \geq 2$. There are two cases:

1. $M_{n-1} = N_{l(M)-1}$. Then $M_{n-1} = N_{l(M)-1}$ has l at most $l(M) - 1$. Thus by the inductive hypothesis any two filtrations on M_{n-1} have the same length, so $n - 1 = l(M) - 1$ implying what we want.

2. We have $M_{n-1} \cap N_{l(M)-1} \subsetneq M_{n-1}, N_{l(M)-1}$. Call this intersection K.

   Now we can replace the filtrations of $M_{n-1}, N_{l(M)-1}$ such that the next term after that is K, because any two filtrations on these proper submodules have the same length. So we find that $n-1 = l(K)+1$ and $l(M)-1 = l(K)+1$ by the inductive hypothesis. This implies what we want.

▲

§2 Introduction to dimension theory

Let R be a ring.

Question. What is a good definition for $\dim(R)$? Actually, more generally, we want the dimension at a point.

Geometrically, think of Spec$R$, for any ring; pick some point corresponding to a maximal ideal $\mathfrak{m} \subset R$. We want to define the **dimension of** R at $\mathfrak{m}$. This is to be thought of kind of like "dimension over the complex numbers," for algebraic varieties defined over $\mathbb{C}$. But it should be purely algebraic.

What might you do?

Here's an idea. For a topological space X to be n-dimensional at $x \in X$, this should mean that there are n coordinates at the point x. The point x is defined by the zero locus of n points on the space.

26.6 Definition (Proposal)**.** We could try defining $\dim_{\mathfrak{m}} R$ to be the number of gnerators of $\mathfrak{m}$.

This is a bad definition, as $\mathfrak{m}$ may not have the same number of generators as $\mathfrak{m}R_{\mathfrak{m}}$. We want our definition to be local. So this leads us to:

26.7 Definition. If R is a (noetherian) *local* ring with maximal ideal $\mathfrak{m}$, then the **embedding dimension** of R is the minimal number of gnerators for $\mathfrak{m}$.

By Nakayama's lemma, this is the minimal number of gnerators of $\mathfrak{m}/\mathfrak{m}^2$, or the $R/\mathfrak{m}$-dimension of that vector space. However, this isn't going to coincide with the dimension of an algebraic variety.

26.8 Example. Let $R = \mathbb{C}[t^2, t^3] \subset \mathbb{C}[t]$, which is the coordinate ring of a cubic curve. Let us localize at the prime ideal $\mathfrak{p} = (t^2, t^3)$: we get $R_{\mathfrak{p}}$.

Now Spec$R$ is singular at the origin. In fact, as a result, $\mathfrak{p}R_{\mathfrak{p}} \subset R_{\mathfrak{p}}$ needs two generators, but the variety it corresponds to is one-dimensional.

So the embedding dimension is the smallest dimension into which you can embed R into a smooth space. But for singular varieties this is not the dimension we want.

Well, we can consider the sequence of finite-dimensional vector spaces

$$\mathfrak{m}^k/\mathfrak{m}^{k+1}.$$

Computing these dimensions gives some invariant that describes the local geometry of Spec$R$.

26.9 Example. Consider the local ring $(R, \mathfrak{m}) = \mathbb{C}[t]_{(t)}$. Then $\mathfrak{m} = (t)$ and $\mathfrak{m}^k/\mathfrak{m}^{k+1}$ is one-dimensional, generated by t^k.

26.10 Example. Consider $R = \mathbb{C}[t^2, t^3]_{(t^2,t^3)}$, the local ring of $y^2 = x^3$ at zero. Then $\mathfrak{m}^n$ is generated by $t^{2n}, t^{2n+1}, \dots$. $\mathfrak{m}^{n+1}$ is generated by $t^{2n+2}, t^{2n+3}, \dots$. So the quotients all have dimension two. The dimension of these quotients is a little larger than we expected, but they don't grow.

26.11 Example. Consider $R = \mathbb{C}[x, y]_{(x,y)}$. Then $\mathfrak{m}^k$ is generated by polynomials homogeneous in degree k. So $\mathfrak{m}^k/\mathfrak{m}^{k+1}$ has dimensions that *grow* in k. This is a genuinely two-dimensional example.

This is the difference that we want to quantify to be the dimension.

26.12 Proposition. *Let $(R, \mathfrak{m})$ be a local noetherian ring. Then there exists a polynomial $f \in \mathbb{Q}[t]$ such that*

$$\ell(R/\mathfrak{m}^n) = \sum_{i=0}^{n-1} \dim \mathfrak{m}^i/\mathfrak{m}^{i+1} = f(n) \quad \forall n \gg 0.$$

Moreover, $\deg f \leq \dim \mathfrak{m}/\mathfrak{m}^2$.

Note that this polynomial is well-defined, as any two polynomials agreeing for large n coincide. Note also that $R/\mathfrak{m}^n$ is artinian so of finite length, and that we have used the fact that the length is additive for short exact sequences. We would have liked to write $\dim R/\mathfrak{m}^n$, but we can't, in general, so we use the substitute of the length.

Based on this, we define

26.13 Definition. The **dimension** of R is the degree of the polynomial f above.

26.14 Example. Consider $R = \mathbb{C}[x_1, \dots, x_n]_{(x_1, \dots, x_n)}$. What is the polynomial f above? Well, $R/\mathfrak{m}^k$ looks like the set of polynomials of degree $< k$ in $\mathbb{C}$. The dimension as a vector space is given by some binomial coefficient $\binom{n+k-1}{n}$. This is a polynomial in k of degree n. So R is n-dimensional. Which is what we wanted.

26.15 Example. Let R be a DVR. Then $\mathfrak{m}^k/\mathfrak{m}^{k+1}$ is of length one for each k. So $R/\mathfrak{m}^k$ has length k. Thus we can take $f(t) = t$ so R has dimension one.

Now we have to prove the proposition, i.e. that there is always such a polynomial.

Proof. Let $S = \bigoplus_n \mathfrak{m}^n/\mathfrak{m}^{n+1}$. Then S has a natural grading, and in fact it is a graded ring in a natural way from the map

$$\mathfrak{m}^{n_1} \times \mathfrak{m}^{n_2} \to \mathfrak{m}^{n_1+n_2}.$$

(It is the associated graded ring of the $\mathfrak{m}$-adic filtration.) Note that $S_0 = R/\mathfrak{m}$ is a field.

Choose n generators $x_1, \dots, x_n \in \mathfrak{m}$, where n is what we called the embedding dimension of R. So these n generators give generators of S_1 as an S_0-vector space. In fact, they generate S as an S_0-algebra because S is generated by degree one terms over S_0. So S is a graded quotient of the polynomial ring $\kappa[t_1, \dots, t_n]$ for $\kappa = R/\mathfrak{m}$. Note that $\ell(R/\mathfrak{m}^a) = \dim_\kappa(S_0) + \dots + \dim_\kappa(S_{a-1})$ for any a, thanks to the filtration.

It will now suffice to prove the following more general proposition.

26.16 Proposition. *Let M be any finitely generated graded module over the polynomial ring $\kappa[x_1, \dots, x_n]$. Then there exists a polynomial $f_M \in \mathbb{Q}[t]$ of degree $\leq n$, such that*

$$f_M(t) = \sum_{s \leq t} \dim M_s \quad t \gg 0.$$

Applying this to $M = S$ will give the desired result. We can forget about everything else, and look at this problem over graded polynomial rings.

This function is called the **Hilbert function**.

Proof. Note that if we have an exact sequence of gaded modules over the polynomial ring,

$$0 \to M' \to M \to M'' \to 0,$$

and $f_{M'}, f_{M''}$ exist as polynomials, then f_M exists and

$$f_M = f_{M'} + f_{M''}.$$

This is obvious from the definitions. We will induct on n.

If $n = 0$, then M is a finite-dimensional graded vector space over κ, and the grading must be concentrated in finitely many degrees. Thus the result is evident as $f_M(t)$ will just equal $\dim M$ (which will be the appropriate dimension for $t \gg 0$).

Suppose $n > 0$. Let x be one of the variables $x_1, \dots, x_n$. Then consider

$$0 \subset \ker(x : M \to M) \subset \ker(x^2 : M \to M) \subset \dots.$$

This must stabilize by noetherianness at some $M' \subset M$. Each of the quotients $\ker(x^i)/\ker(x^{i+1})$ is a finitely generated module over $\kappa[x_1, \dots, x_n]/(x)$, which is a smaller polynomial ring. So each of these subquotients $\ker(x^i)/\ker(x^{i+1})$ has a Hilbert function of degree $\leq n-1$.

Thus M' has a Hilbert function which is the sum of the Hilbert functions of these subquotients. In particular, $f_{M'}$ exists. If we show that $f_{M/M'}$ exists, then f_M necessarily exists. So we might as well show that the Hilbert function f_M exists when x is a non-zerodivisor on M.

We are out of time, so next time we will finish the proof. ▲

▲

Lecture 27
10/29

We started last time talking about the dimension theory about local noetherian rings.

§1 Hilbert polynomials

Last time, we were in the middle of the proof of a lemma.

Suppose $S = k[x_1, \dots, x_n]$ is a polynomial ring over a field k. It is a graded ring; the m-th graded piece is the set of polynomials homogeneous of degree m. Let M be a finitely generated graded S-module.

27.1 Definition. The **Hilbert function** H_M of M is defined via $H_M(m) = \dim_k M_m$. This is always finite for M a finitely generated graded S-module, as M is a quotient of copies of S (or twisted pieces).

Similarly, we define

$$H_M^+(m) = \sum_{m' \leq m} H_M(m').$$

This measures the dimension of $\deg m$ and below.

What we were proving last time was that:

27.2 Proposition. *There exist polynomials $f_M(t), f_M^+(t) \in \mathbb{Q}[t]$ such that $f_M(t) = H_M(t)$ and $f_M^+(t) = H_M^+(t)$ for sufficiently large t. Moreover,* $\deg f_M \leq n-1, \deg f_M^+ \leq n$.

In other words, the Hilbert functions eventually become polynomials.

These polynomials don't generally have integer coefficients, but they are close, as they take integer values at large values. In fact, they take integer values everywhere.

Remark. A function $f : \mathbb{Z} \to \mathbb{Z}$ is polynomial iff

$$f(t) = \sum_n c_n \binom{t}{n}, \quad c_n \in \mathbb{Z}.$$

So f is a $\mathbb{Z}$-linear function of binomial coefficients.

Proof. Note that the set $\left\{\binom{t}{n}\right\}$ forms a basis for the set of polynomials, that is $\mathbb{Q}[t]$. It is clear that $f(t)$ can be written as $\sum c_n\binom{t}{n}$ for the $c_n \in \mathbb{Q}$. By looking at the function $\Delta f(t) = f(t) - f(t-1)$ (which takes values in $\mathbb{Z}$) and the fact that $\Delta\binom{t}{n} = \binom{t}{n-1}$, it is easy to see that the $c_n \in \mathbb{Z}$ by induction on the degree. It is also easy to see that the binomial coefficients take values in $\mathbb{Z}$. ▲

Remark. The same remark applies if f is polynomial and $f(t) \in \mathbb{Z}$ for $t \gg 0$, by the same argument. It follows that $f(t) \in \mathbb{Z}$ for all t.

Let us now prove the proposition.

Proof. I claim, first, that the polynomiality of $H_M(t)$ (for t large) is equivalent to that of $H_M^+(t)$ (for t large). This is because H_M is the successive difference of H_M^+, i.e. $H_M(t) = H_M^+(t) - H_M^+(t-1)$. Similarly

$$H_M^+(t) = \sum_{t' \leq t} H_M(t),$$

and the successive sums of a polynomial form a polynomial.

So if f_M exists as in the proposition, then f_M^+ exists. Let us now show that f_M exists. Moreover, we will show that f_M has degree $\leq n-1$, which will prove the result, since f_M^+ has degree one higher.

Induction on n. When $n = 0$, this is trivial, since $H_M(t) = 0$ for $t \gg 0$. In the general case, we reduced to the case of M having no x_1-torsion. The argument for this reduction can be found in the previous lecture.

So M has a filtration

$$M \supset x_1 M \supset x_1^2 M \supset \dots$$

which is an exhaustive filtration of M in that nothing can be divisible by powers of x_1 over and over, for considerations of degree. Multiplication by x_1 raises the degree by one. This states that $\bigcap x_1^m M = 0$.

Let $N = M/x_1M \simeq x_1^m M / x_1^{m+1} M$ since $M \xrightarrow{x_1} M$ is injective. Now N is a graded module over $k[x_2, \dots, x_n]$, and by the inductive hypothesis on n So there is a polynomial f_N^+ of degree $\leq n-1$ such that

$$f_N^+(t) = \sum_{t' \leq t} \dim N_{t'}, \quad t \gg 0.$$

Let's look at M_t, which has a finite filtration

$$M_t \supset (x_1 M)_t \supset (x_1^2 M)_t \supset \dots$$

which has successive quotients that are the graded pieces of $N \simeq M/x_1M \simeq x_1M/x_1^2M \simeq \dots$ in dimensions $t, t-1, \dots$. We find that

$$(x_1^2 M)_t / (x_1^3 M)_t \simeq N_{t-2},$$

for instance. We find that

$$\dim M_t = \dim N_t + \dim N_{t-1} + \dots$$

which implies that $f_M(t)$ exists and coincides with f_N^+. ▲

§2 Back to dimension theory

27.3 Example. Let R be a local noetherian ring with maximal ideal $\mathfrak{m}$. Then we have the module $M = \bigoplus \mathfrak{m}_1^k/\mathfrak{m}_1^{k+1}$ over the ring $(R/\mathfrak{m})[x_1, \dots, x_n]$ where $x_1, \dots, x_n$ are generators of $\mathfrak{m}$.

The upshot is that

$$f_M^+(t) = \ell(R/\mathfrak{m}^t), \quad t \gg 0.$$

This is a polynomial of degree $\leq n$.

27.4 Definition. The **dimension** of R is the degree of f_M^+.

Remark. As we have seen, the dimension is at most the number of gnerators of $\mathfrak{m}$. So the dimension is at most the embedding dimension.

27.5 Definition. If R is local noetherian, N a finite R-module, define

$$M = \bigoplus \mathfrak{m}^a N/\mathfrak{m}^{a+1}N,$$

which is a module over the associated graded ring $\bigoplus \mathfrak{m}^a/\mathfrak{m}^{a+1}$, which in turn is a quotient of a polynomial ring. It too has a Hilbert polynomial. We say that the **dimension of** N is the degree of the Hilbert polynomial f_M^+. Evaluated at $t \gg 0$, this gives the length $\ell(N/\mathfrak{m}^t N)$.

27.6 Proposition. $\dim R$ *is the same as* $\dim R/\mathrm{Rad}R$*.*

I.e., the dimension doesn't change when you kill off nilpotent elements, which is what you would expect, as nilpotents don't affect $\mathrm{Spec}(R)$.

Proof. For this, we need a little more information about Hilbert functions. We thus digress substantially.

27.7 Proposition. *Suppose we have an exact sequence*

$$0 \to M' \to M \to M'' \to 0$$

of gaded modules over a polynomial ring $k[x_1, \dots, x_n]$*. Then*

$$f_M(t) = f_{M'}(t) + f_{M''}(t), \quad f_M^+(t) = f_{M'}^+(t) + f_{M''}^+(t).$$

As a result, $\deg f_M = \max \deg f_{M'}, \deg f_{M''}$*.*

Proof. The first part is obvious as the dimension is additive on vector spaces. The second part follows because Hilbert functions have nonnegative leading coefficients. ▲

In particular,

27.8 Corollary. *Say we have an exact sequence*

$$0 \to N' \to N \to N'' \to 0$$

of finite R*-modules. Then* $\dim N = \max(\dim N', \dim N'')$*.*

Proof. We have an exact sequence

$$0 \to K \to N/\mathfrak{m}^t N \to N''/\mathfrak{m}^t N'' \to 0$$

where K is the kernel. Here $K = (N' + \mathfrak{m}^t N)/\mathfrak{m}^t N = N'/(N' \cap \mathfrak{m}^t N)$. This is not quite $N'/\mathfrak{m}^t N'$, but it's pretty close. We have a surjection

$$N'/\mathfrak{m}^t N \twoheadrightarrow N'/(N' \cap \mathfrak{m}^t N) = K.$$

In particular,

$$\ell(K) \leq \ell(N'/\mathfrak{m}^t N').$$

On the other hand, we have the Artin-Rees lemma, which gives an inequality in the opposite direction. We have a containment

$$\mathfrak{m}^t N' \subset N' \cap \mathfrak{m}^t N \subset \mathfrak{m}^{t-c} N'$$

for some c. This implies that $\ell(K) \geq \ell(N'/\mathfrak{m}^{t-c} N')$.

Define $M = \bigoplus \mathfrak{m}^t N/\mathfrak{m}^{t+1} N$, and define M', M'' similarly in terms of N', N''. Then we have seen that

$$\boxed{f^+_M(t-c) \leq \ell(K) \leq f^+_M(t).}$$

We also know that the length of K plus the length of $N''/\mathfrak{m}^t N''$ is $f^+_M(t)$, i.e.

$$\ell(K) + f^+_{M''}(t) = f^+_M(t).$$

Now the length of K is a polynomial in t which is pretty similar to $f^+_{M'}$, in that the leading coefficient is the same. So we have an approximate equality $f^+_{M'}(t) + f^+_{M''}(t) \simeq f^+_M(t)$. This implies the result since the degree of f^+_M is $\dim N$ (and similarly for the others). ▲

Finally, let us return to the claim about dimension and nilpotents. Let R be a local noetherian ring and $I = \mathrm{Rad}(R)$. Then I is a finite R-module. In particular, I is nilpotent, so $I^n = 0$ for $n \gg 0$. We will show that

$$\dim R/I = \dim R/I^2 = \dots$$

which will imply the result, as eventually the powers become zero.

In particular, we have to show for each k,

$$\dim R/I^k = \dim R/I^{k+1}.$$

There is an exact sequence

$$0 \to I^k/I^{k+1} \to R/I^{k+1} \to R/I^k \to 0.$$

The dimension of these rings is the same thing as the dimensions as R-modules. So we can use this short exact sequence of modules. By the previous result, we are reduced to showing that

$$\dim I^k/I^{k+1} \leq \dim R/I^k.$$

Well, note that I kills I^k/I^{k+1}. In particular, I^k/I^{k+1} is a finitely generated R/I^k-module. There is an exact sequence

$$\bigoplus_N R/I^k \to I^k/I^{k+1} \to 0$$

which implies that $\dim I^k/I^{k+1} \leq \dim \bigoplus_N R/I^k = \dim R/I^k$. ▲

27.9 Example. Let $\mathfrak{p} \subset \mathbb{C}[x_1, \dots, x_n]$ and let $R = (\mathbb{C}[x_1, \dots, x_n]/\mathfrak{p})_{\mathfrak{m}}$ for some maximal ideal $\mathfrak{m}$. What is $\dim R$? What does dimension mean for coordinate rings over $\mathbb{C}$?

Recall by the Noether normalization theorem that there exists a polynomial ring $\mathbb{C}[y_1, \dots, y_m]$ contained in $S = \mathbb{C}[x_1, \dots, x_n]/\mathfrak{p}$ and S is a finite integral extension over this polynomial ring. We claim that

$$\dim R = m.$$

There is not sufficient time for that today.

Lecture 28
11/1

Last time, we were talking about the dimension theory of local noetherian rings.

§1 Recap

Let $(R, \mathfrak{m})$ be a local noetherian ring. Let M be a finitely generated R-module. We defined the **Hilbert polynomial** of M to be the polynomial which evaluates at $t \gg 0$ to $\ell(M/\mathfrak{m}^t M)$. We proved last time that such a polynomial always exists, and called its degree the **dimension of** M. More accurately, we shall start calling it $\dim \mathrm{supp} M$.

Recall that $\mathrm{supp} M = \{\mathfrak{p} : M_{\mathfrak{p}} \neq 0\}$. To make sense of this, we must show:

28.1 Proposition. $\dim M$ *depends only on* $\mathrm{supp} M$*.*

In fact, we shall show:

28.2 Proposition. $\dim M = \max_{\mathfrak{p} \in \mathrm{supp} M} \dim R/\mathfrak{p}$*.*

Proof. There is a finite filtration

$$0 = M_0 \subset M_1 \subset \cdots \subset M_m = M,$$

such that each of the successive quotients is isomorphic to $R/\mathfrak{p}_i$ for some prime ideal $\mathfrak{p}_i$. But if you have a short exact sequence of modules, the dimension in the middle is the maximum of the dimensions at the two ends. Iterating this, we see that the dimension of M is the sup of the dimension of the successive quotients. But the $\mathfrak{p}_i$'s that occur are all in $\mathrm{supp} M$, so we find

$$\dim M = \max_{\mathfrak{p}_i} R/\mathfrak{p}_i \leq \max_{\mathfrak{p} \in \mathrm{supp} M} \dim R/\mathfrak{p}.$$

We must show the reverse inequality. But fix any prime $\mathfrak{p} \in \mathrm{supp}M$. Then $M_{\mathfrak{p}} \neq 0$, so one of the $R/\mathfrak{p}_i$ localized at $\mathfrak{p}$ must be nonzero, as localization is an exact functor. Thus $\mathfrak{p}$ must contain some $\mathfrak{p}_i$. So $R/\mathfrak{p}$ is a quotient of $R/\mathfrak{p}_i$. In particular,

$$\dim R/\mathfrak{p} \leq \dim R/\mathfrak{p}_i.$$

▲

Having proved this, we throw out the notation $\dim M$, and henceforth write instead $\dim \mathrm{supp}M$.

§2 The dimension of an affine ring

Last time, we made a claim. If R is a domain and a finite module over a polynomial ring $k[x_1, \dots, x_n]$, then $R_{\mathfrak{m}}$ for any maximal $\mathfrak{m} \subset R$ has dimension n. This connects the dimension with the transcendence degree.

First, let us talk about finite extensions of rings. Let R be a commutative ring and let $R \to R'$ be a morphism that makes R' a finitely generated R-module (in particular, integral over R). Let $\mathfrak{m}' \subset R'$ be maximal. Let $\mathfrak{m}$ be the pull-back to R, which is also maximal (as $R \to R'$ is integral). Let M be a finitely generated R'-module, hence also a finitely generated R-module.

We can look at $M_{\mathfrak{m}}$ as an $R_{\mathfrak{m}}$-module or $M_{\mathfrak{m}'}$ as an $R'_{\mathfrak{m}'}$-module. Either of these will be finitely generated.

28.3 Proposition. $\dim \mathrm{supp}M_{\mathfrak{m}} \geq \dim \mathrm{supp}M_{\mathfrak{m}'}$.

Here $M_{\mathfrak{m}}$ is an $R_{\mathfrak{m}}$-module, $M_{\mathfrak{m}'}$ is an $R'_{\mathfrak{m}'}$-module.

Proof. Consider $R/\mathfrak{m} \to R'/\mathfrak{m}R' \to R'/\mathfrak{m}'$. Then we see that $R'/\mathfrak{m}R'$ is a finite $R/\mathfrak{m}$-module, so a finite-dimensional $R/\mathfrak{m}$-vector space. In particular, $R'/\mathfrak{m}R'$ is of finite length as an $R/\mathfrak{m}$-module, in particular an artinian ring. It is thus a product of local artinian rings. These artinian rings are the localizations of $R'/\mathfrak{m}R'$ at ideals of R' lying over $\mathfrak{m}$. One of these ideals is $\mathfrak{m}'$. So in particular

$$R'/\mathfrak{m}R \simeq R'/\mathfrak{m}' \times \text{other factors}.$$

The nilradical of an artinian ring being nilpotent, we see that $\mathfrak{m}'^c R'_{\mathfrak{m}'} \subset \mathfrak{m}R'_{\mathfrak{m}}$ for some c.

OK, I'm not following this—too tired. Will pick this up someday. ▲

28.4 Proposition. $\dim \mathrm{supp}M_{\mathfrak{m}} = \max_{\mathfrak{m}'|\mathfrak{m}} \dim \mathrm{supp}M_{\mathfrak{m}'}$.

This means $\mathfrak{m}'$ lies over $\mathfrak{m}$.

Proof. Done similarly, using artinian techniques. I'm kind of tired. ▲

28.5 Example. Let $R' = \mathbb{C}[x_1, \dots, x_n]/\mathfrak{p}$. Noether normalization says that there exists a finite injective map $\mathbb{C}[y_1, \dots, y_a] \to R'$. The claim is that

$$\dim R'_{\mathfrak{m}} = a$$

for any maximal ideal $\mathfrak{m} \subset R'$. We are set up to prove a slightly weaker definition. In particular (see below for the definition of the dimension of a non-local ring), by the proposition, we find the weaker claim

$$\dim R' = a,$$

as the dimension of a polynomial ring $\mathbb{C}[y_1, \dots, y_a]$ is a. (**I don't think we have proved this yet.**)

§3 Dimension in general

28.6 Definition. If R is a noetherian ring, we define $\dim(R) = \sup_{\mathfrak{p}} R_{\mathfrak{p}}$ for $\mathfrak{p} \in \mathrm{Spec}(R)$ maximal. This may be infinite. The localizations can grow arbitrarily large in dimension, but these examples are kind of pathological.

§4 A topological characterization

We now want a topological characterization of dimension. So, first, we want to study how dimension changes as we do things to a module. Let M be a finitely generated R-module over a local noetherian ring R. Let $x \in \mathfrak{m}$ for $\mathfrak{m}$ as the maximal ideal. You might ask

> What is the relation between $\dim \mathrm{supp} M$ and $\dim \mathrm{supp} M/xM$?

Well, M surjects onto M/xM, so we have the inequality $\geq$. But we think of dimension as describing the number of parameters you need to describe something. The number of parameters shouldn't change too much with going from M to M/xM. Indeed, as one can check,

$$\mathrm{supp} M/xM = \mathrm{supp} M \cap V(x)$$

and intersecting $\mathrm{supp} M$ with the "hypersurface" $V(x)$ should shrink the dimension by one.

We thus make:

Prediction.

$$\dim \mathrm{supp} M/xM = \dim \mathrm{supp} M - 1.$$

Obviously this is not always true, e.g. if x acts by zero on M. But we want to rule that out. Under reasonable cases, in fact, the prediction is correct:

28.7 Proposition. *Suppose $x \in \mathfrak{m}$ is a nonzerodivisor on M. Then*

$$\dim \mathrm{supp} M/xM = \dim \mathrm{supp} M - 1.$$

Proof. To see this, we look at Hilbert polynomials. Let us consider the exact sequence

$$0 \to xM \to M \to M/xM \to 0$$

which leads to an exact sequence for each t,

$$0 \to xM/(xM \cap \mathfrak{m}^t M) \to M/\mathfrak{m}^t M \to M/(xM + \mathfrak{m}^t M) \to 0.$$

For t large, the lengths of these things are given by Hilbert polynomials, as the thing on the right is $M/xM \otimes_R R/\mathfrak{m}^t$. We have

$$f_M^+(t) = f_{M/xM}^+(t) + \ell(xM/(xM \cap \mathfrak{m}^t M), \quad t \gg 0.$$

In particular, $\ell(xM/(xM \cap \mathfrak{m}^t M))$ is a polynomial in t. What can we say about it? Well, $xM \simeq M$ as x is a nonzerodivisor. In particular

$$xM/(xM \cap \mathfrak{m}^t M) \simeq M/N_t$$

where

$$N_t = \left\{ a \in M : xa \in \mathfrak{m}^t M \right\}.$$

In particular, $N_t \supset \mathfrak{m}^{t-1}M$. This tells us that $\ell(M/N_t) \leq \ell(M/\mathfrak{m}^{t-1}M) = f_M^+(t-1)$ for $t \gg 0$. Combining this with the above information, we learn that

$$f_M^+(t) \leq f_{M/xM}^+(t) + f_M^+(t-1),$$

which implies that $f_{M/xM}^+(t)$ is at least the successive difference $f_M^+(t) - f_M^+(t-1)$. This last polynomial has degree $\dim \operatorname{supp} M - 1$. In particular, $f_{M/xM}^+(t)$ has degree at least $\dim \operatorname{supp} M - 1$. This gives us one direction, actually the hard one. We showed that intersecting something with codimension one doesn't drive the dimension down too much.

Let us now do the other direction. We essentially did this last time via the Artin-Rees lemma. We know that $N_t = \left\{ a \in M : xa \in \mathfrak{m}^t \right\}$. The Artin-Rees lemma tells us that there is a constant c such that $N_{t+c} \subset \mathfrak{m}^t M$ for all t. Therefore, $\ell(M/N_{t+c}) \geq \ell(M/\mathfrak{m}^t M) = f_M^+(t), t \gg 0$. Now remember the exact sequence $0 \to M/N_t \to M/\mathfrak{m}^t M \to M/(xM + \mathfrak{m}^t M) \to 0$. We see from this that

$$\ell(M/\mathfrak{m}^t M) = \ell(M/N_t) + f_{M/xM}^+(t) \geq f_M^+(t-c) + f_{M/xM}^+(t), \quad t \gg 0,$$

which implies that

$$f_{M/xM}^+(t) \leq f_M^+(t) - f_M^+(t-c),$$

so the degree must go down. And we find that $\deg f_{M/xM}^+ < \deg f_M^+$. ▲

This gives us an algorithm of computing the dimension of an R-module M. First, it reduces to computing $\dim R/\mathfrak{p}$ for $\mathfrak{p} \subset R$ a prime ideal. We may assume that R is a domain and that we are looking for $\dim R$. Geometrically, this corresponds to taking an irreducible component of $\operatorname{Spec} R$.

Now choose any $x \in R$ such that x is nonzero but noninvertible. If there is no such element, then R is a field and has dimension zero. Then compute $\dim R/x$ (recursively) and add one.

Notice that this algorithm said nothing about Hilbert polynomials, and only talked about the structure of prime ideals.

Lecture 29
11/3

§1 Recap

Last time, we were talking about dimension theory. Recall that R is a local noetherian ring with maximal ideal $\mathfrak{m}$, M a finitely generated R-module. We can look at the lengths $\ell(M/\mathfrak{m}^t M)$ for varying t; for $t \gg 0$ this is a polynomial function. The degree of this polynomial is called the **dimension** of supp$M$.

Remark. If $M = 0$, then we define $\dim \mathrm{supp} M = -1$ by convention.

Last time, we showed that if $M \neq 0$ and $x \in \mathfrak{m}$ such that x is a nonzerodivisor on M (i.e. $M \overset{x}{\to} M$ injective), then

$$\boxed{\dim \mathrm{supp} M/xM = \dim \mathrm{supp} M - 1.}$$

Using this, we could give a recursion for calculating the dimension. To compute $\dim R = \dim \mathrm{Spec} R$, we note three properties:

1. $\dim R = \sup_{\mathfrak{p} \text{ a minimal prime}} R/\mathfrak{p}$. Intuitively, this says that a variety which is the union of irreducible components has dimension equal to the maximum of these irreducibles.
2. $\dim R = 0$ for R a field. This is obvious from the definitions.
3. If R is a domain, and $x \in \mathfrak{m} - \{0\}$, then $\dim R/(x) + 1 = \dim R$. This is obvious from the boxed formula as x is a nonzerodivisor.

These three properties *uniquely characterize* the dimension invariant.

More precisely, if $d : \{\text{local noetherian rings}\} \to \mathbb{Z}_{\geq 0}$ **satisfies the above three properties, then** $d = \dim$**.**

Proof. Induction on $\dim R$. It is clearly sufficient to prove this for R a domain. If R is a field, then it's clear; if $\dim R > 0$, the third condition lets us reduce to a case covered by the inductive hypothesis (i.e. go down). ▲

Let us rephrase 3 above:

3': If R is a domain and not a field, then

$$\dim R = \sup_{x \in \mathfrak{m} - 0} \dim R/(x) + 1.$$

Obviously 3' implies 3, and it is clear by the same argument that 1,2, 3' characterize the notion of dimension.

§2 Another notion of dimension

We shall now define another notion of dimension, and show that it is equivalent to the older one by showing that it satisfies these axioms.

29.1 Definition. Let R be a commutative ring. A **chain of prime ideals** in R is a finite sequence

$$\mathfrak{p}_0 \subsetneq \mathfrak{p}_1 \subsetneq \cdots \subsetneq \mathfrak{p}_n.$$

This chain is said to have **length** n**.**

29.2 Definition. The **Krull dimension** of R is equal to the maximum length of any chain of prime ideals. This might be ∞, but we will soon see this cannot happen for R local and noetherian.

Remark. For any maximal chain $\{\mathfrak{p}_i, 0 \leq i \leq n\}$ of primes (i.e. which can't be expanded), we must have that $\mathfrak{p}_0$ is minimal prime and $\mathfrak{p}_n$ a maximal ideal.

29.3 Theorem. *For a noetherian local ring R, the Krull dimension of R exists and is equal to the usual* $\dim R$*.*

Proof. We will show that the Krull dimension satisfies the above axioms. For now, write Krdim for Krull dimension.

1. First, note that $\mathrm{Krdim}(R) = \max_{\mathfrak{p} \in R \text{ minimal}} \mathrm{Krdim}(R/\mathfrak{p})$. This is because any chain of prime ideals in R contains a minimal prime. So any chain of prime ideals in R can be viewed as a chain in *some* $R/\mathfrak{p}$, and conversely.

2. Second, we need to check that $\mathrm{Krdim}(R) = 0$ for R a field. This is obvious, as there is precisely one prime ideal.

3. The third condition is interesting. We must check that for $(R, \mathfrak{m})$ a local domain,

   $$\mathrm{Krdim}(R) = \max_{x \in \mathfrak{m} - \{0\}} \mathrm{Krdim}(R/(x)) + 1.$$

   If we prove this, we will have shown that condition 3' is satisfied by the Krull dimension. It will follow by the inductive argument above that $\mathrm{Krdim}(R) = \dim(R)$ for any R. There are two inequalities to prove. First, we must show

   $$\mathrm{Krdim}(R) \geq \mathrm{Krdim}(R/x) + 1, \quad \forall x \in \mathfrak{m} - 0.$$

   So suppose $k = \mathrm{Krdim}(R/x)$. We want to show that there is a chain of prime ideals of length $k+1$ in R. So say $\mathfrak{p}_0 \subsetneq \cdots \subsetneq \mathfrak{p}_k$ is a chain of length k in $R/(x)$. The inverse images in R give a proper chain of primes in R of length k, all of which contain (x) and thus properly contain 0. Thus adding zero will give a chain of primes in R of length $k+1$.

   Conversely, we want to show that if there is a chain of primes in R of length $k+1$, then there is a chain of length k in $R/(x)$ for some $x \in \mathfrak{m} - \{0\}$. Let us write the chain of length $k+1$:

   $$\mathfrak{q}_{-1} \subset \mathfrak{q}_0 \subsetneq \cdots \subsetneq \mathfrak{q}_k \subset R.$$

Now evidently $\mathfrak{q}_0$ contains some $x \in \mathfrak{m} - 0$. Then the chain $\mathfrak{q}_0 \subsetneq \cdots \subsetneq \mathfrak{q}_k$ can be identified with a chain in $R/(x)$ for this x. So for this x, we have that $\mathrm{Krdim} R \leq \sup \mathrm{Krdim} R/(x) + 1$.

▲

There is thus a combinatorial definition of definition.

Remark. Geometrically, let $X = \mathrm{Spec} R$ for R an affine ring over $\mathbb{C}$ (a polynomial ring mod some ideal). Then R has Krull dimension $\geq k$ iff there is a chain of irreducible subvarieties of X,

$$X_0 \supset X_1 \supset \cdots \supset X_k.$$

Remark (Warning!). Let R be a local noetherian ring of dimension k. This means that there is a chain of prime ideals of length k, and no longer chains. Thus there is a maximal chain whose length is k. However, not all maximal chains in $\mathrm{Spec} R$ have length k.

29.4 Example. Let $R = (\mathbb{C}[X, Y, Z]/(XY, XZ))_{(X,Y,Z)}$. It is left as an exercise to the reader to see that there are maximal chains of length not two.

There are more complicated local noetherian *domains* which have maximal chains of prime ideals not of the same length. These examples are not what you would encounter in daily experience, and are necessarily complicated. This cannot happen for finitely generated domains over a field.

29.5 Example. An easier way all maximal chains could fail to be of the same length is if $\mathrm{Spec} R$ has two components (in which case $R = R_0 \times R_1$ for rings R_0, R_1).

§3 Yet another definition

Let's start by thinking about the definition of a module. Recall that if $(R, \mathfrak{m})$ is a local noetherian ring and M a finitely generated R-module, and $x \in \mathfrak{m}$ is a nonzerodivisor on M, then

$$\dim \mathrm{supp} M/xM = \dim \mathrm{supp} M - 1.$$

Question. What if x is a zerodivisor?

This is not necessarily true (e.g. if $x \in \mathrm{Ann}(M)$). Nonetheless, we claim that even in this case:

29.6 Proposition. *For any $x \in \mathfrak{m}$,*

$$\boxed{\dim \mathrm{supp} M \geq \dim \mathrm{supp} M/xM \geq \dim \mathrm{supp} M - 1.}$$

The upper bound on $\dim M/xM$ is obvious as M/xM is a quotient of M. The lower bound is trickier.

Proof. Let $N = \{a \in M : x^n a = 0 \text{ for some } n\}$. We can construct an exact sequence

$$0 \to N \to M \to M/N \to 0.$$

Let $M'' = M/N$. Now x is a nonzerodivisor on M/N by construction. We claim that

$$0 \to N/xN \to M/xM \to M''/xM'' \to 0$$

is exact as well. For this we only need to see exactness at the beginning, i.e. injectivity of $N/xN \to M/xM$. So we need to show that if $a \in N$ and $a \in xM$, then $a \in xN$.

To see this, suppose $a = xb$ where $b \in M$. Then if $\phi : M \to M''$, then $\phi(b) \in M''$ is killed by x as $x\phi(b) = \phi(bx) = \phi(a)$. This means that $\phi(b) = 0$ as $M'' \overset{x}{\to} M''$ is injective. Thus $b \in N$ in fact. So $a \in xN$ in fact.

From the exactness, we see that (as x is a nonzerodivisor on M'')

$$\begin{aligned} \dim M/xM &= \max(\dim M''/xM'', \dim N/xN) \geq \max(\dim M'' - 1, \dim N) \\ &\geq \max(\dim M'', \dim N) - 1. \end{aligned}$$

The reason for the last claim is that $\mathrm{supp} N/xN = \mathrm{supp} N$ as N is x-torsion, and the dimension depends only on the support. But the thing on the right is just $\dim M - 1$. ▲

As a result, we find:

29.7 Proposition. $\dim \mathrm{supp} M$ *is the minimal integer* n *such that there exist elements* $x_1, \dots, x_n \in \mathfrak{m}$ *with* $M/(x_1, \dots, x_n)M$ *has finite length.*

Note that n always exists, since we can look at a bunch of gnerators of the maximal ideal, and $M/\mathfrak{m}M$ is a finite-dimensional vector space and is thus of finite length.

Proof. Induction on $\dim \mathrm{supp} M$. Note that $\dim \mathrm{supp}(M) = 0$ if and only if the Hilbert polynomial has degree zero, i.e. M has finite length or that $n = 0$ (n being defined as in the statement).

Suppose $\dim \mathrm{supp} M > 0$.

1. We first show that there are $x_1, \dots, x_{\dim M}$ with $M/(x_1, \dots, x_{\dim M})M$ have finite length. Let $M' \subset M$ be the maximal submodule having finite length. There is an exact sequence
$$0 \to M' \to M \to M'' \to 0$$
where $M'' = M/M'$ has no finite length submodules. In this case, we can basically ignore M', and replace M by M''. The reason is that modding out by M' doesn't affect either n or the dimension.

   So let us replace M with M'' and thereby assume that M has no finite length submodules. In particular, M does not contain a copy of $R/\mathfrak{m}$, i.e. $\mathfrak{m} \notin \mathrm{Ass}(M)$. By prime avoidance, this means that there is $x_1 \in \mathfrak{m}$ that acts as a nonzerodivisor on M. Thus
$$\dim M/x_1M = \dim M - 1.$$
The inductive hypothesis says that there are $x_2, \dots, x_{\dim M}$ with
$$(M/x_1M)/(x_2, \dots, x_{\dim M})(M/xM) \simeq M/(x_1, \dots, x_{\dim M})M$$
of finite length. This shows the claim.

2. Conversely, suppose that there $M/(x_1, \dots, x_n)M$ has finite length. Then we claim that $n \geq \dim M$. This follows because we had the previous result that modding out by a single element can chop off the dimension by at most 1. Recursively applying this, and using the fact that dim of a finite length module is zero, we find
$$0 = \dim M/(x_1, \dots, x_n)M \geq \dim M - n.$$

▲

29.8 Corollary. *Let $(R, \mathfrak{m})$ be a local noetherian ring. Then $\dim R$ is equal to the minimal n such that there exist $x_1, \dots, x_n \in R$ with $R/(x_1, \dots, x_n)R$ is artinian. Or, equivalently, such that $(x_1, \dots, x_n)$ contains a power of $\mathfrak{m}$.*

Remark. We manifestly have here that the dimension of R is at most the embedding dimension. Here, we're not worried about generating the maximal ideal, but simply something containing a power of it.

Lecture 30
11/5

We have been talking about dimension. Let R be a local noetherian ring with maximal ideal $\mathfrak{m}$. Then, as we have said in previous lectures, $\dim R$ can be characterized by:

1. The minimal n such that there is an n-primary ideal generated by n elements $x_1, \dots, x_n \in \mathfrak{m}$. That is, the closed point $\mathfrak{m}$ of Spec$R$ is cut out *set-theoretically* by the intersection $\bigcap V(x_i)$. This is one way of saying that the closed point can be defined by n parameters.

2. The *maximal* n such that there exists a chain of prime ideals
$$\mathfrak{p}_0 \subset \mathfrak{p}_1 \subset \dots \subset \mathfrak{p}_n.$$

3. The degree of the Hilbert polynomial $f^+(t)$, which equals $\ell(R/\mathfrak{m}^t)$ for $t \gg 0$.

§1 Consequences of the notion of dimension

Let R be a local noetherian ring. The following is now clear from what we have shown:

30.1 Theorem (Krull's Hauptidealsatz)**.** *R has dimension 1 if and only if there is a nonzerodivisor $x \in \mathfrak{m}$ such that $R/(x)$ is artinian.*

Remark. Let R be a domain. We said that a nonzero prime $\mathfrak{p} \subset R$ is **height one** if $\mathfrak{p}$ is minimal among the prime ideals containing some nonzero $x \in R$.

According to Krull's Hauptidealsatz, $\mathfrak{p}$ has height one **if and only if** $\dim R_{\mathfrak{p}} = 1$**.**

We can generalize the notion of $\mathfrak{p}$ as follows.

30.2 Definition. Let R be a noetherian ring (not necessarily local), and $\mathfrak{p} \in \mathrm{Spec} R$. Then we define the **height** of $\mathfrak{p}$, denoted height($\mathfrak{p}$), as $\dim R_{\mathfrak{p}}$. We know that this is the length of a maximal chain of primes in $R_{\mathfrak{p}}$. This is thus the maximal length of prime ideals of R,

$$\mathfrak{p}_0 \subset \cdots \subset \mathfrak{p}_n = \mathfrak{p}$$

that ends in $\mathfrak{p}$. This is the origin of the term "height."

Remark. Sometimes, the height is called the **codimension**. This corresponds to the codimension in $\mathrm{Spec} R$ of the corresponding irreducible closed subset of $\mathrm{Spec} R$.

§2 Further remarks

We can recast earlier notions in terms of dimension.

Remark. A noetherian ring has dimension zero if and only if R is artinian. Indeed, R has dimension zero iff all primes are maximal.

Remark. A noetherian domain has dimension zero iff it is a field. Indeed, in this case (0) is maximal.

Remark. R has dimension ≤ 1 if and only if every non-minimal prime of R is maximal. That is, there are no chains of length ≥ 2.

Remark. A (noetherian) domain R has dimension ≤ 1 iff every nonzero prime ideal is maximal.

In particular,

30.3 Proposition. *R is Dedekind iff it is a noetherian, integrally closed domain of dimension* 1.

§3 Change of rings

Let $f : R \to R'$ be a map of noetherian rings.

Question. What is the relationship between $\dim R$ and $\dim R'$?

A map f gives a map $\mathrm{Spec} R' \to \mathrm{Spec} R$, where $\mathrm{Spec} R'$ is the union of various fibers over the points of $\mathrm{Spec} R$. You might imagine that the dimension is the dimension of R plus the fiber dimension. This is sometimes true.

Now assume that R, R' are *local* with maximal ideals $\mathfrak{m}, \mathfrak{m}'$. Assume furthermore that f is local, i.e. $f(\mathfrak{m}) \subset \mathfrak{m}'$.

30.4 Theorem. $\dim R' \leq \dim R + \dim R'/\mathfrak{m}R'$. *Equality holds if $f : R \to R'$ is flat.*

Here $R'/\mathfrak{m}R'$ is to be interpreted as the "fiber" of $\mathrm{Spec} R'$ above $\mathfrak{m} \in \mathrm{Spec} R$. The fibers can behave weirdly as the basepoint varies in $\mathrm{Spec} R$, so we can't expect equality in general.

Remark. Let us review flatness as it has been a while. An R-module M is *flat* iff the operation of tensoring with M is an exact functor. The map $f : R \to R'$ is *flat* iff R' is a flat R-module. Since the construction of taking fibers is a tensor product (i.e. $R'/\mathfrak{m}R' = R' \otimes_R R/\mathfrak{m}$), perhaps the condition of flatness here is not as surprising as it might be.

Proof. Let us first prove the inequality. Say

$$\dim R = a,\ \dim R'/\mathfrak{m}R' = b.$$

We'd like to see that

$$\dim R' \leq a + b.$$

To do this, we need to find $a + b$ elements in the maximal ideal $\mathfrak{m}'$ that generate a $\mathfrak{m}'$-primary ideal of R'.

There are elements $x_1, \dots, x_a \in \mathfrak{m}$ that generate an $\mathfrak{m}$-primary ideal $I = (x_1, \dots, x_a)$ in R. There is a surjection $R'/IR' \twoheadrightarrow R'/\mathfrak{m}R'$. The kernel $\mathfrak{m}R'/IR'$ is nilpotent since I contains a power of $\mathfrak{m}$. We've seen that nilpotents *don't* affect the dimension. In particular,

$$\dim R'/IR' = \dim R'/\mathfrak{m}R' = b.$$

There are thus elements $y_1, \dots, y_b \in \mathfrak{m}'/IR'$ such that the ideal $J = (y_1, \dots, y_b) \subset R'/IR'$ is $\mathfrak{m}'/IR'$-primary. The inverse image of J in R', call it $\overline{J} \subset R'$, is $\mathfrak{m}'$-primary. However, $\overline{J}$ is generated by the $a + b$ elements

$$f(x_1), \dots, f(x_a), \overline{y_1}, \dots, \overline{y_b}$$

if the $\overline{y_i}$ lift y_i.

But we don't always have equality. Nonetheless, if all the fibers are similar, then we should expect that the dimension of the "total space" SpecR' is the dimension of the "base" Spec$R$ plus the "fiber" dimension Spec$R'/\mathfrak{m}R'$. *The precise condition of f flat articulates the condition that the fibers "behave well."* Why this is so is something of a mystery, for now. But for some evidence, take the present result about fiber dimension.

Anyway, let us now prove equality for flat R-algebras. As before, write $a = \dim R, b = \dim R'/\mathfrak{m}R'$. We'd like to show that

$$\dim R' \geq a + b.$$

By what has been shown, this will be enough. This is going to be tricky since we now need to give *lower bounds* on the dimension; finding a sequence $x_1, \dots, x_{a+b}$ such that the quotient $R/(x_1, \dots, x_{a+b})$ is artinian would bound *above* the dimension.

So our strategy will be to find a chain of primes of length $a+b$. Well, first we know that there are primes

$$\mathfrak{q}_0 \subset \mathfrak{q}_1 \subset \dots \subset \mathfrak{q}_b \subset R'/\mathfrak{m}R'.$$

Let $\overline{\mathfrak{q}_i}$ be the inverse images in R'. Then the $\overline{\mathfrak{q}_i}$ are a strictly ascending chain of primes in R' where $\overline{\mathfrak{q}_0}$ contains $\mathfrak{m}R'$. So we have a chain of length b; we need to extend this by additional terms.

Now $f^{-1}(\overline{\mathfrak{q}_0})$ contains $\mathfrak{m}$, hence is $\mathfrak{m}$. Since $\dim R = a$, there is a chain $\{\mathfrak{p}_i\}$ of prime ideals of length a going down from $f^{-1}(\overline{\mathfrak{q}_0}) = \mathfrak{m}$. We are now going to find primes $\mathfrak{p}'_i \subset R'$ forming a chain such that $f^{-1}(\mathfrak{p}'_i) = \mathfrak{p}_i$. In other words, we are going to *lift* the chain $\mathfrak{p}_i$ to SpecR'. We can do this at the first stage for $i = a$, where $\mathfrak{p}_a = \mathfrak{m}$ and we can set $\mathfrak{p}'_a = \overline{\mathfrak{q}_0}$. If we can indeed do this lifting, and catenate the chains $\overline{\mathfrak{q}_j}, \mathfrak{p}'_i$, then we will have a chain of the appropriate length.

We will proceed by descending induction. Assume that we have $\mathfrak{p}'_{i+1} \subset R'$ and $f^{-1}(\mathfrak{p}'_{i+1}) = \mathfrak{p}_{i+1} \subset R$. We want to find $\mathfrak{p}'_i \subset \mathfrak{p}'_{i+1}$ such that $f^{-1}(\mathfrak{p}'_i) = \mathfrak{p}_i$. The existence of that prime is a consequence of the following general fact.

30.5 Theorem (Going down)**.** *Let $f : R \to R'$ be a flat map of noetherian commutative rings. Suppose $\mathfrak{q} \in$ SpecR', and let $\mathfrak{p} = f^{-1}(\mathfrak{q})$. Suppose $\mathfrak{p}_0 \subset \mathfrak{p}$ is a prime of R. Then there is a prime $\mathfrak{q}_0 \subset \mathfrak{q}$ with*

$$f^{-1}(\mathfrak{q}_0) = \mathfrak{p}_0.$$

Proof. We may replace R' with $R'_{\mathfrak{q}}$. There is still a map

$$R \to R'_{\mathfrak{q}}$$

which is flat as localization is flat. The maximal ideal in $R'_{\mathfrak{q}}$ has inverse image $\mathfrak{p}$. So the problem now reduces to finding *some* $\mathfrak{p}_0$ in the localization that pulls back appropriately.

Anyhow, throwing out the old R and replacing with the localization, we may assume that R' is local and $\mathfrak{q}$ the maximal ideal. (The condition $\mathfrak{q}_0 \subset \mathfrak{q}$ is now automatic.)

The claim now is that we can replace R with $R/\mathfrak{p}_0$ and R' with $R'/\mathfrak{p}_0 R' = R' \otimes R/\mathfrak{p}_0$. We can do this because base change preserves flatness (see below), and in this case we can reduce to the case of $\mathfrak{p}_0 = (0)$—in particular, R is a domain. Taking these quotients just replaces Spec$R$, SpecR' with closed subsets where all the action happens anyhow.

Under these replacements, we now have:

1. R' is local with maximal ideal $\mathfrak{q}$
2. R is a domain and $\mathfrak{p}_0 = (0)$.

We want a prime of R' that pulls back to (0) in R. I claim that any minimal prime of R' will work. Suppose otherwise. Let $\mathfrak{q}_0 \subset R'$ be a minimal prime, and suppose $x \in R \cap f^{-1}(\mathfrak{q}_0) - \{0\}$. But $\mathfrak{q}_0 \in \mathrm{Ass}(R')$. So $f(x)$ is a zerodivisor on R'. Thus multiplication by x on R' is not injective.

But, R is a domain, so $R \xrightarrow{x} R$ is injective. Tensoring with R' must preserve this, implying that $R' \xrightarrow{x} R'$ is injective because R' is flat. This is a contradiction. ▲

We used:

30.6 Lemma. *Let $R \to R'$ be a flat map, and S an R-algebra. Then $S \to S \otimes_R R'$ is a flat map.*

Proof. The construction of taking an S-module with $S \otimes_R R'$ is an exact functor, because that's the same thing as taking an S-module, restricting to R, and tensoring with R'. ▲

The proof of the fiber dimension theorem is now complete.

▲

We are done with the syllabus, and will now do "bonus" material.

Lecture 31
11/8

§1 Regular local rings

We have been talking about the dimension theory of local noetherian rings. If R is such a ring with maximal ideal $\mathfrak{m}$, then the *dimension* of R has been defined in several ways. One of these ways is that $\dim(R)$ is the minimum $n \in \mathbb{Z}_{\geq 0}$ such that there are n elements $x_1, \dots, x_n \in \mathfrak{m}$ such that $R/(x_1, \dots, x_n)$ is an artinian ring. If these n elements were to generate $\mathfrak{m}$, then we'd get not only an artinian ring, but in fact a field.

Let $k = R/\mathfrak{m}$.

31.1 Proposition. *For any noetherian local ring R,* $\dim(R) \leq \dim_k \mathfrak{m}/\mathfrak{m}^2$.

Proof. Indeed, $\dim_k \mathfrak{m}/\mathfrak{m}^2$ is, by Nakayama, the smallest number of generators for $\mathfrak{m}$. So this vector-space dimension is the *embedding dimension* defined earlier. ▲

31.2 Definition. R is **regular** if $\dim(R) = \dim_k \mathfrak{m}/\mathfrak{m}^2$. Alternatively, R is regular if $\mathfrak{m}$ can be generated by $\dim(R)$ elements.

§2 A bunch of examples

31.3 Example. If $\dim(R) = 0$, i.e. R is artinian, then R is regular iff the maximal ideal is zero, i.e. if R is a field.

31.4 Example. If $\dim(R) = 1$, then it is regular iff $\mathfrak{m}$ is principal. In a noetherian local ring, the maximal ideal is principal iff R is a DVR. This is *likely* already proved in these notes.

We find:

31.5 Proposition. *A one-dimensional regular local ring is the same thing as a DVR.*

31.6 Example. Let R be be the coordinate ring $\mathbb{C}[x_1, \dots, x_n]/I$ of an algebraic variety. Let $\mathfrak{m}$ be a maximal ideal corresponding to the origin. Then $\mathrm{MaxSpec} R \subset \mathrm{Spec} R$ is a subvariety of $\mathbb{C}^n$, and 0 is in this subvariety.

Then I claim:

31.7 Proposition. $R_{\mathfrak{m}}$ *is regular iff* $\mathrm{MaxSpec} R$ *is a smooth submanifold near* 0.

Proof. We will show that regularity implies smoothness. The other direction is omitted.

We have a surjection $\mathbb{C}[x_1, \dots, x_n] \twoheadrightarrow R$, with kernel I. There is a maximal ideal $\mathfrak{m}' \subset \mathbb{C}[x_1, \dots, x_n]$ defined as $(x_1, \dots, x_n)$. Then we have a surjection

$$\mathfrak{m}'/\mathfrak{m}'^2 \twoheadrightarrow \mathfrak{m}/\mathfrak{m}^2$$

whose kernel is $I + \mathfrak{m}'^2/\mathfrak{m}'^2$. We find that

$$\mathfrak{m}/\mathfrak{m}^2 = \mathfrak{m}'/(I + \mathfrak{m}'^2).$$

Note that $\mathbb{C}[x_1, \dots, x_n]_{\mathfrak{m}'}$ is a regular local ring of dimension n.

The first claim is that $R_{\mathfrak{m}}$ is regular if and only if, after localizing the polynomial ring at the maximal ideal $\mathfrak{m}'$, the ideal I is generated by $n - \dim(R)$ functions having linearly independent derivatives. Granting this claim, say $I_{\mathfrak{m}'}$ is generated by elements $f_1, \dots, f_m \in I$; then there is a map

$$\mathbb{C}^n \overset{(f_1,\dots,f_m)}{\to} \mathbb{C}^m$$

which is a submersion at the origin as the derivatives ∇f_i are linearly independent at the origin. The implicit function theorem tells us that the inverse image of zero, i.e. $\mathrm{MaxSpec} R$, is locally a submanifold.

Now we need to verify the claim made earlier. Namely, we will show that regularity of R implies that $I_{\mathfrak{m}}$ is generated by elements whose derivatives are linearly independent. However, we will postpone this until next time. ▲

§3 Regular local rings look alike

So, as we've seen, regularity corresponds to smoothness. Complex analytically, all smooth points are the same though—they're locally manifolds. We'd like an algebraic version of this. The vague claim is that all regular local rings of the same dimension "look alike."

Let $(R, \mathfrak{m})$ be a noetherian local ring. Consider the graded ring

$$S = R/\mathfrak{m} \oplus \mathfrak{m}/\mathfrak{m}^2 \oplus \dots.$$

If we write $k = R/\mathfrak{m}$ be the residue field, it is easy to see that this is a finitely generated k-algebra. If we choose elements $x_1, \dots, x_n \in \mathfrak{m}/\mathfrak{m}^2$ generating this vector space, then they generate S as an algebra.

31.8 Proposition. *R is regular if and only if S is isomorphic to the polynomial ring $k[x_1, \dots, x_n]$, i.e. for every $f \in k[x_1, \dots, x_n]$, if f maps to zero in S, then $f = 0$.*

Proof. Suppose first that $k[x_1, \dots, x_n] \twoheadrightarrow S$ isn't injective. Then there exists a $f \neq 0$ in this polynomial ring which maps to zero in S. Then S is not just a quotient of this polynomial ring, but a quotient of $k[x_1, \dots, x_n]/(f) \twoheadrightarrow S$. As this is a map of gaded rings, we can assume that f is homogeneous.

In particular, the Hilbert function of S is less than or equal to the Hilbert function of $k[x_1, \dots, x_n]/(f)$. In particular, the degree of the Hilbert function of S, namely the dimension of R, is at most the degree of the Hilbert function of this quotient—and quotienting by f will reduce the degree of the Hilbert function so that it is $< n$. So $\dim(R) < n$.

If S is isomorphic to a polynomial ring, then we can just read off what the Hilbert function of R will be, and we find that its degree is n. ▲

As we have seen, regularity is equivalent to a statement about the associated graded of R. Now we would like to transfer this to statements about things closer to R.

Assume now for simplicity that the residue field of $k = R/\mathfrak{m}$ maps back into R. This is always true in complex algebraic geometry, as the residue field is just $\mathbb{C}$.

Choose generators $y_1, \dots, y_m \in \mathfrak{m}$ where $n = \dim_k \mathfrak{m}/\mathfrak{m}^2$ is the embedding dimension. We get a map in the other direction

$$\phi : k[y_1, \dots, y_m] \to R$$

thanks to the section $k \to R$. This map from the polynomial ring is maybe not an isomorphism, but if we let $\mathfrak{m} \subset R$ be the maximal ideal, and $\mathfrak{n} = (y_1, \dots, y_m)$, the maps on associated gradeds will be the same.

We find, by the previous result:

31.9 Proposition. *R is regular iff ϕ induces an isomorphism on the associated graded, i.e. if $\mathfrak{n}^t/\mathfrak{n}^{t+1} \to \mathfrak{m}^t/\mathfrak{m}^{t+1}$ is an isomorphism.*

That is, ϕ induces an isomorphism

$$k[y_1, \dots, y_m]/\mathfrak{n}^t \simeq R/\mathfrak{m}^t$$

for all t, because it is an isomorphism on the associated graded level. So this in turn is equivalent, upon taking inverse limits, to the statement that ϕ induces an isomorphism

$$k[[y_1, \dots, y_m]] \to \hat{R}$$

at the level of completions.

We can now conclude:

31.10 Theorem. *Let R be a regular local ring of dimension m. Suppose R contains a copy of its residue field k.*[21] *Then $\hat{R} \simeq k[[x_1, \dots, x_m]]$.*

Let us now state this informally. First, note that:

31.11 Proposition. *For any local noetherian ring R, we have* $\dim(R) = \dim(\hat{R})$.

Proof. Immediate from the expression of dimension via Hilbert polynomials. ▲

On a similar note, the *embedding dimension* of R is the same as that of the completion, because $\mathfrak{m}/\mathfrak{m}^2$ is regular. So:

31.12 Proposition. *R is regular local iff $\hat{R}$ is regular local.*

Finally:

31.13 Corollary. *A complete noetherian regular local ring that contains a copy of its residue field k is a power series ring over k.*

It now makes sense to say:

> **All *complete* regular local rings of the same dimension look alike.** (More precisely, this is true when R is assumed to contain a copy of its residue field, but this is not a strong assumption in practice. One can show that this will be satisfied if R contains *any* field.[22])

We won't get into the precise statement of the general structure theorem, when the ring is not assumed to contain its residue field, but a safe intuition to take away from this is the above bolded statement.

[21] I.e. there is a section of the map $R \twoheadrightarrow R/\mathfrak{m}$.

[22] This is not always satisfied—take the p-adic integers, for instance.

§4 Regular local rings are domains

Here is one nice property of regular local rings.

31.14 Proposition. *If R is a regular local (noetherian, as always) ring, then R is a domain.*

Geometrically, this is saying that smooth points are locally irreducible.

Proof. Say $xy = 0$ in R. We want to prove that one of x, y is zero. Let us invoke the Krull intersection theorem, which states that $(0) = \bigcap \mathfrak{m}^i$. Then if $x \neq 0$, $x \in \mathfrak{m}^t - \mathfrak{m}^{t+1}$ for some t. Same for y, if it is not zero: we can choose $y \in \mathfrak{m}^u - \mathfrak{m}^{u+1}$. Then x, y correspond to elements $\overline{x}, \overline{y}$ in the associated graded ring (in the tth and uth pieces) which are nonzero. Their product is nonzero in the associated graded ring because that is a polynomial ring, hence a domain. So $\overline{xy} \neq 0$ in $\mathfrak{m}^{s+t}/\mathfrak{m}^{s+t+1}$.

Thus $xy \neq 0$, contradiction.

▲

Later we will prove much more. In fact, a regular local ring is a factorial ring. This is something we're not ready to prove yet, but one consequence of that will be the following algebro-geometric fact. Let $X = \mathrm{Spec}\mathbb{C}[X_1, \dots, X_n]/I$ for some ideal I; so X is basically a subset of $\mathbb{C}^n$ plus some nonclosed points. Then if X is smooth, we find that $\mathbb{C}[X_1, \dots, X_n]/I$ is locally factorial. Indeed, smoothness implies regularity, hence local factoriality. The whole apparatus of Weil and Cartier divisors now kicks in.

Lecture 32
11/10

§1 Regularity and algebraic geometry

We were talking about the theory of regular local rings. Recall an assertion made last time.

Take the ring $\mathbb{C}[X_1, \dots, X_n]$, and $\mathfrak{m} = (X_1, \dots, X_n)$ the maximal ideal at zero. Let $R = (\mathbb{C}[X_1, \dots, X_n]_{\mathfrak{m}})/I$ for some ideal I. Let $\phi : \mathbb{C}[X_1, \dots, X_n] \to R$ be the canonical map. The maximal ideal $\mathfrak{n}$ of R is generated by $\phi(\mathfrak{m})$.

Last time, we claimed:

32.1 Proposition. *R is regular local iff I is generated by functions $f_1, \dots, f_m$ which have linearly independent derivatives at zero.*

Proof. Let's first think about what the condition of having linearly independent derivatives means.

If we consider $\mathbb{C}[X_1, \dots, X_n]/\mathfrak{m}$, this is isomorphic to $\mathbb{C}$, the isomorphism being given by evaluation at zero. Now $\mathfrak{m}/\mathfrak{m}^2 = \mathbb{C}^n$ having a basis given by the images of $X_1, \dots, X_n$. A more canonical way of describing this is as the **cotangent space** of $\mathbb{C}^n$ at the origin. The idea is that any polynomial f corresponds to the 1-form $df = \sum \frac{\partial f}{\partial X_i} dX_i$. The evaluation of this 1-form at the origin gives a formal linear combination of the symbols dX_i. It is easy to see that $df|_0$ vanishes if f is constant or is in $\mathfrak{m}^2$. Restricting to $\mathfrak{m}$, we get a map

$$\mathfrak{m}/\mathfrak{m}^2 \to \mathbb{C}^n, \quad f \to df|_0,$$

which is obviously an isomorphism.

Consider $f_1, \dots, f_a \in \mathfrak{m}$. We have seen that *the derivatives (or gradients) are linearly independent at the origin iff the images of $f_1, \dots, f_a$ are linearly independent in $\mathfrak{m}/\mathfrak{m}^2$.*

If we consider $\mathbb{C}[X_1, \dots, X_n]_{\mathfrak{m}}$, last time we mentioned that it was a regular local ring. The result will now follow from

32.2 Lemma. *Let R be a quotient of a regular local ring S, say $R = S/I$ for some I. Let $\mathfrak{m} \subset S$ be the maximal ideal. Then R is regular iff I is generated by elements $f_1, \dots, f_a$ which are linearly independent in $\mathfrak{m}/\mathfrak{m}^2$.*

Proof. First, the easy direction. Say $I = (f_1, \dots, f_a)$ where $f_1, \dots, f_a$ are linearly independent in $\mathfrak{m}/\mathfrak{m}^2$. S is regular, so the dimension is equal to the embedding dimension of S. We want to show the same thing for R.

Now $\dim R = \dim S/(f_1, \dots, f_a)$. We would expect that the dimension drops by a; we can't immediately conclude this, but at least can argue that

$$\dim R \geq \dim S - a$$

by the principal ideal theorem. Let now $\mathfrak{n} \subset R$ be the maximal ideal. The embedding dimension of R is the dimension of $\mathfrak{n}/\mathfrak{n}^2 \simeq \mathfrak{m}/(I + \mathfrak{m}^2)$. This is a quotient of $\mathfrak{m}/\mathfrak{m}^2$, so its dimension is the dimension of $\mathfrak{m}/\mathfrak{m}^2$ minus the image of I in $\mathfrak{m}/\mathfrak{m}^2$. This is precisely the embedding dimension of S minus a, i.e. $\dim S - a$. We learn that

$$\dim R \geq \dim S - a = \text{embedding } \dim R,$$

which implies that R is local, as the converse implication is true in any noetherian local ring.

Now we want to do the converse. Say that R is regular of dimension $\dim S - a$. We want to find elements $f_1, \dots, f_a$. So far, we know that the embedding dimension of R is equal to the embedding dimension of S minus a. In particular,

$$\dim \mathfrak{n}/\mathfrak{n}^2 = \dim \mathfrak{m}/(\mathfrak{m}^2 + I) = \dim \mathfrak{m}/\mathfrak{m}^2 - a.$$

We can choose $f_1, \dots, f_a \in I$ such that their images in $\mathfrak{m}/\mathfrak{m}^2$ are a basis for the image of I. We have maps

$$S \twoheadrightarrow S/(f_1, \dots, f_a) \twoheadrightarrow S/I = R.$$

What can we say about the intermediate ring $R' = S/(f_1, \dots, f_a)$? It is obtained from a regular local ring by killing elements linearly independent in $\mathfrak{m}/\mathfrak{m}^2$. In particular, R' is regular local of dimension $\dim(S) - a$.

We want to prove that $I = (f_1, \dots, f_a)$, i.e. $R = R'$. Suppose not. Then $R = R'/J$ for some ideal $J \neq 0$. Choose any $x \in J$ which is not zero. Then x is a nonzerodivisor on R' because R' is regular. In particular, $R'/(x)$ has dimension $\dim R' - 1$. Since R is a quotient of this, we have that $\dim R < \dim R' = \dim S - a$. This is a contradiction from our earlier assumptions. ▲

▲

The upshot of this is that in algebraic geometry, regularity has something to do with smoothness.

Remark (Warning)**.** This argument proves that if $R \simeq K[x_1, \dots, x_n]/I$ for K algebraically closed, then $R_{\mathfrak{m}}$ is regular local for some maximal ideal $\mathfrak{m}$ if the corresponding algebraic variety is smooth at the corresponding point. We proved this in the special case $K = \mathbb{C}$ and $\mathfrak{m}$ the ideal of the origin.

If K is not algebraically closed, we **can't assume** that any maximal ideal corresponds to a point in the usual sense. Moreover, if K is not perfect, regularity does **not** imply smoothness. We have not quite defined smoothness, but here's a definition: smoothness means that the local ring you get by base-changing K to the algebraic closure is regular. So what this means is that regularity of affine rings over a field K is not preserved under base-change from K to $\overline{K}$.

32.3 Example. Let K be non-perfect of characteristic p. Let a not have a pth root. Consider $K[x]/(x^p - a)$. This is a regular local ring of dimension zero, i.e. is a field. If K is replaced by its algebraic closure, then we get $\overline{K}[x]/(x^p - a)$, which is $\overline{K}[x]/(x - a^{1/p})^p$. This is still zero-dimensional but is not a field. Over the algebraic closure, the ring fails to be regular.

§2 Derivations and Kähler differentials

Let R be a ring with the maximal ideal $\mathfrak{m}$. Then there is a $R/\mathfrak{m}$-vector space $\mathfrak{m}/\mathfrak{m}^2$. This is what we would like to think of as the "**cotangent space**" of Spec$R$ at $\mathfrak{m}$. Intuitively, the cotangent space is what you get by differentiating functions which vanish at the point, but differentiating functions that vanish twice should give zero. This is the moral justification.

A goal might be to generalize this. What if you wanted to think about all points at once? We'd like to describe the "cotangent bundle" to Spec$R$ in an analogous way. Let's try and describe what would be a section to this cotangent bundle. Morally, a section of $\Omega^*_{\mathrm{Spec} R}$ should be the same thing as a "1-form" on Spec$R$. We don't know what a 1-form is yet, but at least we can give some examples. If $f \in R$, then f is a "function" on Spec$R$, and its "differential" should be a 1-form. So there should be a "*df*" which should be a 1-form.

We should expect the rules $d(f + g) = df + dg$ and $d(fg) = f(dg) + g(df)$ as the usual rules of differentiation. For this to make sense, 1-forms should be an R-module.

32.4 Definition. Let R be a commutative ring, M an R-module. A **derivation** from R to M is a map $D : R \to M$ such that the two identities

$$D(f + g) = Df + Dg$$

and

$$D(fg) = f(Dg) + g(Df)$$

hold.

These equations make sense as M is an R-module.

Whatever a 1-form might be, there should be a derivation

$$R \to \{1 - \text{forms}\}.$$

An idea would be to *define* the 1-forms or the "cotangent bundle" Ω_R by a universal property. It should be universal among R-modules with a derivation.

To make this precise:

32.5 Proposition. *There is an R-module Ω_R and a derivation $d_{\text{univ}} : R \to \Omega_R$ satisfying the following universal property. For all R-modules M, there is a canonical isomorphism*

$$\operatorname{Hom}_R(\Omega_R, M) \simeq \operatorname{Der}(R, M)$$

given by composing the universal d_{univ} with a map $\Omega_R \to M$.

That is, any derivation $d : R \to M$ factors through this universal derivation in a unique way. Given $d : R \to M$, we can make the following diagram commutative in a natural way:

$$\begin{tikzcd}
R \arrow[r, "d"] \arrow[d, "d_{\text{univ}}"] & M \\
\Omega_R \arrow[ur] &
\end{tikzcd}$$

32.6 Definition. Ω_R is called the module of **Kähler differentials** of R.

Let us now verify this proposition.

Proof. This is like the verification of the tensor product. Namely, build a free gadget and quotient out by whatever you need.

Let Ω_R be the quotient of the free R-module generated by elements da for $a \in R$ by enforcing the relations

1. $d(a + b) = da + db$.
2. $d(ab) = adb + bda$.

By construction, the map $a \to da$ is a derivation $R \to \Omega_R$. It is easy to see that is universal. Given a derivation $d : R \to M$, we get a map $\Omega_R \to M$ sending $da \to d(a), a \in R$. ▲

We are going to need a slight variant.

§3 Relative differentials

32.7 Definition. Let $f : R \to R'$ be a ring-homomorphism. Let M be an R'-module. A derivation $d : R' \to M$ is R-**linear if** $d(f(a)) = 0, a \in R$**.** This is equivalent to saying that d is an R-homomorphism by the Leibniz rule.

32.8 Proposition. *There is a universal R-linear derivation $R' \overset{d_{\text{univ}}}{\to} \Omega_{R'/R}$.*

Proof. Use the same construction as in the absolute case. We get a map $R' \to \Omega_{R'}$ as before. This is not generally R-linear, so you have to quotient out by the images of $d(f(b)), b \in R$. ▲

Remark. We see that $\Omega_{R'/R}$ as in the proposition is obtained by killing the images of $d(f(b)), b \in R$.

32.9 Definition. This is called the module of **relative Kähler differentials.**

32.10 Theorem. *There is a canonical exact sequence of R'-modules*

$$R' \otimes_R \Omega_R \to \Omega_{R'} \to \Omega_{R'/R} \to 0.$$

This is generally not exact on the left.

Proof. This follows from the remark. ▲

§4 Examples

Let us do some examples to make this more concrete.

32.11 Example. Let $R' = \mathbb{C}[x_1, \dots, x_n], R = \mathbb{C}$. In this case, the claim is that there is an isomorphism

$$\Omega_{R'/R} \simeq R'^n.$$

More precisely, $\Omega_{R'/R}$ is free on $dx_1, \dots, dx_n$. So the cotangent bundle is "free."

Proof. The construction $f \to \left(\frac{\partial f}{\partial x_i}\right)$ gives a map $R' \to R'^n$. By elementary calculus, this is a derivation, even an R-linear derivation. We get a map

$$\phi : \Omega_{R'/R} \to R'^n$$

by the universal property of the Kähler differentials. The claim is that this map is an isomorphism. The map is characterized by sending df to $\left(\frac{\partial f}{\partial x_i}\right)$. Note that $dx_1, \dots, dx_n$ map to a basis of R'^n because differentiating x_i gives 1 at i and zero at $j \neq i$. So we see that ϕ is surjective.

There is a map $\psi : R'^n \to \Omega_{R'/R}$ sending (a_i) to $\sum a_i dx_i$. It is easy to check that $\phi \circ \psi = 1$ from the definition of ϕ. What we still need to show is that $\psi \circ \phi = 1$. Namely, for any f, we want to show that $\psi \circ \phi(df) = df$ for $f \in R'$. This is precisely the claim that $df = \sum \frac{\partial f}{\partial x_i} dx_i$. Both sides are additive in f, indeed are derivations, and coincide on monomials of degree one, so they are equal. ▲

Lecture 33
11/12

§1 Formal properties of Kähler differentials

So we were talking about Kähler differentials yesterday. Recall that if $\phi : A \to B$ is a map of rings, we can define a B-module

$\Omega_{B/A} =$ generated by $dx|_{x \in B} / \left\{d(x+y) = dx + dy, d(a) = 0 \ \forall a \in A, d(xy) = xdy + ydx\right\}.$

By construction, $\Omega_{B/A}$ is the receptacle from the universal A-linear derivation into a B-module.

Let $A \to B \to C$ be a map of rings. There is an obvious map $dx \to dx$

$$\Omega_{C/A} \to \Omega_{C/B}$$

where both sides have the same generators, except with a few additional relations on $\Omega_{C/B}$. We have to quotient by $db, b \in B$. In particular, there is a map $\Omega_{B/A} \to \Omega_{C/A}$, $dx \to dx$, whose images generates the kernel. This induces a map

$$C \otimes_B \Omega_{B/A} \to \Omega_{C/A}.$$

We have proved:

33.1 Proposition. *Given a sequence $A \to B \to C$ of rings, there is an exact sequence*

$$C \otimes_B \Omega_{B/A} \to \Omega_{C/A} \to \Omega_{C/B} \to 0.$$

Let us list another property. Last time, we showed:

33.2 Proposition. *If R is a ring, then*

$$\Omega_{R[x_1,\dots,x_n]/R} = R[x_1, \dots, x_n]^n.$$

Finally, let us look at the Kähler differentials for quotient rings. Let $A \to B$ be a homomorphism of rings and $I \subset B$ an ideal. We would like to describe $\Omega_{B/I/A}$. There is a map

$$\Omega_{B/A} \to \Omega_{B/I/A}$$

sending dx to $d\overline{x}$ for $\overline{x}$ the reduction of x in B/I. This is surjective on generators, so it is surjective. It is not injective, though. In $\Omega_{B/I/A}$, the generators dx, dx' are identified if $x \equiv x' \mod I$. Moreover, $\Omega_{B/I/A}$ is a B/I-module. This means that there will be additional relations for that. To remedy this, we can tensor and consider the morphism

$$\Omega_{B/A} \otimes_B B/I \to \Omega_{B/I/A} \to 0.$$

Let us now define a map

$$\phi : I/I^2 \to \Omega_{B/A} \otimes_B B/I,$$

which we claim will generate the kernel. Given $x \in I$, we define $\phi(x) = dx$. If $x \in I^2$, then $dx \in I\Omega_{B/A}$ so ϕ is indeed a map of abelian groups $I/I^2 \to \Omega_{B/A} \otimes_B B/I$. Let us check that this is a B/I-module homorphism. We would like to check that $\phi(xy) = y\phi(x)$ for $x \in I$ in $\Omega_{B/A}/I\Omega_{B/A}$. This follows from the Leibnitz rule, $\phi(xy) = y\phi(x) + xdy \equiv x\phi(x) \mod I\Omega_{B/A}$. So ϕ is also defined. Its image is the submodule of $\Omega_{B/A}/I\Omega_{B/A}$ generated by $dx, x \in I$. This is precisely what one has to quotient out by to get $\Omega_{B/I/A}$. In particular:

33.3 Proposition. *Let B be an A-algebra and $I \subset B$ an ideal. There is an exact sequence*

$$I/I^2 \to \Omega_{B/A} \otimes_B B/I \to \Omega_{B/I/A} \to 0.$$

These results will let us compute the module of Kähler differentials in cases we want.

33.4 Example. Let $B = A[x_1, \dots, x_n]/I$ for I an ideal. We will compute $\Omega_{B/A}$.

First, $\Omega_{A[x_1,\dots,x_n]/A} \otimes B \simeq B^n$ generated by symbols dx_i. There is a surjection of

$$B^n \to \Omega_{B/A} \to 0$$

whose kernel is generated by $dx, x \in I$, by the second exact sequence above. If $I = (f_1, \dots, f_m)$, then the kernel is generated by $\{df_i\}$. It follows that $\Omega_{B/A}$ is the cokernel of the map

$$B^m \to B^n$$

that sends the ith generator of B^m to df_i thought of as an element in the free B-module B^n on generators $dx_1, \dots, dx_n$. Here, thanks to the Leibnitz rule, df_i is given by formally differentiating the polynomial, i.e.

$$df_i = \sum_j \frac{\partial f_i}{\partial x_j} dx_j.$$

We have thus explicitly represented $\Omega_{B/A}$ as the cokernel of the matrix $\left(\frac{\partial f_i}{\partial x_j}\right)$.

Last time, we were talking about the connection of Kähler differentials and the cotangent bundle.

33.5 Example. Let $R = \mathbb{C}[x_1, \dots, x_n]/I$ be the coordinate ring of an algebraic variety. Let $\mathfrak{m} \subset R$ be the maximal ideal. Then $\Omega_{R/\mathbb{C}}$ is what you should think of as containing information of the cotangent bundle of Spec$R$. You might ask what the fiber over a point $\mathfrak{m} \in$ Spec$R$ is, though. That is, we might ask what

$$\Omega_{R/\mathbb{C}} \otimes_R R/\mathfrak{m}$$

is. To see this, we note that there are maps

$$\mathbb{C} \to R \to R/\mathfrak{m} \simeq \mathbb{C}.$$

There is now an exact sequence by our general properties

$$\mathfrak{m}/\mathfrak{m}^2 \to \Omega_{R/\mathbb{C}} \otimes_R R/\mathfrak{m} \to \Omega_{\mathbb{R}/\mathfrak{m}/\mathbb{C}} \to 0$$

where the last thing is zero as $R/\mathfrak{m} \simeq \mathbb{C}$ by the Nullstellensatz. The upshot is that $\Omega_{R/\mathbb{C}} \otimes_R R/\mathfrak{m}$ is a quotient of $\mathfrak{m}/\mathfrak{m}^2$. Let's leave it there for now.

§2 Kähler differentials for fields

Let us start with the simplest examples—fields.

33.6 Example. Let k be a field, k'/k an extension.

Question. What does $\Omega_{k'/k}$ look like? When does it vanish?

$\Omega_{k'/k}$ is a k'-vector space.

33.7 Proposition. *Let k'/k be a separable algebraic extension of fields. Then $\Omega_{k'/k} = 0$.*

Proof. We will need a formal property of Kähler differentials that is easy to check, namely that they are compatible with filtered colimits. If $B = \varinjlim B_\alpha$ for A-algebras B_α, then there is a canonical isomorphism

$$\Omega_{B/A} \simeq \varinjlim \Omega_{B_\alpha/A}.$$

One can check this on generators and relations, for instance.

Given this, we can reduce to the case of k'/k finite and separable.

Remark. Given a sequence of fields and morphisms $k \to k' \to k''$, then there is an exact sequence

$$\Omega_{k'/k} \otimes k'' \to \Omega_{k''/k} \to \Omega_{k''/k'} \to 0.$$

In particular, if $\Omega_{k'/k} = \Omega_{k''/k'} = 0$, then $\Omega_{k''/k} = 0$. This is a kind of dévissage argument.

Anyway, recall that we have a finite separable extension k'/k where $k' = k(x_1, \dots, x_n)$.[23] We will show that

$$\Omega_{k(x_1,\dots,x_i)/k(x_1,\dots,x_{i-1})} = 0 \quad \forall i,$$

which will imply by the devissage argument that $\Omega_{k'/k} = 0$. In particular, we are reduced to showing the proposition when k' is generated over k by a *single element* x. Then we have that

$$k' \simeq k[X]/(f(X))$$

for $f(X)$ an irreducible polynomial. Set $I = (f(X))$. We have an exact sequence

$$I/I^2 \to \Omega_{k[X]/k} \otimes_{k[X]} k' \to \Omega_{k'/k} \to 0$$

The middle term is a copy of k' and the first term is isomorphic to $k[X]/I \simeq k'$. So there is an exact sequence

$$k' \to k' \to \Omega_{k'/k} \to 0.$$

The first term is, as we have computed, multiplication by $f'(x)$; however this is nonzero by separability. Thus we find that $\Omega_{k'/k} = 0$. ▲

Remark. The above result is **not true** for inseparable extensions in general.

33.8 Example. Let k be an imperfect field of characteristic $p > 0$. There is $x \in k$ such that $x^{1/p} \notin k$, by definition. Let $k' = k(x^{1/p})$. As a ring, this looks like $k[t]/(t^p - x)$. In writing the exact sequence, we find that $\Omega_{k'/k} = k'$ as this is the cokernel of the map $k' \to k'$ given by multiplication $\frac{d}{dt}|_{x^{1/p}}(t^p - x)$. That polynomial has identically vanishing derivative, though. We find that a generator of $\Omega_{k'/k}$ is dt where t is a pth root of x, and $\Omega_{k'/k} \simeq k$.

[23] We can take $n = 1$ by the primitive element theorem, but shall not need this.

Now let us consider transcendental extensions. Let $k' = k(x_1, \dots, x_n)$ be a purely transcendental extension, i.e. the field of rational functions of $x_1, \dots, x_n$.

33.9 Proposition. *If $k' = k(x_1, \dots, x_n)$, then $\Omega_{k'/k}$ is a free k'-module on the generators dx_i.*

Proof. We already know this for the polynomial ring $k[x_1, \dots, x_n]$. However, the rational function field is just a localization of the polynomial ring at the zero ideal. So the result will follow from: ▲

33.10 Proposition. *Let $f : A \to B$ be a map of rings. Let $S \subset B$ be multiplicatively closed. Then the natural map*

$$S^{-1}\Omega_{B/A} \to \Omega_{S^{-1}B/A}$$

is an isomorphism.

So the formation of Kähler differentials commutes with localization.

Proof. We could prove this by the calculational definition, but perhaps it is better to prove it via the universal property. If M is any $S^{-1}B$-module, then we can look at

$$\mathrm{Hom}_{S^{-1}B}(\Omega_{S^{-1}B/A}, M)$$

which is given by the group of A-linear derivations $S^{-1}B \to M$, by the universal property.

On the other hand,

$$\mathrm{Hom}_{S^{-1}B}(S^{-1}\Omega_{B/A}, M)$$

is the same thing as the set of B-linear maps $\Omega_{B/A} \to M$, i.e. the set of A-linear derivations $B \to M$.

We want to show that these two are the same thing. Given an A-derivation $S^{-1}B \to M$, we get an A-derivation $B \to M$ by pulling back. We want to show that any A-linear derivation $B \to M$ arises in this way. So we need to show that any A-linear derivation $d : B \to M$ extends uniquely to an A-linear $\overline{d} : S^{-1}B \to M$. Here are two proofs:

1. (Lowbrow proof.) For $x/s \in S^{-1}B$, with $x \in B, s \in S$, we define $\overline{d}(x/s) = dx/s - xds/s^2$ as in calculus. The claim is that this works, and is the only thing that works. One should check this—**exercise**.

2. (Highbrow proof.) We start with a digression. Let B be a commutative ring, M a B-module. Consider $B \oplus M$, which is a B-module. We can make it into a ring (via **square zero multiplication**) by multiplying

$$(b, x)(b', x') = (bb', bx' + b'x).$$

This is compatible with the B-module structure on $M \subset B \oplus M$. Note that M is an ideal in this ring with square zero. Then the projection $\pi : B \oplus M \to B$ is a ring-homomorphism as well. There is also a ring-homomorphism in the other direction $b \to (b, 0)$, which is a section of π. There may be other homomorphisms $B \to B \oplus M$.

You might ask what all the right inverses to π are, i.e. ring-homomorphisms $\phi : B \to B \oplus M$ such that $\pi \circ \phi = 1_B$. This must be of the form $\phi : b \to (b, db)$ where $d : B \to M$ is some map. It is easy to check that ϕ is a homomorphism precisely when d is a derivation.

Suppose now $A \to B$ is a morphism of rings making B an A-algebra. Then $B \oplus M$ is an A-algebra via the inclusion $a \to (a, 0)$. Then you might ask when $\phi : b \to (b, db), B \to B \oplus M$ is an A-homomorphism. The answer is clear: when d is an A-derivation.

Recall that we were in the situation of $f : A \to B$ a morphism of rings, $S \subset B$ a multiplicatively closed subset, and M an $S^{-1}B$-module. The claim was that any A-linear derivation $d : B \to M$ extends uniquely to $\overline{d} : S^{-1}B \to M$. We can draw a diagram

$$\begin{tikzcd}
 & B \oplus M \arrow[r] \arrow[d] & S^{-1}B \oplus M \arrow[d] \\
A \arrow[r] & B \arrow[r] & S^{-1}B
\end{tikzcd}$$

This is a cartesian diagram. So given a section of A-algebras $B \to B \oplus M$, we have to construct a section of A-algebras $S^{-1}B \to S^{-1}B \oplus M$. We can do this by the universal property of localization, since S acts by invertible elements on $S^{-1}B \oplus M$. (To see this, note that S acts by invertible elements on $S^{-1}B$, and M is a nilpotent ideal.)

▲

Lecture 34
11/15

§1 Continuation of field theory

We have been talking about the theory of regular local rings, and more recently about Kähler differentials. Last time, we showed:

34.1 Proposition. *If L/K is a separable algebraic field extension, then $\Omega_{L/K} = 0$.*

Furthermore:

34.2 Proposition. *If L/K is a finitely generated purely transcendental extension $K(x_1, \dots, x_n)$, then*

$$\Omega_{L/K} = L^n = \bigoplus L dx_i.$$

More generally, this is true for an infinitely generated transcendental extension. In this case, $\Omega_{L/K}$ is a free vector space on a transcendence basis.

The only thing we did not already prove is the infinite case, which follows as Kähler differentials are compatible with filtered colimits.

We can deduce from this:

34.3 Corollary. *Let L/K be a field extension of fields of char 0. Then*

$$\dim_L \Omega_{L/K} = \operatorname{trdeg}(L/K).$$

Partial proof. Put the above two facts together. Choose a transcendence basis $\{x_\alpha\}$ for L/K. This means that L is algebraic over $K(\{x_\alpha\})$ and the $\{x_\alpha\}$ are algebraically independent. Moreover $L/K(\{x_\alpha\})$ is *separable* algebraic. Now let us use a few things about these cotangent complexes. There is an exact sequence:

$$\Omega_{K(\{x_\alpha\})} \otimes_{K(\{x_\alpha\})} L \to \Omega_{L/K} \to \Omega_{L/K(\{x_\alpha\})} \to 0$$

The last thing is zero, and we know what the first thing is; it's free on the dx_α. So we find that $\Omega_{L/K}$ is generated by the elements dx_α. If we knew that the dx_α were linearly independent, then we would be done. But we don't, yet. ▲

This is **not true** in characteristic p. If $L = K(\alpha^{1/p})$ for $\alpha \in K$ and $\alpha^{1/p} \notin K$, then $\Omega_{L/K} \neq 0$.

§2 Regularity, smoothness, and Kähler differentials

From this, let us revisit a statement made last time. Let K be an algebraically closed field, let $R = k[x_1, \dots, x_n]/I$ and let $\mathfrak{m} \subset R$ be a maximal ideal. Recall that the Nullstellensatz implies that $R/\mathfrak{m} \simeq k$. We were studying

$$\Omega_{R/k}.$$

This is an R-module, so $\Omega_{R/k} \otimes_R k$ makes sense. There is a surjection

$$\mathfrak{m}/\mathfrak{m}^2 \to \Omega_{R/k} \otimes_R k \to 0,$$

that sends $x \to dx$.

34.4 Proposition. *This map is an isomorphism.*

Proof. We construct a map going the other way. Call the map $\mathfrak{m}/\mathfrak{m}^2 \to \Omega_{R/k} \otimes_R k$ as ϕ. We want to construct

$$\psi : \Omega_{R/k} \otimes_R k \to \mathfrak{m}/\mathfrak{m}^2.$$

This is equivalent to giving an R-module map

$$\Omega_{R/k} \to \mathfrak{m}/\mathfrak{m}^2,$$

that is a derivation $\partial : R \to \mathfrak{m}/\mathfrak{m}^2$. This acts via $\partial(\lambda + x) = x$ for $\lambda \in k, x \in \mathfrak{m}$. Since $k + \mathfrak{m} = R$, this is indeed well-defined. We must check that ∂ is a derivation. That is, we have to compute $\partial((\lambda + x)(\lambda' + x'))$. But this is

$$\partial(\lambda\lambda' + (\lambda x' + \lambda' x) + xx').$$

The definition of ∂ is to ignore the constant term and look at the nonconstant term mod $\mathfrak{m}^2$. So this becomes

$$\lambda x' + \lambda' x = (\partial(\lambda + x))(x' + \lambda') + (\partial(\lambda' + x'))(x + \lambda)$$

because $xx' \in \mathfrak{m}^2$, and because $\mathfrak{m}$ acts trivially on $\mathfrak{m}/\mathfrak{m}^2$. Thus we get the map ψ in the inverse direction, and one checks that ϕ, ψ are inverses. This is because ϕ sends $x \to dx$ and ψ sends $dx \to x$. ▲

34.5 Corollary. *Let R be as before. Then $R_{\mathfrak{m}}$ is regular iff* $\dim R_{\mathfrak{m}} = \dim_k \Omega_{R/k} \otimes_R R/\mathfrak{m}$.

In particular, the modules of Kähler differentials detect regularity for certain rings.

34.6 Definition. Let R be a noetherian ring. We say that R is **regular** if $R_{\mathfrak{m}}$ is regular for every maximal ideal $\mathfrak{m}$. (This actually implies that $R_{\mathfrak{p}}$ is regular for all primes $\mathfrak{p}$, though we are not ready to see this. It will follow from the fact that the localization of a regular local ring at a prime ideal is regular.)

Let $R = k[x_1, \dots, x_n]/I$ be an affine ring over an algebraically closed field k. Then:

34.7 Proposition. *TFAE:*

1. *R is regular.*
2. *"R is smooth over k" (to be defined)*
3. *$\Omega_{R/k}$ is a projective module over R of rank* $\dim R$.

A finitely generated projective module is locally free. So the last statement is that $(\Omega_{R/k})_{\mathfrak{p}}$ is free of rank $\dim R$ for each prime $\mathfrak{p}$.

Remark. A projective module does not necessarily have a well-defined rank as an integer. For instance, if $R = R_1 \times R_2$ and $M = R_1 \times 0$, then M is a summand of R, hence is projective. But there are two candidates for what the rank should be. The problem is that Spec$R$ is disconnected into two pieces, and M is of rank one on one piece, and of rank zero on the other. But in this case, it does not happen.

Remark. The smoothness condition states that locally on Spec$R$, we have an isomorphism with $k[y_1, \dots, y_n]/(f_1, \dots, f_m)$ with the gradients ∇f_i linearly independent. Equivalently, if $R_{\mathfrak{m}}$ is the localization of R at a maximal ideal $\mathfrak{m}$, then $R_{\mathfrak{m}}$ is a regular local ring, as we have seen.

Proof. We have already seen that 1 and 2 are equivalent. The new thing is that they are equivalent to 3. First, assume 1 (or 2). First, note that $\Omega_{R/k}$ is a finitely generated R-module; that's a general observation:

34.8 Proposition. *If $f : A \to B$ is a map of rings that makes B a finitely generated A-algebra, then $\Omega_{B/A}$ is a finitely generated B-module.*

Proof. We've seen this is true for polynomial rings, and we can use the exact sequence. If B is a quotient of a polynomial ring, then $\Omega_{B/A}$ is a quotient of the Kähler differentials of the polynomial ring. ▲

Return to the main proof. In particular, $\Omega_{R/k}$ is projective if and only if $(\Omega_{R/k})_{\mathfrak{m}}$ is projective for every maximal ideal $\mathfrak{m}$. According to the second assertion, we have that $R_{\mathfrak{m}}$ looks like $(k[y_1, \dots, y_n]/(f_1, \dots, f_m))_{\mathfrak{n}}$ for some maximal ideal $\mathfrak{n}$, with the gradients ∇f_i linearly independent. Thus $(\Omega_{R/k})_{\mathfrak{m}} = \Omega_{R_{\mathfrak{m}}/k}$ looks like the cokernel of

$$R_{\mathfrak{m}}^m \to R_{\mathfrak{m}}^n$$

where the map is multiplication by the Jacobian matrix $\left(\frac{\partial f_i}{\partial y_j}\right)$. By assumption this matrix has full rank. We see that there is a left inverse of the reduced map $k^m \to k^n$. We can lift this to a map $R_{\mathfrak{m}}^n \to R_{\mathfrak{m}}^m$. Since this is a left inverse mod $\mathfrak{m}$, the composite is at least an isomorphism (looking at determinants). Anyway, we see that $\Omega_{R/k}$ is given by the cokernel of a map of free module that splits, hence is projective. The rank is $n - m = \dim R_{\mathfrak{m}}$.

Finally, let us prove that 3 implies 1. Suppose $\Omega_{R/k}$ is projective of rank $\dim R$. So this means that $\Omega_{R_{\mathfrak{m}}/k}$ is free of dimension $\dim R_{\mathfrak{m}}$. But this implies that $(\Omega_{R/k}) \otimes_R R/\mathfrak{m}$ is free of the appropriate rank, and that is—as we have seen already—the embedding dimension $\mathfrak{m}/\mathfrak{m}^2$. So if 3 holds, the embedding dimension equals the usual dimension, and we get regularity. ▲

34.9 Corollary. *Let $R = \mathbb{C}[x_1, \dots, x_n]/\mathfrak{p}$ for $\mathfrak{p}$ a prime. Then there is a nonzero $f \in R$ such that $R[f^{-1}]$ is regular.*

Geometrically, this says the following. Spec$R$ is some algebraic variety, and Spec$R[f^{-1}]$ is a Zariski open subset. What we are saying is that, in characteristic zero, any algebraic variety has a nonempty open smooth locus. The singular locus is always smaller than the entire variety.

Proof. $\Omega_{R/\mathbb{C}}$ is a finitely generated R-module. Let $K(R)$ be the fraction field of R. Now

$$\Omega_{R/\mathbb{C}} \otimes_R K(R) = \Omega_{K(R)/\mathbb{C}}$$

is a finite $K(R)$-vector space. The dimension is $\operatorname{trdeg}(K(R)/\mathbb{C})$. That is also $d = \dim R$, as we have seen. Choose elements $x_1, \dots, x_d \in \Omega_{R/\mathbb{C}}$ which form a basis for $\Omega_{K(R)/\mathbb{C}}$. There is a map

$$R^d \to \Omega_{R/\mathbb{C}}$$

which is an isomorphism after localization at (0). This implies that there is $f \in R$ such that the map is an isomorphism after localization at f.[24] We find that $\Omega_{R[f^{-1}]/\mathbb{C}}$ is free of rank d for some f, which is what we wanted. ▲

This argument works over any algebraically closed field of characteristic zero, or really any field of characteristic zero.

Remark (Warning)**.** Over imperfect fields in characteristic p, two things can happen:

1. Varieties need not be generically smooth
2. $\Omega_{R/k}$ can be projective with the wrong rank

(Nothing goes wrong for **algebraically closed fields** of characteristic p.)

34.10 Example. Here is a dumb example. Say $R = k[y]/(y^p - x)$ where $x \in K$ has no pth root. We know that $\Omega_{R/k}$ is free of rank one. However, the rank is wrong: the variety has dimension zero.

[24] There is an inverse defined over the fraction field, so it is defined over some localization.

Lecture 35
11/17

Last time, were trying to show that $\Omega_{L/K}$ is free on a transcendence basis if L/K is an extension in characteristic zero. So we had a tower of fields

$$K \to K' \to L,$$

where L/K' was separable algebraic. We claim in this case that

$$\Omega_{L/K} \simeq \Omega_{K'/K} \otimes_{K'} L.$$

This will prove the result. But we had not done this yesterday.

Proof. This doesn't follow directly from the previous calculations. Wlog, L is finite over K', and in particular, $L = K'[x]/(f(x))$ for f separable. The claim is that

$$\Omega_{L/K} \simeq (\Omega_{K'/K} \otimes_{K'} L \oplus K'dx)/f'(x)dx + \dots$$

When we kill the vector $f'(x)dx + \dots$, we kill the second component. ▲

§1 Basic definitions in homological algebra

We don't have time to do all the homological algebra we need to prove results such as the homological criterion for regularity.

35.1 Definition. Let R be a commutative ring, M an R-module. A **projective resolution** of M is an exact sequence of R-modules

$$\dots \to P_1 \to P_0 \to M \to 0$$

where all the P_i are projective modules.

35.2 Proposition. *These always exist.*

Proof. If you start with M, choose a surjection $P_0 \twoheadrightarrow M$ for some P_0 projective. E.g., P free on the elements of M. Choose a surjection from some projective P_1 onto the kernel of $P_0 \to M$. Then there is an exact sequence

$$P_1 \to P_0 \to M \to 0,$$

and we can iterate this procedure to get a projective resolution. ▲

Here is a useful observation:

35.3 Proposition. *If R is noetherian, and M is finitely generated, then we can choose a projective resolution where each P_i is finitely generated.*

Proof. To say that M is finitely generated is to say that it is a quotient of a free module on finitely many generators, so we can take P_0 free. The kernel of $P_0 \to M$ is finitely generated by noetherianness, and we can proceed as before, at each step choosing a finitely generated object. ▲

§2 Ext **functors**

Let M, M' be R-modules. Choose a projective resolution

$$\dots \to P_2 \to P_1 \to P_0 \to M \to 0$$

and consider what happens when you hom this resolution into M. Namely, we can consider $\mathrm{Hom}_R(M, N)$, which is the kernel of $\mathrm{Hom}(P_0, M) \to \mathrm{Hom}(P_1, M)$ by exactness of the sequence

$$0 \to \mathrm{Hom}_R(M, N) \to \mathrm{Hom}_R(P_0, N) \to \mathrm{Hom}_R(P_1, N).$$

You might try to continue this with the sequence

$$0 \to \mathrm{Hom}_R(M, N) \to \mathrm{Hom}_R(P_0, N) \to \mathrm{Hom}_R(P_1, N) \to \mathrm{Hom}_R(P_2, N) \to \dots.$$

In general, it won't be exact, because Hom_R is only left-exact. But it is a chain complex. You can thus consider the homologies.

35.4 Definition. The homology of the complex $\{\mathrm{Hom}_R(P_i, N)\}$ is denoted $\mathrm{Ext}^i_R(M, N)$. By definition, this is $\ker(\mathrm{Hom}(P_i, N) \to \mathrm{Hom}(P_{i+1}, N))/\mathrm{Im}(\mathrm{Hom}(P_{i-1}, N) \to \mathrm{Hom}(P_i, N))$. This is an R-module, and is called the ith ext group.

Let us list some properties:

35.5 Proposition. $\mathrm{Ext}^0_R(M, N) = \mathrm{Hom}_R(M, N)$.

Proof. This is obvious from the left-exactness of $\mathrm{Hom}(-, N)$. (We discussed this.) ▲

35.6 Proposition. $\mathrm{Ext}^i(M, N)$ *is a functor of* N.

Proof. Obvious from the definition. ▲

Here is a harder statement.

35.7 Proposition. $\mathrm{Ext}^i(M, N)$ *is well-defined, independent of the projective resolution* $P_* \to M$*, and is in fact a contravariant additive functor of* M.[25]

Proof. Omitted. We won't really need this, though; it requires more theory about chain complexes. ▲

35.8 Proposition. *If* M *is annihilated by some ideal* $I \subset R$*, then so is* $\mathrm{Ext}^i(M, N)$ *for each* i.

Proof. This is a consequence of the functoriality in M. If $x \in I$, then $x : M \to M$ is the zero map, so it induces the zero map on $\mathrm{Ext}^i(M, N)$. ▲

35.9 Proposition. $\mathrm{Ext}^i(M, N) = 0$ *if* M *projective and* $i > 0$.

[25] I.e. a map $M \to M'$ induces $\mathrm{Ext}^i(M', N) \to \mathrm{Ext}^i(M, N)$.

Proof. In that case, one can use the projective resolution

$$0 \to M \to M \to 0.$$

Computing Ext via this gives the result. ▲

35.10 Proposition. *If there is an exact sequence*

$$0 \to N' \to N \to N'' \to 0,$$

there is a long exact sequence of Ext *groups*

$$0 \to \mathrm{Hom}(M, N') \to \mathrm{Hom}(M, N) \to \mathrm{Hom}(M, N'') \to \mathrm{Ext}^1(M, N') \to \mathrm{Ext}^1(M, N) \to \dots$$

Proof. This proof will assume a little homological algebra. Choose a projective resolution $P_* \to M$. (The notation P_* means the chain complex $\cdots \to P_2 \to P_1 \to P_0$.) In general, homming out of M is not exact, but homming out of a projective module is exact. For each i, we get an exact sequence

$$0 \to \mathrm{Hom}_R(P_i, N') \to \mathrm{Hom}_R(P_i, N) \to \mathrm{Hom}_R(P_i, N'') \to 0,$$

which leads to an exact sequence of *chain complexes*

$$0 \to \mathrm{Hom}_R(P_*, N') \to \mathrm{Hom}_R(P_*, N) \to \mathrm{Hom}_R(P_*, N'') \to 0.$$

Taking the long exact sequence in homology gives the result. ▲

Much less obvious is:

35.11 Proposition. *There is a long exact sequence in the M variable. That is, a short exact sequence*

$$0 \to M' \to M \to M'' \to 0$$

leads a long exact sequence

$$0 \to \mathrm{Hom}_R(M'', N) \to \mathrm{Hom}_R(M, N) \to \mathrm{Hom}_R(M', N) \to \mathrm{Ext}^1(M'', N) \to \mathrm{Ext}^1(M, N) \to \dots.$$

Proof. Omitted. ▲

We now can characterize projectivity:

35.12 Corollary. *TFAE:*

1. *M is projective.*
2. $\mathrm{Ext}^i(M, N) = 0$ *for all R-modules N and $i > 0$.*
3. $\mathrm{Ext}^1(M, N) = 0$ *for all N.*

Proof. We have seen that 1 implies 2 because projective modules have simple projective resolutions. 2 obviously implies 3. Let's show that 3 implies 1. Choose a projective module P and a surjection $P \twoheadrightarrow M$ with kernel K. There is a short exact sequence $0 \to K \to P \to M \to 0$. The sequence

$$0 \to \mathrm{Hom}(M, K) \to \mathrm{Hom}(P, K) \to \mathrm{Hom}(K, K) \to \mathrm{Ext}^1(M, K) = 0$$

shows that there is a map $P \to K$ which restricts to the identity $K \to K$. The sequence $0 \to K \to P \to M \to 0$ thus splits, so M is a direct summand in a projective module, so is projective. ▲

§3 Injective modules

Finally, we note that there is another way of constructing Ext. We constructed them by choosing a projective resolution of M. But you can also do this by resolving N by *injective* modules.

35.13 Definition. An R-module Q is **injective** if $\mathrm{Hom}_R(-, Q)$ is an exact (or, equivalently, right-exact) functor. That is, if $M_0 \subset M$ is an inclusion of R-modules, then any map $M_0 \to Q$ can be extended to $M \to Q$.

35.14 Example. An abelian group is injective iff it is divisible. That is, Q is injective iff $n : Q \to Q$ is surjective for each $n \in \mathbb{Z} - \{0\}$. In particular, $\mathbb{Q}$ and $\mathbb{Q}/\mathbb{Z}$ are injective.

An important fact is that:

35.15 Proposition. *If N is an R-module, there is an injection*

$$0 \to N \to Q,$$

where Q is injective.

This is harder to see than the statement for projective modules. It is generally hard to give examples of injective modules.

Idea of proof. If N is injective, then we're done.

If not, there is an injection $M \hookrightarrow M_0$ and a map $f_0 : M_0 \to N$ that does not extend to M. Let $N' = N \oplus_{M_0} M$ be the push-out, i.e. $(N \oplus M)/M_0$ where the map $M_0 \to N \oplus M$ is by f_0 and the inclusion. By construction, we have an inclusion $N \to N'$, and from the push-out construction, the map $M_0 \to N$ extends to $M \to N'$.

The point is that N' "looks more injective" than N. Repeat this construction *many, many* times. Namely, if N' is injective, you're done; if not, there's some piece of evidence N' is not injective, and that piece of evidence lets you extend N'. The claim is that if you do it carefully, you eventually end up at an injective module.

▲

35.16 Corollary. *Injective resolutions of any N exist. For any N, there is an exact sequence*

$$0 \to N \to Q^0 \to Q^1 \to \dots$$

where all the Q_i are injective.

If we are given M, N, and an injective resolution $N \to Q_*$, we can look at the chain complex $\{\mathrm{Hom}(M, Q_i)\}$, i.e. the chain complex

$$0 \to \mathrm{Hom}(M, Q^0) \to \mathrm{Hom}(M, Q^1) \to \dots$$

and we can consider the cohomologies.

35.17 Definition. We call these cohomologies

$$\mathrm{Ext}^i_R(M, N)' = \ker(\mathrm{Hom}(M, Q^i) \to \mathrm{Hom}(M, Q^{i+1}))/\mathrm{Im}(\mathrm{Hom}(M, Q^{i-1}) \to \mathrm{Hom}(M, Q^i)).$$

This is dual to the previous definitions, and it is easy to check that the properties that we couldn't verify for the previous Exts are true for the Ext′'s.

Nonetheless:

35.18 Theorem. *There are canonical isomorphisms:*

$$\mathrm{Ext}^i(M,N)' \simeq \mathrm{Ext}^i(M,N).$$

In particular, to compute Ext groups, you are free either to take a projective resolution of M, or an injective resolution of N.

Idea of proof. In general, it might be a good idea to construct a third more complex construction that resembles both. Given M, N construct a projective resolution $P_* \to M$ and an injective resolution $N \to Q^*$. Having made these choices, we get a *double complex*

$$\mathrm{Hom}_R(P_i, Q^j)$$

of a whole lot of R-modules. The claim is that in such a situation, where you have a double complex C_{ij}, you can form an ordinary chain complex C' by adding along the diagonals. Namely, the nth term is $C'_n = \bigoplus_{i+j=n} C_{ij}$. This *total complex* will receive a map from the chain complex used to compute the Ext groups and a chain complex used to compute the Ext′ groups. There are maps on cohomology,

$$\mathrm{Ext}^i(M,N) \to H^i(C'_*), \quad \mathrm{Ext}^i(M,N)' \to H^i(C'_*).$$

The claim is that isomorphisms on cohomology will be induced in each case. That will prove the result, but we shall not prove the claim. ▲

Lecture 36
11/19

Last time we were talking about Ext groups over commutative rings. For R a commutative ring and M, N R-modules, we defined an R-module $\mathrm{Ext}^i(M,N)$ for each i, and proved various properties. We forgot to mention one.

36.1 Proposition. *If R noetherian, and M, N are finitely generated,* $\mathrm{Ext}^i(M,N)$ *is also finitely generated*

Proof. We can take a projective resolution P_* of M by finitely generated free modules, R being noetherian. Consequently the complex $\mathrm{Hom}(P_*, N)$ consists of finitely generated modules. Thus the cohomology is finitely generated, and this cohomology consists of the Ext groups. ▲

§1 Depth

Let $(R, \mathfrak{m})$ be a noetherian local ring. Let $k = R/\mathfrak{m}$.

Let $M \neq 0$ be a finitely generated R-module.

36.2 Definition. The **depth** of M is equal to the smallest integer i such that $\mathrm{Ext}^i(k, M) \neq 0$.

We'll give another characterization of this in just a minute. Note that contained in this definition is an assertion: that there is such an i.

36.3 Example. Depth zero is equivalent to saying that $\mathrm{Ext}^0(k, M) \neq 0$, i.e. there is a nontrivial morphism

$$k \to M.$$

As $k = R/\mathfrak{m}$, the existence of such a map is equivalent to the existence of a nonzero x such that $\mathrm{Ann}(x) = \mathfrak{m}$, i.e. $\mathfrak{m} \in \mathrm{Ass}(M)$. So depth zero is equivalent to having $\mathfrak{m} \in \mathrm{Ass}(M)$.

Suppose now that $\mathrm{depth}(M) \neq 0$. In particular, $\mathfrak{m} \notin \mathrm{Ass}(M)$. Since $\mathrm{Ass}(M)$ is finite, prime avoidance that $\mathfrak{m} \not\subset \bigcup_{\mathfrak{p} \in \mathrm{Ass}(M)} \mathfrak{p}$. Thus $\mathfrak{m}$ contains an element which is a nonzerodivisor on M. So we find:

36.4 Proposition. *M has depth zero iff every element in $\mathfrak{m}$ is a zerodivisor on M.*

Now suppose $\mathrm{depth} M \neq 0$. There is $a \in \mathfrak{m}$ which is a nonzerodivisor on M, i.e. such that there is an exact sequence

$$0 \to M \xrightarrow{a} M \to M/aM \to 0.$$

There is a long exact sequence in Ext groups:

$$\mathrm{Ext}^{i-1}(k, M) \to \mathrm{Ext}^i(k, M) \xrightarrow{a} \mathrm{Ext}^i(k, M) \to \mathrm{Ext}^i(k, M/aM) \to \mathrm{Ext}^{i+1}(k, M).$$

However, the map $a : \mathrm{Ext}^i(k, M) \to \mathrm{Ext}^i(k, M)$ as multiplication by a kills k. (As we said last time, if a kills a module N, then it kills $\mathrm{Ext}^*(N, M)$ for all M.) We see from this that

$$\mathrm{Ext}^i(k, M) \hookrightarrow \mathrm{Ext}^i(k, M/aM)$$

is injective, and

$$\mathrm{Ext}^{i-1}(k, M/aM) \twoheadrightarrow \mathrm{Ext}^i(k, M)$$

is surjective.

36.5 Corollary. *If $a \in \mathfrak{m}$ is a nonzerodivisor on M, then*

$$\mathrm{depth}(M/aM) = \mathrm{depth} M - 1.$$

Proof. When $\mathrm{depth} M = \infty$, this is easy (left to the reader) from the exact sequence. Suppose $\mathrm{depth}(M) = n$. We would like to see that $\mathrm{depth} M/aM = n - 1$. That is, we want to see that $\mathrm{Ext}^{n-1}(k, M/aM) \neq 0$, but $\mathrm{Ext}^i(k, M/aM) = 0$ for $i < n - 1$. This is direct from the injectivity and surjectivity above.

In fact surjectivity of $\mathrm{Ext}^{n-1}(k, M/aM) \to \mathrm{Ext}^n(k, M)$ shows that $\mathrm{Ext}^{n-1}(k, M/aM) \neq 0$. Now let $i < n - 1$. Then the exact sequence

$$\mathrm{Ext}^i(k, M) \to \mathrm{Ext}^i(k, M/aM) \to \mathrm{Ext}^{i+1}(k, M)$$

shows that $\mathrm{Ext}^i(k, M/aM)$. ▲

When you mod out by a nonzerodivisor, the depth drops by one.

36.6 Corollary. *The depth of M is well-defined. In fact,*

$$\mathrm{depth} M \leq \dim \mathrm{supp} M.$$

Proof. If $\mathrm{depth} M = 0$, then we're done.

In general, we induct on $\dim \mathrm{supp} M$, which we know is finite. Otherwise, there is $a \in \mathfrak{m}$ which is a nonzerodivisor on M. We know that

$$\mathrm{depth} M/aM = \mathrm{depth} M - 1$$

and

$$\dim \mathrm{supp} M/aM = \dim \mathrm{supp} M - 1.$$

By induction, we have that $\mathrm{depth} M/aM \leq \dim \mathrm{supp} M/aM$. From this the induction step is clear. ▲

Generally, the depth is not the dimension.

36.7 Example. Given any M, if you add k to it, then you make the depth zero: $M \oplus k$ has $\mathfrak{m}$ as an associated prime. But the dimension generally does not jump to zero.

In fact, we have described a recursive algorithm for computing $\mathrm{depth}(M)$.

1. If $\mathfrak{m} \in \mathrm{Ass}(M)$, output zero.

2. If $\mathfrak{m} \notin \mathrm{Ass}(M)$, choose an element $a \in \mathfrak{m}$ which is a nonzerodivisor on M. Output $\mathrm{depth}(M/aM) + 1$.

If you were to apply this in practice, you would start by looking for a nonzerodivisor $a_1 \in \mathfrak{m}$ on M, then looking for one on M/a_1M, etc. From this we make:

36.8 Definition. Let $(R, \mathfrak{m})$ be a local noetherian ring, M a finite R-module. A sequence $a_1, \dots, a_n \in \mathfrak{m}$ is said to be M**-regular** iff:

1. a_1 is a nonzerodivisor on M

2. a_2 is a nonzerodivisor on M/a_1M

3. ...

4. a_i is a nonzerodivisor on $M/(a_1, \dots, a_{i-1})M$ for all i.

A regular sequence $a_1, \dots, a_n$ is **maximal** if it can be extended no further, i.e. there is no a_{n+1} such that $a_1, \dots, a_{n+1}$ is M-regular.

36.9 Corollary. $\mathrm{depth}(M)$ *is the length of every maximal M-regular sequence. In particular, all M-regular sequences have the same length.*

Proof. If $a_1, \dots, a_n$ is M-regular, then

$$\mathrm{depth} M/(a_1, \dots, a_i)M = \mathrm{depth} M - i$$

for each i, by an easy induction on i and the definition. Finally, if the sequence is maximal, then $\mathfrak{m} \in \mathrm{Ass}(M/(a_1, \dots, a_n)M)$ so $\mathrm{depth} M/(a_1, \dots, a_n)M = 0$. ▲

Remark. We could define the depth via the length of a maximal M-regular sequence.

§2 Cohen-Macaulayness

36.10 Definition. Let $(R, \mathfrak{m})$ be a noetherian local ring. Then we set $\mathrm{depth} R$ to be the its depth as an R-module.

36.11 Example. If R is regular, then $\mathrm{depth} R = \dim R$.

Proof. Induction on $\dim R$. If $\dim R = 0$, then this is obvious by the inequality $\leq$ which is always true.

Suppose $\dim R = 0$. Then $\mathfrak{m} \neq 0$ and in particular $\mathfrak{m}/\mathfrak{m}^2 \neq 0$. Choose $x \in \mathfrak{m} - \mathfrak{m}^2$. Let $R' = R/(x)$. We know that $\dim R' = \dim R - 1$ as x is a nonzerodivisor (by regularity). On the other hand, the embedding dimension of R' also drops by one, as we have divided out by something in $\mathfrak{m} - \mathfrak{m}^2$. In particular, R' is regular local too. So the inductive hypothesis states that

$$\mathrm{depth} R - 1 = \mathrm{depth} R' = \dim R' = \dim R - 1.$$

Differently phrased, we could choose $x_1, \dots, x_n \in \mathfrak{m}$ which forms a basis for $\mathfrak{m}/\mathfrak{m}^2$; this is a *regular sequence* (that is, an R-regular sequence) by this argument. It is maximal as $x_1, \dots, x_n$ generate $\mathfrak{m}$ and $R/(x_1, \dots, x_n)$ clearly has depth zero. ▲

More generally:

36.12 Definition. A noetherian local ring $(R, \mathfrak{m})$ is called **Cohen-Macaulay** if $\dim R = \mathrm{depth} R$. A general noetherian ring R is **Cohen-Macaulay** if $R_{\mathfrak{p}}$ is Cohen-Macaulay for all $\mathfrak{p} \in \mathrm{Spec} R$.

For instance, any regular local ring is Cohen-Macaulay, as is any local artinian ring (because the dimension is zero for an artinian ring).

We shall eventually prove:

36.13 Proposition. *Let $R = \mathbb{C}[X_1, \dots, X_n]/\mathfrak{p}$ for $\mathfrak{p}$ prime. Choose an injective map $\mathbb{C}[y_1, \dots, y_n] \hookrightarrow R$ making R a finite module. Then R is Cohen-Macaulay iff R is projective as a module over $\mathbb{C}[y_1, \dots, y_n]$.*[26]

The picture is that the inclusion $\mathbb{C}[y_1, \dots, y_m] \hookrightarrow \mathbb{C}[x_1, \dots, x_n]/\mathfrak{p}$ corresponds to a map

$$X \to \mathbb{C}^m$$

for $X = V(\mathfrak{p}) \subset \mathbb{C}^n$. This statement of freeness is a statement about how the fibers of this finite map stay similar in some sense.

36.14 Example. Consider $\mathbb{C}[x, y]/(xy)$, the coordinate ring of the union of two axes intersecting at the origin. This is Cohen-Macaulay (but not regular, as it is not a domain). Indeed, we can project the associated variety $X = V(xy)$ onto the affine line by adding the coordinates. This corresponds to the map

$$\mathbb{C}[z] \to \mathbb{C}[x, y]/(xy)$$

[26] In fact, this is equivalent to freeness, although we will not prove it. Any projective finite module over a polynomial ring over a field is free, though this is a hard theorem.

sending $z \to x + y$. This makes $\mathbb{C}[x, y]/(xy)$ into a free $\mathbb{C}[z]$-module of rank two (with generators $1, x$), as one can check. So by the previous result (strictly speaking, its extension to non-domains), the ring in question is Cohen-Macaulay.

36.15 Example. $R = \mathbb{C}[x, y, z]/(xy, xz)$ is not Cohen-Macaulay (at the origin). The associated variety looks geometrically like the union of the plane $x = 0$ and the line $y = z = 0$ in affine 3-space. Here there are two components of different dimensions intersecting. Let's choose a regular sequence (that is, regular after localization at the origin). The dimension at the origin is clearly two because of the plane. First, we need a nonzerodivisor in this ring, which vanishes at the origin, say $x + y + z$. (**Exercise:** Check this.) When we quotient by this, we get

$$S = \mathbb{C}[x, y, z]/(xy, xz, x + y + z) = \mathbb{C}[y, z]/((y + z)y, (y + z)z).$$

The claim is that S localized at the ideal corresponding to $(0, 0)$ has depth zero. We have $y + z \neq 0$, which is killed by both y, z, and hence by the maximal ideal at zero. In particular the maximal ideal at zero is an associated prime, which implies the claim about the depth.

As it happens, a Cohen-Macaulay variety is always equidimensional. The rough reason is that each irreducible piece puts an upper bound on the depth given by the dimension of the piece. If any piece is too small, the total depth will be too small.

Anyway, we shall not say much more about Cohen-Macaulayness, but instead focus on understanding regular local rings. We want, for next time, to understand the relationship between depth and lengths of projective resolutions. We will prove:

36.16 Theorem (Auslander-Buchsbaum formula)**.** *Let $(R, \mathfrak{m})$ be a noetherian local ring and M a finite R-module. Suppose M has a finite projective resolution of length d, where d is minimal.*

Then

$$d = \operatorname{depth}(R) - \operatorname{depth}(M).$$

So in a sense, depth measures how far M is from being a free module. If the depth is large, then you need a lot of projective modules to resolve M.

Lecture 37
11/22

Last time we were talking about depth. Let's use this to reformulate a few definitions made earlier.

§1 Reduced rings

Recall that a noetherian ring is **reduced** iff:

1. For any minimal prime $\mathfrak{p} \subset R$, $R_{\mathfrak{p}}$ is a field.

2. Every associated prime of R is minimal.

Condition 1 can be reduced as follows. To say that $\mathfrak{p} \subset R$ is minimal is to say that it is zero-dimensional, and that is regular iff it is a field. So the first condition is that *for every height zero prime,* $R_{\mathfrak{p}}$ *is regular.* For the second condition, $\mathfrak{p} \in \mathrm{Ass}(R)$ iff $\mathfrak{p} \in \mathrm{Ass}(R_{\mathfrak{p}})$, which is equivalent to $\mathrm{depth} R_{\mathfrak{p}} = 0$.

Namely, the two conditions are:

1. For every height zero prime $\mathfrak{p}$, $R_{\mathfrak{p}}$ is regular.

2. For every prime $\mathfrak{p}$ of height > 0, $\mathrm{depth} R_{\mathfrak{p}} > 0$.

Condition two is always satisfied in a Cohen-Macaulay ring.

§2 Serre's criterion again

Recall that

37.1 Definition. A noetherian ring is **normal** iff it is a finite direct product of integrally closed domains.

In the homework, we showed:

37.2 Proposition. *A reduced ring R is normal iff*

1. *For every height one prime* $\mathfrak{p} \in \mathrm{Spec} R$*,* $R_{\mathfrak{p}}$ *is a DVR (i.e. regular).*

2. *For every nonzerodivisor* $x \in R$*, every associated prime of* R/x *is minimal.*

(We had proved this for *domains* earlier.) These conditions are equivalent to:

1. For every prime $\mathfrak{p}$ of height ≤ 1, $R_{\mathfrak{p}}$ is regular.

2. For every prime $\mathfrak{p}$ of height ≥ 1, $\mathrm{depth} R_{\mathfrak{p}} \geq 1$ (necessary for reducedness)

3. $\mathrm{depth} R_{\mathfrak{p}} \geq 2$ for $\mathfrak{p}$ not minimal over any principal ideal (x) for x a nonzerodivisor. Condition three is the last condition of the proposition as quotienting out by x drops the depth by one.

The first and third conditions imply the second. In particular, we find:

37.3 Theorem (Serre's criterion)**.** *A noetherian ring is normal iff:*

1. *For every prime* $\mathfrak{p}$ *of height* ≤ 1*,* $R_{\mathfrak{p}}$ *is regular.*

2. $\mathrm{depth} R_{\mathfrak{p}} \geq 2$ *for* $\mathfrak{p}$ *not minimal over any principal ideal* (x) *for* x *a nonzerodivisor.*

For a Cohen-Macaulay ring, the last condition is automatic, as the depth is the codimension.

§3 Projective dimension

Let R be a commutative ring, M an R-module.

37.4 Definition. The **projective dimension** of M is the largest integer n such that there exists a module N with

$$\mathrm{Ext}^n(M, N) \neq 0.$$

(If no such n, N exist, then we say that the projective dimension is ∞.) We write $\mathrm{pd}(M)$ for the projective dimension.

Remark. $\mathrm{pd}(M) = 0$ iff M is projective. Indeed, we have seen that the Ext groups $\mathrm{Ext}^i(M, N), i > 0$ vanish always.

If you wanted to compute the projective dimension, you could go as follows. Take any M. Choose a surjection $P \twoheadrightarrow M$ with P projective; call the kernel K and draw a short exact sequence

$$0 \to K \to P \to M \to 0.$$

For any R-module N, we have a long exact sequence

$$\mathrm{Ext}^{i-1}(P, N) \to \mathrm{Ext}^{i-1}(K, N) \to \mathrm{Ext}^i(M, N) \to \mathrm{Ext}^i(P, N).$$

If $i > 0$, the right end vanishes; if $i > 1$, the left end vanishes. So if $i > 1$, this map $\mathrm{Ext}^{i-1}(K, N) \to \mathrm{Ext}^i(M, N)$ is an *isomorphism.*

Suppose that $\mathrm{pd}(K) = d \geq 0$. We find that $\mathrm{Ext}^{i-1}(K, N) = 0$ for $i - 1 > d$. This implies that $\mathrm{Ext}^i(M, N) = 0$ for such $i > d + 1$. In particular, $\mathrm{pd}(M) \leq d + 1$. This argument is completely reversible if $d > 0$. Then we see from these isomorphisms that

$$\boxed{\mathrm{pd}(M) = \mathrm{pd}(K) + 1}, \quad \text{unless } \mathrm{pd}(M) = 0$$

If M is projective, the sequence $0 \to K \to P \to M \to 0$ splits, and $\mathrm{pd}(K) = 0$ too.

The upshot is that **we can compute projective dimension by choosing a projective resolution.**

37.5 Proposition. *Let M be an R-module. Then $\mathrm{pd}(M) \leq n$ iff there exists a finite projective resolution of M having $n + 1$ terms,*

$$0 \to P_n \to \cdots \to P_1 \to P_0 \to M \to 0.$$

Proof. Induction on n. When $n = 0$, M is projective, and we can use the resolution $0 \to M \to M \to 0$.

Suppose $\mathrm{pd}(M) \leq n$, where $n > 0$. We can get a short exact sequence

$$0 \to K \to P_0 \to M \to 0$$

with P_0 projective, so $\mathrm{pd}(K) \leq n - 1$. The inductive hypothesis implies that there is a projective resolution of K of length $\leq n - 1$. We can splice this in with the short exact sequence to get a projective resolution of M of length n.

The argument is reversible. Choose any projective resolution

$$0 \to P_n \to \cdots \to P_1 \to P_0 \to M \to 0$$

and split into short exact sequences, and argue inductively. ▲

Let $\mathrm{pd}(M) = n$. Choose any projective resolution $\cdots \to P_2 \to P_1 \to P_0 \to M$. Choose $K_i = \ker(P_i \to P_{i-1})$ for each i. Then there is a short exact sequence $0 \to K_0 \to P_0 \to M \to 0$. Moreover, there are exact sequences

$$0 \to K_i \to P_i \to K_{i-1} \to 0$$

for each i. From these, we see that the projective dimensions of the K_i drop by one as i increments. So K_{n-1} is projective if $\mathrm{pd}(M) = n$ as $\mathrm{pd}(K_{n-1}) = 0$. In particular, we can get a projective resolution

$$0 \to K_{n-1} \to P_{n-1} \to \cdots \to P_0 \to M \to 0$$

which is of length n. In particular, if you ever start trying to write a projective resolution of M, you can stop after going out n terms, because the kernels will become projective.

§4 Minimal projective resolutions

Usually projective resolutions are non-unique. But sometimes they kind of are. Let $(R, \mathfrak{m})$ be a local noetherian ring, M a finitely generated R-module.

37.6 Definition. A projective resolution $P_* \to M$ of finitely generated modules is **minimal** if for each i, the induced map $P_i \otimes R/\mathfrak{m} \to P_{i-1} \otimes R/\mathfrak{m}$ is zero, and same for $P_0 \otimes R/\mathfrak{m} \to M/\mathfrak{m}M$.

This is equivalent to saying that for each i, the map $P_i \to \ker(P_{i-1} \to P_{i-2})$ is an isomorphism modulo $\mathfrak{m}$.

37.7 Proposition. *Every M (over a local noetherian ring) has a minimal projective resolution.*

Proof. Start with a module M. Then $M/\mathfrak{m}M$ is a finite-dimensional vector space over $R/\mathfrak{m}$, of dimension say d_0. We can choose a basis for that vector space, which we can lift to M. That determines a map of free modules

$$R^{d_0} \to M,$$

which is a surjection by Nakayama's lemma. It is by construction an isomorphism modulo $\mathfrak{m}$. Then define $K = \ker(R^{d_0} \to M)$; this is finitely generated by noetherianness, and we can do the same thing for K, and repeat to get a map $R^{d_1} \twoheadrightarrow K$ which is an isomorphism modulo $\mathfrak{m}$. Then

$$R^{d_1} \to R^{d_0} \to M \to 0$$

is exact, and minimal; we can continue this by the same procedure. ▲

37.8 Proposition. *Minimal projective resolutions are unique up to isomorphism.*

Proof. Suppose we have one minimal projective resolution:

$$\cdots \to P_2 \to P_1 \to P_0 \to M \to 0$$

and another:

$$\cdots \to Q_2 \to Q_1 \to Q_0 \to M \to 0.$$

There is always a map of projective resolutions $P_* \to Q_*$ by general homological algebra. There is, equivalently, a commutative diagram

$$\begin{tikzcd}
\cdots \arrow[r] \arrow[d] & P_2 \arrow[r] \arrow[d] & P_1 \arrow[r] \arrow[d] & P_0 \arrow[r] \arrow[d] & M \arrow[r] \arrow[d, "\mathrm{id}"] & 0 \\
\cdots \arrow[r] & Q_2 \arrow[r] & Q_1 \arrow[r] & Q_0 \arrow[r] & M \arrow[r] & 0
\end{tikzcd}$$

If both resolutions are minimal, the claim is that this map is an isomorphism. That is, $\phi_i : P_i \to Q_i$ is an isomorphism, for each i.

To see this, note that P_i, Q_i are finite free R-modules.[27] So ϕ_i is an isomorphism iff ϕ_i is an isomorphism modulo the maximal ideal, i.e. if

$$P_i/\mathfrak{m}P_i \to Q_i/\mathfrak{m}Q_i$$

is an isomorphism. Indeed, if ϕ_i is an isomorphism, then its tensor product with $R/\mathfrak{m}$ obviously is an isomorphism. Conversely suppose that the reductions mod $\mathfrak{m}$ make an isomorphism. Then the ranks of P_i, Q_i are the same, and ϕ_i is an n-by-n matrix whose determinant is not in the maximal ideal, so is invertible. This means that ϕ_i is invertible by the usual formula for the inverse matrix.

So we are to check that $P_i/\mathfrak{m}P_i \to Q_i/\mathfrak{m}Q_i$ is an isomorphism for each i. This is equivalent to the assertion that

$$(Q_i/\mathfrak{m}Q_i)^\vee \to (P_i/\mathfrak{m}P_i)^\vee$$

is an isomorphism. But this is the map

$$\mathrm{Hom}_R(Q_i, R/\mathfrak{m}) \to \mathrm{Hom}_R(P_i, R/\mathfrak{m}).$$

If we look at the chain complexes $\mathrm{Hom}(P_*, R/\mathfrak{m}), \mathrm{Hom}(Q_*, R/\mathfrak{m})$, the cohomologies compute the Ext groups of $(M, R/\mathfrak{m})$. But all the maps in this chain complex are zero because the resolution is minimal, and we have that the image of P_i is contained in $\mathfrak{m}P_{i-1}$ (ditto for Q_i). So the cohomologies are just the individual terms, and the maps $\mathrm{Hom}_R(Q_i, R/\mathfrak{m}) \to \mathrm{Hom}_R(P_i, R/\mathfrak{m})$ correspond to the identities on $\mathrm{Ext}^i(M, R/\mathfrak{m})$. So these are isomorphisms.[28] ▲

37.9 Corollary. *If $\cdots \to P_2 \to P_1 \to P_0 \to M$ is a minimal projective resolution of M, then the ranks* $\mathrm{rank}(P_i)$ *are well-defined (i.e. don't depend on the choice of the minimal resolution).*

[27] We are using the fact that a finite projective module over a local ring is *free*.

[28] We are sweeping under the rug the statement that Ext can be computed via *any* projective resolution. More precisely, if you take any two projective resolutions, and take the induced maps between the projective resolutions, hom them into $R/\mathfrak{m}$, then the maps on cohomology are isomorphisms.

Proof. Immediate from the proposition. In fact, the ranks are the dimensions (as $R/\mathfrak{m}$-vector spaces) of $\mathrm{Ext}^i(M, R/\mathfrak{m})$. ▲

Let us advertise the goal for next time. We would like to prove Serre's criterion for regularity.

37.10 Theorem. *Let* $(R, \mathfrak{m})$ *be a local noetherian ring. Then* R *is regular iff* $R/\mathfrak{m}$ *has finite projective dimension. In this case,* $\mathrm{pd}(R/\mathfrak{m}) = \dim R$.

Lecture 38
11/24

§1 The Auslander-Buchsbaum formula

Today, we shall start by proving:

38.1 Theorem (Auslander-Buschsbaum formula)**.** *Let* R *be a local noetherian ring,* M *a f.g.* R*-module of finite projective dimension. If* $\mathrm{pd}(R) < \infty$*, then* $\mathrm{pd}(M) = \mathrm{depth}(R) - \mathrm{depth}(M)$.

Proof. Induction on $\mathrm{pd}(M)$. When $\mathrm{pd}(M) = 0$, then M is projective, so isomorphic to R^n for some n. Thus $\mathrm{depth}(M) = \mathrm{depth}(R)$.

Assume $\mathrm{pd}(M) > 0$. Choose a surjection $P \twoheadrightarrow M$ and write an exact sequence

$$0 \to K \to P \to M \to 0,$$

where $\mathrm{pd}(K) = \mathrm{pd}(M) - 1$. We also know by induction that

$$\mathrm{pd}(K) = \mathrm{depth} R - \mathrm{depth}(K).$$

What we want to prove is that

$$\mathrm{depth} R - \mathrm{depth} M = \mathrm{pd}(M) = \mathrm{pd}(K) + 1.$$

This is equivalent to wanting know that $\mathrm{depth}(K) = \mathrm{depth}(M) + 1$. In general, this may not be true, though, but we will prove it under minimality hypotheses.

Without loss of generality, we can choose that P is *minimal*, i.e. becomes an isomorphism modulo the maximal ideal $\mathfrak{m}$. This means that the rank of P is $\dim M/\mathfrak{m}M$. So $K = 0$ iff $P \to M$ is an isomorphism; we've assumed that M is not free, so $K \neq 0$.

Recall that the depth of M is the smallest value i such that $\mathrm{Ext}^i(R/\mathfrak{m}, M) \neq 0$. So we should look at the long exact sequence from the above short exact sequence:

$$\mathrm{Ext}^i(R/\mathfrak{m}, P) \to \mathrm{Ext}^i(R/\mathfrak{m}, M) \to \mathrm{Ext}^{i+1}(R/\mathfrak{m}, K) \to \mathrm{Ext}^{i+1}(R/\mathfrak{m}, P).$$

Now P is just a direct sum of copies of R, so $\mathrm{Ext}^i(R/\mathfrak{m}, P)$ and $\mathrm{Ext}^{i+1}(R/\mathfrak{m}, P)$ are zero if $i + 1 < \mathrm{depth} R$. In particular, if $i + 1 < \mathrm{depth} R$, then the map $\mathrm{Ext}^i(R/\mathfrak{m}, M) \to \mathrm{Ext}^{i+1}(R/\mathfrak{m}, K)$ is an isomorphism. So we find that $\mathrm{depth} M + 1 = \mathrm{depth} K$ in this case.

We have seen that *if* $\mathrm{depth} K < \mathrm{depth} R$, *then* by taking i over all integers $< \mathrm{depth} K$, we find that

$$\mathrm{Ext}^i(R/\mathfrak{m}, M) = \begin{cases} 0 & \text{if } i+1 < \mathrm{depth} K \\ \mathrm{Ext}^{i+1}(R/\mathfrak{m}, K) & \text{if } i+1 = \mathrm{depth} K \end{cases}.$$

In particular, we are **done** unless $\mathrm{depth} K \geq \mathrm{depth} R$. By the inductive hypothesis, this is equivalent to saying that K is projective.

So let us consider the case where K is projective, i.e. $\mathrm{pd}(M) = 1$. We want to show that $\mathrm{depth} M = d - 1$ if $d = \mathrm{depth} R$. We need a slightly different argument in this case. Let $d = \mathrm{depth}(R) = \mathrm{depth}(P) = \mathrm{depth}(K)$ since P, K are free. We have a short exact sequence

$$0 \to K \to P \to M \to 0$$

and a long exact sequence of Ext groups:

$$0 \to \mathrm{Ext}^{d-1}(R/\mathfrak{m}, M) \to \mathrm{Ext}^d(R/\mathfrak{m}, K) \to \mathrm{Ext}^d(R/\mathfrak{m}, P).$$

We know that $\mathrm{Ext}^d(R/\mathfrak{m}, K)$ is nonzero as K is free and R has depth d. However, $\mathrm{Ext}^i(R/\mathfrak{m}, K) = \mathrm{Ext}^i(R/\mathfrak{m}, P) = 0$ for $i < d$. This implies that $\mathrm{Ext}^{i-1}(R/\mathfrak{m}, M) = 0$ for $i < d$.

We will show:

The map $\mathrm{Ext}^d(R/\mathfrak{m}, K) \to \mathrm{Ext}^d(R/\mathfrak{m}, P)$ is zero.

This will imply that the depth of M is *precisely* $d - 1$.

This is because the matrix $K \to P$ is given by multiplication by a matrix with coefficients in $\mathfrak{m}$ as $K/\mathfrak{m}K \to P/\mathfrak{m}P$ is zero. In particular, the map on the Ext groups is zero, because it is annihilated by $\mathfrak{m}$. ▲

38.2 Example. Let $R = \mathbb{C}[x_1, \ldots, x_n]/\mathfrak{p}$ for $\mathfrak{p}$ prime. Choose an injection $R' \to R$ where $R' = \mathbb{C}[y_1, \ldots, y_m]$ and R is a f.g. R'-module. This exists by the Noether normalization lemma.

We wanted to show:

38.3 Theorem. *R is Cohen-Macaulay*[29] *iff R is a projective R'-module.*

We shall use the fact that projectiveness can be tested locally at every maximal ideal.

Proof. Choose a maximal ideal $\mathfrak{m} \subset R'$. We will show that $R_\mathfrak{m}$ is a free $R'_\mathfrak{m}$-module via the injection of rings $R'_\mathfrak{m} \hookrightarrow R_\mathfrak{m}$ (where $R_\mathfrak{m}$ is defined as R localized at the multiplicative subset of elements of $R' - \mathfrak{m}$) at each $\mathfrak{m}$ iff Cohen-Macaulayness holds.

Now $R'_\mathfrak{m}$ is a regular local ring, so its depth is m. By the Auslander-Buchsbaum formula, $R_\mathfrak{m}$ is projective as an $R'_\mathfrak{m}$-module iff

$$\mathrm{depth}_{R'_\mathfrak{m}} R_\mathfrak{m} = m.$$

[29] That is, its localizations at any prime—or, though we haven't proved yet, at any maximal ideal—are.

Now R is a projective module iff the above condition holds for all maximal ideals $\mathfrak{m} \subset R'$. The claim is that this is equivalent to saying that $\mathrm{depth} R_{\mathfrak{n}} = m = \dim R_{\mathfrak{n}}$ for every maximal ideal $\mathfrak{n} \subset R$ (depth over R!).

These two statements are almost the same, but one is about the depth of R as an R-module, and another as an R'-module.

> Issue: There may be several maximal ideals of R lying over the maximal ideal $\mathfrak{m} \subset R'$.

The problem is that $R_{\mathfrak{m}}$ is not generally local, and not generally equal to $R_{\mathfrak{n}}$ if $\mathfrak{n}$ lies over $\mathfrak{m}$. Fortunately, depth makes sense even over semi-local rings (rings with finitely many maximal ideals).

Let us just assume that this does not occur, though. Let us assume that $R_{\mathfrak{m}}$ is a local ring for every maximal ideal $\mathfrak{m} \subset R$. Then we are reduced to showing that if $S = R_{\mathfrak{m}}$, then the depth of S as an $R'_{\mathfrak{m}}$-module is the same as the depth as an $R_{\mathfrak{m}}$-module. That is, the depth doesn't depend too much on the ring, since $R'_{\mathfrak{m}}, R_{\mathfrak{m}}$ are "pretty close." If you believe this, then you believe the theorem, by the first paragraph.

Let's prove this claim in a more general form:

38.4 Proposition. *Let $\phi : S' \to S$ be a local[30] map of local noetherian rings such that S is a f.g. S'-module. Then, for any finitely generated S-module M,*

$$\mathrm{depth}_S M = \mathrm{depth}_{S'} M.$$

With this, the theorem will be proved.

Remark. This result generealizes to the semi-local case, which is how one side-steps the issue above.

Proof. By induction on $\mathrm{depth}_{S'} M$. There are two cases.

Let $\mathfrak{m}', \mathfrak{m}$ be the maximal ideals of S', S. If $\mathrm{depth}_{S'}(M) > 0$, then there is an element a in $\mathfrak{m}'$ such that

$$M \overset{\phi(a)}{\to} M$$

is injective. Now $\phi(a) \in \mathfrak{m}$. So $\phi(a)$ is a nonzerodivisor, and we have an exact sequence

$$0 \to M \overset{\phi(a)}{\to} M \to M/\phi(a)M \to 0.$$

Thus we find

$$\mathrm{depth}_S M > 0.$$

Moreover, we find that $\mathrm{depth}_S M = \mathrm{depth}_S(M/\phi(a)M)+1$ and $\mathrm{depth}_{S'} M = \mathrm{depth}_{S'}(M/\phi(a)M))+1$. The inductive hypothesis now tells us that

$$\mathrm{depth}_S M = \mathrm{depth}_{S'} M.$$

The hard case is where $\mathrm{depth}_{S'} M = 0$. We need to show that this is equivalent to $\mathrm{depth}_S M = 0$. So we know at first that $\mathfrak{m}' \in \mathrm{Ass}(M)$. That is, there is an element $x \in M$ such that $\mathrm{Ann}_{S'}(x) = \mathfrak{m}'$. Now $\mathrm{Ann}_S(x) \subsetneq S$ and contains $\mathfrak{m}' S$.

[30] I.e. ϕ sends non-units into non-units.

$Sx \subset M$ is a submodule, surjected onto by S by the map $a \to ax$. This map actually, as we have seen, factors through $S/\mathfrak{m}'S$. Here S is a finite S'-module, so $S/\mathfrak{m}'S$ is a finite $S'/\mathfrak{m}'$-module. In particular, it is a finite-dimensional vector space over a field. It is thus a local artinian ring. But Sx is a module over this local artinian ring. It must have an associated prime, which is a maximal ideal in $S/\mathfrak{m}'S$. The only maximal ideal can be $\mathfrak{m}/\mathfrak{m}'S$. It follows that $\mathfrak{m} \in \mathrm{Ass}(Sx) \subset \mathrm{Ass}(M)$.

In particular, $\mathrm{depth}_S M = 0$ too, and we are done. ▲

▲

Lecture 39
11/29

§1 The projective dimension for noetherian local rings

Let R be a local noetherian ring. Let us think about a condition that would put a bound on the projective dimension of R-modules.

Let $n \in \mathbb{Z}_{\geq 0}$.

39.1 Proposition. *TFAE:*

1. *Every R-module has projective dimension $\leq n$.*
2. *Every finitely R-module has projective dimension $\leq n$.*
3. *The residue field $R/\mathfrak{m}$ has projective dimension $\leq n$.*

In some sense, the residue field is the worst case one can get when measuring the projective dimension.

Proof. The only non-obvious implications are that 2 implies 1 and 3 implies 2. Namely, 1 is equivalent to $\mathrm{Ext}^i(M, N) = 0$ for $i > n$ for all modules M, N. The second condition is equivalent to $\mathrm{Ext}^i(M, N) = 0$ for $i > n$ when M si finitely generated.

Let us now check that 2 implies 1. Fix an R-module N. Then I claim:

39.2 Proposition. $\mathrm{Ext}^i(M, N) = 0$ *for $i > n$ and all M if and only if* $\mathrm{Ext}^i(M, N) = 0$ *for $i > n$ and finitely generated M.*

Proof. Induction on n. Choose an injection $N \to Q$ for Q injective. This leads to an exact sequence

$$0 \to N \to Q \to Q/N \to 0.$$

For every M, we have a long exact sequence

$$\mathrm{Ext}^i(M, Q) \to \mathrm{Ext}^i(M, Q/N) \to \mathrm{Ext}^{i+1}(M, N) \to \mathrm{Ext}^{i+1}(M, Q).$$

But Q is injective, so if $i > 0$ the two ends are zero. In particular, for $n > 0$, it suffices to show that $\mathrm{Ext}^i(M, Q/N) = 0$ for $i > n - 1$ and for all M. But this is true for finitely generated M because of the above exact sequence. Now we use the inductive hypothesis.

We just need to show this for $n = 0$ as a result. Then we are assuming that $\mathrm{Ext}^i(M, N) = 0$ for $i > 0$ and M finitely generated; we want to get from this that this is true without M f.g. In particular, we must show that N is injective. We have to show that if $M' \subset M$, any map $M' \to N$ extends to M. But we can extend over any finite module extension by hypothesis on the Ext groups. Then Zorn's lemma implies we can extend to all of M. (In fact, if $\mathrm{Ext}^1(R/I, N) = 0$ for any ideal $I \subset R$, then N is injective.) ▲

But now we have seen that 1 is equivalent to 2 in the proposition. Now we need to check that 3 implies 2. Namely, if the projective dimension of $R/\mathfrak{m}$ is at most n, then the same is true for any f.g. R-module. Let is induct on supp$M$.

Let M be an R-module. There is an exact sequence

$$0 \to M' \to M \to M'' \to 0$$

where M' has finite length and M'' has depth > 0 (i.e. has no artinian submodules). Here M' consists of all elements killed by a power of $\mathfrak{m}$. So M' has a finite filtration where the successive quotients are $R/\mathfrak{m}$, so its projective dimension is at most n (by the long exact sequence). Thus, it suffices to show that $\mathrm{pd}(M'') \leq n$.[31]

If $M'' = 0$, then done. Otherwise, M'' has depth > 0, so there is $x \in \mathfrak{m}$ which is a nonzerodivisor on M''. We have an exact sequence

$$0 \to M'' \xrightarrow{a} M'' \to M''/aM'' \to 0$$

where M''/aM'' has a smaller support, so $\mathrm{pd}(M''/aM'') \leq n$ by induction. Let N be a f.g. R-module. We want to know that

$$\mathrm{Ext}^i(M'', N) = 0 \quad \text{for } i > n.$$

The exact sequence earlier gives a map

$$\mathrm{Ext}^i(M'', N) \xrightarrow{a} \mathrm{Ext}^i(M'', N) \to \mathrm{Ext}^{i+1}(M''/aM'', N).$$

For $i > n$, the end vanishes, so Nakayama says that $\mathrm{Ext}^i(M'', N) = 0$. Done. ▲

39.3 Definition. Let R be a noetherian local ring. R has **global dimension** $\leq n$ if $\mathrm{Ext}^i(M, N) = 0$ for $i > n$. Alternatively, if $\mathrm{pd}(R/\mathfrak{m}) \leq n$, by the above result.

§2 Global dimension and regularity

Our real goal today is to prove the following result of Serre:

39.4 Theorem (Serre)**.** *Let R be a local noetherian ring. Then the global dimension of R is finite iff R is regular. In this case, the global dimension is the Krull dimension.*

[31] Projective dimension behaves well with respect to exact sequences.

Proof. Suppose R regular. Choose elements $x_1, \dots, x_n \in \mathfrak{m}$ forming a basis for $\mathfrak{m}/\mathfrak{m}^2$. Here is a construction that will be useful.

The **Koszul complex** $K(x_1, \dots, x_n)$ is the chain complex

$$\dots \to \wedge^2 R^n \to R^n \to R$$

where R^n is the free R-module on a basis $e_1, \dots, e_n$. The differential d is determined by the following properties:

1. $d(e_i) = x_i$.
2. d satisfies the Leibniz rule. In other words, $d(a \wedge b) = da \wedge b + (-1)^q a \wedge db$ if b has degree q.

The claim is that the Koszul complex is a projective resolution of $R/\mathfrak{m}$. In fact, it is a minimal projective resolution, and by construction it has length n. It is easy to see that the cokernel at the end is $R/\mathfrak{m}$. This is *minimal* because it always multiplies by something in $\mathfrak{m}$. The claim is that it is actually exact.

A more general claim:

39.5 Proposition. *If $x_1, \dots, x_j \in R$ is a subset of these generators in $\mathfrak{m}$, the Koszul complex $K(x_1, \dots, x_j)$ is exact and is a resolution of $R/(x_1, \dots, x_j)$. (Except in degree zero.)*

Proof. Induction on j. We omit the details. ▲

So this is a sketch of the proof that a regular local has finite global dimension: you explicitly write down the resolution of the residue field.

The hard direction is the converse. Suppose $\mathrm{pd}(R/\mathfrak{m}) = n < \infty$. We want to show that R is regular and $\dim(R) = n$. The latter is clear from the minimality of the Koszul complex if we prove regularity.

We know the Auslander-Buchsbaum formula implies that

$$\mathrm{pd}(R/\mathfrak{m}) = \mathrm{depth}(R) - \mathrm{depth}(R/\mathfrak{m}).$$

The module $R/\mathfrak{m}$ is artinian and has length zero. In particular,

$$\mathrm{pd}(R/\mathfrak{m}) = \mathrm{depth}(R) \leq \dim(R).$$

We will show that the embedding dimension of R is at most the projective dimension. This will imply that the embedding dimension is at most the dimension, which will prove regularity.

Let $d = \dim \mathfrak{m}/\mathfrak{m}^2$. Choose elements $x_1, \dots, x_d \in \mathfrak{m}$ forming a basis of $\mathfrak{m}/\mathfrak{m}^2$. Consider, again, the Koszul complex $K(x_1, \dots, x_n)$. This complex looks like

$$\to \wedge^2 R^d \to R^d \to R;$$

we don't know that this is acyclic, since a priori we don't know that the ring is regular. All we know is that the cokernel at the end is $R/\mathfrak{m}$. Choose a minimal projective resolution $P_* \to R/\mathfrak{m}$. This is finite; it stops somewhere.

We know that there are two finite complexes

$$P_* \to R/\mathfrak{m}$$

and the Koszul complex

$$K_*(x_1, \dots, x_d) \to R/\mathfrak{m}.$$

We are trying to show that the second complex is shorter. By general nonsense, we can find a map of chain complexes

$$\phi : K_*(x_1, \dots, x_d) \to P_*$$

which commutes with the maps to $R/\mathfrak{m}$. (We are using the fact that P_* is acyclic and the Koszul complex is free.)

I claim that all the maps $\phi : K_* \to P_*$ are vertical. This immediately implies that d is at most the length of P_*. In fact, we will show that the $\phi_i : K_i \to P_i$ are *split injective*. This is the same thing as saying that ϕ_i is injective modulo $\mathfrak{m}$. (**Easy exercise:** split injective for free modules over a local ring is the same thing as injective over the maximal ideal.)

I don't really understand this—sorry Let's prove the claim about the ϕ_i. Induction on i. ϕ_0 is an isomorphism. The first two terms are the same. We have a commutative diagram

$$\begin{tikzcd}
K_i \arrow[r] \arrow[d] & K_{i-1} \arrow[d] \\
P_i \arrow[r] & P_{i-1}
\end{tikzcd}$$

Modulo the maximal ideal, the bottom map is zero. The same is true for the top map. If we tensor with $R/\mathfrak{m}$, we find

$$\begin{tikzcd}
K_i/\mathfrak{m}K_i \arrow[r] \arrow[d] & K_{i-1}/\mathfrak{m}K_{i-1} \arrow[d] \\
P_i/\mathfrak{m}P_i \arrow[r] & P_{i-1}/\mathfrak{m}P_i
\end{tikzcd}$$

This needs to be fixed; the proof is not quite complete ▲

Lecture 40
12/1

§1 Applications of Serre's criterion

Last time, we proved **Serre's criterion.** Namely, a local noetherian ring R is regular if and only if $R/\mathfrak{m}$ has finite projective dimension. This is equivalent to saying that every R-module has finite projective dimension. This is a very useful characterization of regularity.

40.1 Corollary. *Let R be a regular local ring and let $\mathfrak{p} \subset R$ be a prime ideal. Then $R_{\mathfrak{p}}$ is regular.*

In general, this is not at all obvious from the definition of dimension being equal to embedding dimension.

Proof. Let M be a finitely generated $R_{\mathfrak{p}}$-module. We want to show that M has a finite projective resolution. We know that M is finitely generated, so it is in fact finitely presented, meaning that there is an exact sequence

$$R_{\mathfrak{p}}^m \overset{A}{\to} R_{\mathfrak{p}}^n \to M \to 0$$

where A is given by a matrix with $R_{\mathfrak{p}}$-coefficients. Multiplying, we can assume that A comes from a matrix with coefficients in R. Let M_0 be the cokernel of the map

$$R^m \overset{A}{\to} R^n;$$

since localization is exact, we know that $(M_0)_{\mathfrak{p}} = M$. Since R is regular, there is a finite projective (thus free) resolution of M_0. We can localize this resolution at $\mathfrak{p}$ to get a finite free resolution of the $R_{\mathfrak{p}}$-module M; this is exact as localization is exact. Thus M has finite projective dimension. ▲

40.2 Example. Let R be a noetherian ring (possibly not local), and let's look at Spec$R$. Let U be the subset of Spec$R$ consisting of $\mathfrak{p}$ such that $\mathfrak{p}$ is regular. We just showed that if $\mathfrak{p} \in U$ and $\mathfrak{q} \subset \mathfrak{p}$, then $\mathfrak{q} \in U$. That is, U is closed under *generization.*

This suggests that the set U (sometimes called the **regular locus**) might be open. In general, this is false, but in practice, it usually is open.

40.3 Example. Let $R = \mathbb{C}[x_1, \dots, x_n]/I$ be an affine ring over $\mathbb{C}$. Rings that look like this do always satisfy the condition that the regular locus be open. This can be deduced for the criterion for regularity that was discussed earlier.

There is a large class of noetherian rings, including all fields and $\mathbb{Z}$ and closed under familiar constructions (like localization, finite extensions, etc.) for which the answer is yes. These rings are called **excellent rings.**

§2 Factoriality

The goal for the rest of the present lecture is to show that a regular local ring is factorial.

First, we need:

40.4 Definition. Let R be a noetherian ring and M a f.gen. R-module. Then M is **stably free** if $M \oplus R^k$ is free for some k.

Stably free obviously implies "projective." Free implies stably free, clearly—take $k = 0$. Over a local ring, a finitely generated projective module is free, so all three notions are equivalent. Over a general ring, these notions are generally different.

We will need the following lemma:

40.5 Lemma. *Let M be an R-module with a finite free resolution. If M is projective, it is stably free.*

Proof. There is an exact sequence

$$0 \to F_k \to F_{k-1} \to \cdots \to F_1 \to F_0 \to M \to 0$$

with the F_i free and finitely generated, by assumption.

We induct on the length k of the resolution. We know that if N is the kernel of $F_0 \to M$, then N is projective (as the sequence $0 \to N \to F_0 \to M \to 0$ splits) so there is a resolution

$$0 \to F_k \to \cdots \to F_1 \to N \to 0.$$

By the inductive hypothesis, N is stably free. So there is a free module R^d such that $N \oplus R^d$ is free.

We know that $M \oplus N = F_0$ is free. Thus $M \oplus N \oplus R^d = F_0 \oplus R^d$ is free and $N \oplus R^d$ is free. Thus M is stably free. ▲

Remark. Stably freeness does **not** generally imply freeness, though it does over a local noetherian ring.

Nonetheless,

40.6 Proposition. *Stably free does imply free for invertible modules.*

Proof. Let I be stably free and invertible. We must show that $I \simeq R$. Without loss of generality, we can assume that Spec$R$ is connected, i.e. R has no nontrivial idempotents. We will assume this in order to talk about the **rank** of a projective module.

We know that $I \oplus R^n \simeq R^m$ for some m. We know that $m = n+1$ by localization. So $I \oplus R^n \simeq R^{n+1}$ for some n. We will now need to construct the **exterior powers**, for which we digress:

40.7 Definition. Let R be a commutative ring and M an R-module. Then $\wedge M$, the **exterior algebra on** M, is the free (noncommutative) graded R-algebra generated by M (with product $\wedge$) with just enough relations such that $\wedge$ is anticommutative (and, *more strongly*, $x \wedge x = 0$ for x degree one).

Clearly $\wedge M$ is a quotient of the **tensor algebra** $T(M)$, which is by definition $R \oplus M \oplus M \otimes M \oplus \cdots \oplus M^{\otimes n} \oplus \ldots$. The tensor algebra is a graded R-algebra in an obvious way: $(x_1 \otimes \cdots \otimes x_a).(y_1 \otimes \cdots \otimes y_b) = x_1 \otimes \cdots \otimes x_a \otimes y_1 \otimes \cdots \otimes y_b$. This is an associative R-algebra. Then

$$\wedge M = T(M)/(x \otimes x,\ x, y \in M).$$

The grading on $\wedge M$ comes from the grading of $T(M)$.

We are interested in basically one example:

40.8 Example. Say $M = R^m$. Then $\wedge^m M = R$. If $e_1, \ldots, e_m \in M$ are generators, then $e_1 \wedge \cdots \wedge e_m$ is a generator. More generally, $\wedge^k M$ is free on $e_{i_1} \wedge \cdots \wedge e_{i_k}$ for $i_1 < \cdots < i_k$.

We now make:

40.9 Definition. If M is a projective R-module of rank n, then

$$\det(M) = \wedge^n M.$$

If M is free, then $\det(M)$ is free of rank one. So, as we see by localization, $\det(M)$ is always an invertible module for M locally free (i.e. projective) and $\wedge^{n+1} M = 0$.

40.10 Lemma. $\det(M \oplus N) = \det M \otimes \det N$.

Proof. This isomorphism is given by wedging $\wedge^{\text{top}} M \otimes \wedge^{\text{top}} N \to \wedge^{\text{top}}(M \oplus N)$. This is easily checked for oneself. ▲

Anyway, let us finally go back to the proof. If $I \oplus R^n = R^{n+1}$, then taking determinants shows that

$$\det I \otimes R = R,$$

so $\det I = R$. But this is I as I is of rank one. So I is free.

▲

40.11 Theorem. *A regular local ring is factorial.*

Let R be a regular local ring of dimension n. We want to show that R is factorial. Choose a prime ideal $\mathfrak{p}$ of height one. We'd like to show that $\mathfrak{p}$ is principal.

Proof. Induction on n. If $n = 0$, then we are done—we have a field.

If $n = 1$, then a height one prime is maximal, hence principal, because regularity is equivalent to the ring's being a DVR.

Assume $n > 1$. The prime ideal $\mathfrak{p}$ has height one, so it is contained in a maximal ideal $\mathfrak{m}$. Note that $\mathfrak{m}^2 \subset \mathfrak{m}$ as well. I claim that there is an element x of $\mathfrak{m} - \mathfrak{p} - \mathfrak{m}^2$. This follows as an argument like prime avoidance. To see that x exists, choose $x_1 \in \mathfrak{m} - \mathfrak{p}$ and $x_2 \in \mathfrak{m} - \mathfrak{m}^2$. We are done unless $x_1 \in \mathfrak{m}^2$ and $x_2 \in \mathfrak{p}$ (or we could take x to be x_1 or x_2). In this case, we just take $x = x_1 + x_2$.

So choose $x \in \mathfrak{m} - \mathfrak{p} - \mathfrak{m}^2$. Let us examine the ring $R_x = R[1/x]$, which contains an ideal $\mathfrak{p}[x^{-1}]$. This is a proper ideal as $x \notin \mathfrak{p}$. Now $R[1/x]$ is regular (i.e. its localizations at primes are regular local). The dimension, however, is of dimension less than n since by inverting x we have removed $\mathfrak{m}$. By induction we can assume that R_x is locally factorial.

Now $\mathfrak{p}R_x$ is prime and of height one, so it is invertible as R_x is locally factorial. In particular it is projective.

But $\mathfrak{p}$ has a finite resolution by R-modules (by regularity), so $\mathfrak{p}R_x$ has a finite free resolution. In particular, $\mathfrak{p}R_x$ is stably free and invertible, hence free. Thus $\mathfrak{p}R_x$ is **principal**.

We want to show that $\mathfrak{p}$ is principal, not just after localization. We know that there is a $y \in \mathfrak{p}$ such that y generates $\mathfrak{p}R_x$. Choose y such that $(y) \subset \mathfrak{p}$ is as large as possible. We can do this since R is noetherian. This implies that $x \nmid y$ because otherwise we could use y/x instead of y.

We shall now show that

$$\mathfrak{p} = (y).$$

So suppose $z \in \mathfrak{p}$. We know that y generates $\mathfrak{p}$ **after** x **is inverted.** In particular, $z \in \mathfrak{p}R_x$. That is, $zx^a \in (y)$ for a large. That is, we can write

$$zx^a = yw, \quad \text{for some } w \in R.$$

We chose x such that $x \notin \mathfrak{m}^2$. In particular, $R/(x)$ is regular, hence an integral domain; i.e. x is a prime element. We find that x must divide one of y, w if $a > 0$. But we know that $x \nmid y$, so $x \mid w$. Thus $w = w'x$ for some x. We find that, cancelling x,

$$zx^{a-1} = yw'$$

and we can repeat this argument over and over until we find that

$$z \in (y).$$

▲

40.12 Corollary. *Let $R = \mathbb{C}[x_1, \dots, x_n]/(f_1, \dots, f_m)$ for some polynomials f_i having linearly independent derivatives. Then the localization of R at any prime ideal is factorial. The theory of divisors thus goes into effect: Cartier divisors on* Spec$R$ *are the same thing as Weil divisors.*