MATH 221, FALL 2019

WITH BROOKE ULLERY

CONTENTS

PRELIMINARIES

These notes were taken during the fall semester of 2019 in Harvard's Math 221, *Commutative Algebra*. The course was taught by Dr. Brooke Ullery and transcribed by Julian Asilis. The notes have not been carefully proofread and are sure to contain errors, for which Julian takes responsibility. Corrections are welcome at `asilis@college.harvard.edu`.

1. LECTURE 1 — SEPTEMBER 4, 2019

Office hours are 11-1 on Tuesdays. The course is geared toward applications in algebraic geometry, which helps provide some context to the math we'll be learning. The goal is to get through chapters 1-13 of Eisenbud, but we might not cover everything. Topics include:

- Localization
- Primary decomposition
- Nullstellensatz
- Artin-Rees lemma
- Flat families/Tor
- Completions of rings
- Noether normalization
- Systems of parameters
- DVRs
- Dimension theory
- Hilbert-Samuel polynomials (maybe)

Before we get into things, let's discuss conventions and some of the motivation behind what we're doing. Naturally, all rings are commutative and unital. A ring homomorphism respects both operations and sends 1 to 1.

Notation 1.1. For R a ring, an ideal $I \neq R$ is *prime* if $fg \in I \implies f \in I$ or $g \in I$. I is *maximal* if it is not contained in any other proper ideals. R is a *local ring* if it has exactly one maximal ideal.

With regard to motivation, commutative algebra is kind of just arithmetic geometry in disguise. In this class, we'll try not to stay on one side of the algebra/geometry divide. One geometric example is $R = k[x_1, \ldots, x_n]$, for k an algebraically closed field ($k = \bar{k}$). The zero set of a polynomial, say $x_1^2 - x_2$ is a locus in k^n. Prime ideals will then correspond to subvarieties of affine space. More generally, the prime ideals of an arbitrary ring R correspond to the points of the scheme corresponding to R (called an affine scheme).

> "If you hear things you don't understand enough times, then you'll eventually understand them." - Dr. Ullery.

As it turns out, all varieties and schemes can be constructed by glueing *affine* varieties and schemes, which are those associated to rings. So commutative algebra really does give rise to lots of what's going on in algebraic geometry. Essentially, studying rings amounts to studying local algebraic geometry.

> "Commutative algebra is just local algebraic geometry." - Dr. Ullery.

How do local rings fit into this? They describe the geometry of a scheme/variety very close to a point. All of these statements will be made more precise later, but the idea right now is to give a high-level overview of some of the interplay between commutative algebra and algebraic geometry. To see more of the AG side, check out Smith's "An Invitation to Algebraic Geometry."

Now let's really get started. One of the most important kinds of rings is the Noetherian ring, because it tells us about how its ideals are generated. As an example of the importance of finite generation of ideals, for $k[x_1, \ldots, x_n]$ with k a field, the fact that every ideal

is finitely generated is equivalent to the fact that every variety in $\mathbb{A}^n$ is the intersection of finitely many hypersurfaces.

Definition 1.2. A ring R is *Noetherian* if every ideal of R is finitely generated.

Proposition 1.3. *R is Noetherian if and only if every strictly increasing chain of ideals terminates.*

Proof. If I is not finitely generated, we can choose $f_1 \in I$, $f_2 \in I \setminus (f_1)$, $f_3 \in I \setminus (f_1, f_2)$, and so on. So we have a strictly increasing infinite chain of ideals. In the other direction, if $I_1 \subsetneq I_2 \subsetneq \dots$ and $I = \cup I_i$ is finitely generated, then all of the generators are in one I_j so $I = I_j$. □

Example 1.4. All fields are Noetherian rings. So are $\mathbb{Z}$ and $\mathbb{Z}[x]$.

Theorem 1.5 (Hilbert Basis theorem)**.** *If R is Noetherian, then so is $R[x]$.*

Proof. First, two definitions: for $f = a_n x^n + \cdots + a_0 \in R[x]$ with $a_n \neq 0$, we say a_n is the *initial coefficient* and $a_n x^n$ is the *initial term*. Now let $I \subseteq R[x]$ and choose $f_1, f_2, \cdots \in I$ as follows:

1. Let $f_1 \neq 0 \in I$ be an element of least degree in I.
2. Let $f_2 \neq 0$ be an element of least degree in $I \setminus (f_1)$
3. Let $f_3 \neq 0$ be an element of least degree in $I \setminus (f_1, f_2)$

$\vdots$

If $(f_1, \dots, f_n) = I$, we're done. Otherwise, let a_j be the initial coefficient of f_j. Then $J = (a_1, a_2, \dots) \subset R$ is finitely generated. Let m be the smallest integer such that $J = (a_1, \dots, a_m)$.

The claim is that $I = (f_1, \dots, f_m)$. Otherwise, consider f_{m+1}. We have that $a_{m+1} = \sum_{\ell=1}^{m} u_\ell a_\ell$ for some $u_j \in R$. Since $\deg f_{m+1} \geq \deg f_j$ for $m \geq j$, we have

$$g = \sum_{j=1}^{m} u_j f_j x^{\deg f_{m+1} - \deg f_j} \in (f_1, \dots, f_m)$$

Now consider $f_{m+1} - g \in I \setminus (f_1, \dots, f_m)$. It has degree strictly less than that of f_{m+1}, producing contradiction.

□

Corollary 1.6. *Repeatedly applying the Hilbert basis theorem gives us that $R[x_1, \dots, x_n]$ is also Noetherian.*

Corollary 1.7. *If R is Noetherian and S is a finitely generated R-algebra, then S is Noetherian.*

Proof. Because S is a finitely generated R-algebra, $S = R[a_1, \dots, a_n]$ where the $a_i \in S$. In particular, $R[a_1, \dots, a_n]$ - which is Noetherian - surjects on to S. So any $I \subseteq S$ is generated by the images of the generators of its pre-image. □

Definition 1.8. An R-module M is *Noetherian* if its submodules are finitely generated.

Proposition 1.9. *If R is a Noetherian ring and M a finitely generated R-module, then M is a Noetherian module.*

Proof. Let $f_1, \ldots, f_n$ be generators for M and take $N \subseteq M$ a submodule. We induct on n. If $n = 1$, consider the map from R to M which sends 1 to f_1. Then the pre-image of N is an ideal, and the images of its generators generate N.

Supposing this holds for n up to k, we have M/Rf_1 is Noetherian. For $\overline{N}$ the image of N in M/Rf_1, $\overline{N}$, $\overline{N}$ is finitely generated by $g_1, \ldots, g_s$. $N \cap Rf_1$ is a submodule of Rf_1, so it's finitely generated by $h_1, \ldots, h_r$. So for $a \in N$, $\overline{a}$ is a linear combination of the $\overline{g_i}$. Then a is generated by the g_i and the h_j. □

Next time we'll talk a bit about graded modules and Hilbert functions, and after that we'll talk about Hom, tensors, and some slightly more category-theoretic stuff.

2. Lecture 2 — September 9, 2019

Today we're going to talk about graded rings and graded modules. Along with local rings, graded rings are going to be our bread and butter.

Definition 2.1. A *graded ring* is a ring R with a direct sum decomposition $R = R_0 \oplus R_1 \oplus \ldots$ with $R_i R_j \subseteq R_{i+j}$. An element $f \in R$ is *homogeneous* if $f \in R_i$ for some i. An ideal $I \subseteq R$ is *homogeneous* if it's generated by homogeneous elements.

Example 2.2.

$$\begin{aligned} R &= k[x_1, \ldots, x_n] \\ &= S_0 \oplus S_1 \oplus \ldots \end{aligned}$$

where S_d is the vector space of homogeneous polynomials of degree d. S_d is generated by all products of d variables.

Definition 2.3. For $R = R_0 \oplus \ldots$ a graded ring, a *graded R-module* is a module $M = \bigoplus_{-\infty}^{\infty} M_i$ such that $R_i M_j \subseteq M_{i+j}$.

Example 2.4. Let $R = k[x_1, \ldots, x_n]$.

1) If $I \subseteq R$ is a homogeneous ideal, then R/I is a graded module, with grading determined by $R \to R/I$.
2) Let $M = R$ with $M_{-1} = R_0$, $M_0 = R_1$, $M_i = R_{i+1}$, i.e. $\deg x_i = 0$. This shift in grading is referred to as a twist of R by 1, and write $M = R(1)$. More generally for M a graded module, $M(d) \cong M$ as modules and $M(d)_e = M_{d+e}$.

What's the geometric context? If $I \subseteq R$ is an ideal describing a variety X in projective space, then $\dim_k((R/I)_d)$ is the dimension of the space of homogeneous polynomials of degree d that vanish on X. So it's the dimension of the space of degree d hypersurfaces that contain X.

Definition 2.5. Let M be a finitely generated graded module over $R = k[x_1, \ldots, x_n]$. The *Hilbert function* of M is

$$H_M(s) = \dim_k M_S$$

Example 2.6. Take $M = R$ with the standard grading. Then $H_M(s) = \begin{cases} 0 & s < 0 \\ \binom{s+n-1}{n-1} & s \geq 0 \end{cases}$.

Example 2.7. Take $M = k[x,y]/(x^2, y^3)$. Then $M = M_0 \oplus M_1 \oplus M_2 \oplus M_3$ where $M_0 = (1), M_1 = (x,y), M_2 = (xy, y^2), M_3 = (xy^2)$. So $H_M(0) = \begin{cases} 1 & s = 0,3 \\ 2 & s = 1,2. \\ 0 & \text{else} \end{cases}$

So it looks like weird things can happen in low degrees and then things get nicer. In fact, it turns out that for large s, the Hilbert function eventually behaves like a polynomial.

Theorem 2.8 (Hilbert)**.** *If M is a finitely generated graded module over $k[x_0, \ldots, x_r]$, then $H_M(s)$ agrees with a polynomial of degree at most r for sufficiently large s.*

Proof. We assert that if $\tilde{H}(s) = H(s) - H(s-1)$ agrees with a polynomial over $\mathbb{Q}$ of degree at most $n-1$ for $s \geq s_0$, then $H(s)$ agrees with one of degree at most n for $s \geq s_0$. The proof is in Eisenbud.

Now we induct on the number of variables. If M is just a module over k, then it's a finite-dimensional vector space and $H_M(s) = 0$ for sufficiently large s. $r = -1$, so we'll say deg(0) = -1. Now say $r \geq 0$. Consider $M(-1) \to M$ given by multiplication by x_r. It preserves degree, so it's a graded morphisms. The cokernel of this map is M/x_rM and the kernel is $K(-1)$, where K is the kernel of the map $M \to M$ given by multiplication by x_r. We have a short exact sequence

$$0 \to K(-1) \to M(-1) \to M \to M/x_rM \to 0$$

Restricting focus to degree s gives us a short exact sequence (SES) on vector spaces. The alternating sum of degrees is zero, so $H_{M/x_rM}(s) - H_M(s) + H_M(s-1) - H_k(s-1) = 0$ Since x_r annihilates every element of K and M/x_rM, they are both finitely generated $k[x_0, \ldots, x_{r-1}]$-modules. So by induction, the outer terms agree for sufficiently large s with polynomials of degree $\leq r-1$.

Then so does $H_M(s) - H_M(s-1)$ and so $H_M(s)$ agrees with a polynomial of degree $\leq r$. □

Definition 2.9. The above polynomial is denoted $P_M(s)$, and is the *Hilbert polynomial* of M.

Returning to the geometric context, if $X \subseteq \mathbb{R}^r$ is a projective algebraic variety, then the degree of its Hilbert polynomial is equal to its dimension. Additionally, $d!$ times its initial coefficient is equal to the degree of the variety. Finally, Riemann-Roch from algebraic

geometry computes the Hilbert polynomial. The point is that there's lots of geometric data encoded in this polynomial.

Now we're going to change gears and talk about localization.

Definition 2.10. A *local ring* is a ring with exactly one maximal ideal.

Local rings can be partitioned into elements that live in the maximal ideal and elements that don't. If you're not in the maximal ideal, you have to generate the whole ring, so you're a unit. Conversely, everything in the maximal ideal is not a unit. Often times it's helpful to prove properties for rings by reducing to the local case - that's done by adding inverses so

Question 2.11. For a R a ring, for which elements can we 'add inverses'?

Well, if we add f^{-1} and g^{-1}, we also add $(fg)^{-1}$. So the set of elements whose inverses we add needs to at least be closed under multiplication. By convention, this includes the empty product of 1. For instance, if $t \neq 0 \in R$ then $\{1, t, t^2, \dots\}$ is multiplicatively closed. For $P \subseteq R$ an ideal, $R - P$ is multiplicatively closed iff P is prime. Likewise, $R \setminus \{0\}$ is multiplicatively closed iff R is an integral domain.

Definition 2.12. Let M be an R-module and $U \subseteq R$ be multiplicatively closed. The *localization of M at U*, $M[U^{-1}]$ or $U^{-1}M$, is the set of equivalence classes of pairs $m \in M$, $u \in U$, written $\frac{m}{u}$, with the equivalence relation

$$\frac{m}{u} \sim \frac{m'}{u'} \iff \exists v \in U \text{ s.t. } vu'm = vum' \text{ in} M$$

$M[U^{-1}]$ is an R-module with $\frac{m}{u} + \frac{m'}{u'} = \frac{u'm+um'}{uu'}$ and $r(\frac{m}{u}) = \frac{rm}{u}$. In fact, $M[U^{-1}]$ is an $R[U^{-1}]$ module in the obvious way: $(\frac{r}{u})(\frac{m}{u'}) = \frac{rm}{uu'}$.

For $U \subseteq R$ an arbitrary set, we can take its multiplicative closure $\overline{U}$ and define $M[U^{-1}] = M[\overline{U}^{-1}]$.

What happens if $u \in M, m \in M$ such that $um = 0$? Then $\frac{m}{1} = 0$, since $um = u0$. The converse holds as well.

Example 2.13.
1) In an integral domain, $R[(R \setminus 0)]^{-1}$ is the field of fractions of R, denoted $K(R)$.
2) More generally, if P is a prime ideal, we write $R_P := R[(R - P)^{-1}]$. This is a ring whose units are the elements which are not in P. It's a local ring. If M is an R-module, then $M_p := M[(R - P)^{-1}]$ is an R_p-module.

In fact, localization is a functor from R-modules to $R[U^{-1}]$-modules.

For $\phi : M \to N$ a map of R-modules and $U \subseteq R$ multiplicatively closed, there's a natural map $\phi[U^{-1}] : M[U^{-1}] \to N[U^{-1}]$ sending $\frac{m}{u}$ to $\frac{\phi(m)}{u}$.

For $L \xrightarrow{\psi} M \xrightarrow{\phi} N$, you should check that $(\phi \circ \psi)[U^{-1}] = \phi[U^{-1}] \circ \psi[U^{-1}]$.

3. Lecture 3 — September 11, 2019

We'll keep talking about localization today. Last time we defined localization for modules and rings, and we decided that localization is a functor. It has an associated universal property, which is the following: Let $\phi : R \to S$ be a ring homomorphism and $U \subseteq R$ be multiplicatively closed. If U gets sent to units in S, we can uniquely extend ϕ to a map ϕ' from $R[U^{-1}] \to S$ which sends $\frac{a}{b}$ to $\phi(a)\phi(b)^{-1}$.

That's not a great way to define localization, but it is useful for proving properties about localization. Let's talk more about what localizations look like. Let $\phi : R \to R[U^{-1}]$ be the natural map. If $I \subseteq R[U^{-1}]$ and $\frac{r}{u} \in I$, then $r \in I$. So all the numerators are in $\phi^{-1}(I)$ and in fact I is generated by $\phi^{-1}(I)$.

Then the map $I \mapsto \phi^{-1}(I)$ is an injection, since $\phi^{-1}(I)$ determines I. So what kinds of ideals in R take the form $\phi^{-1}(I)$ for $I \subseteq R[U^{-1}]$?

Proposition 3.1. *$J \subseteq R$ is the preimage of an ideal if and only if $J = \phi^{-1}(JR[U^{-1}])$.*

This won't be the case if and only if there's some $b \in J$ and $u \in U$ with $\frac{a}{1} = \frac{b}{u}$ and $a \notin J$. In other words, $u'(ua - b) = 0$ for some $u' \in U$. J is a preimage if and only if there is no $u \in U$ and $a \notin J$ such that $au \in J$. For instance, J is a preimage if J is prime and $U \cap J = \emptyset$.

Proposition 3.2. *The correspondence $I \mapsto \phi^{-1}(U)$ is a bijection on prime ideals avoiding U.*

Example 3.3. If $P \subseteq R$ is prime, then the prime ideals of R_P are in one-to-one correspondence with primes of R contained in P.

Corollary 3.4. *If R is Noetherian, so is $R[U^{-1}]$, because its ideals have the same generators as their preimages.*

It turns out that localization can be expressed as tensor product, which is closely related to Hom, its adjoint.

Definition 3.5. If M, N are R-modules, then $\mathrm{Hom}_R(M, N)$ is the R-module of homomorphisms $M \to N$.

Example 3.6. $\mathrm{Hom}_R(\oplus_{i=1}^n R, N) \cong \oplus_{i=1}^n N$, by looking at where each of the generators go.

Hom is a functor in each of its entries. Fixing an R-module M, $\mathrm{Hom}(M, -)$ is a covariant functor sending $A \to B$ to $\mathrm{Hom}(M, A) \to \mathrm{Hom}(M, B)$ by post-composing. It turns out that $\mathrm{Hom}(M, -)$ is *left-exact*, meaning it preserves left-exact sequences:

$$0 \to A \to B \to C \text{ maps to } 0 \to \mathrm{Hom}(M, A) \to \mathrm{Hom}(M, B) \to \mathrm{Hom}(M, C)$$

$\mathrm{Hom}(-, M)$, on the other hand, is a contravariant functor, since $A \to B$ goes to $\mathrm{Hom}(B, M) \to \mathrm{Hom}(A, M)$ by pre-composing. This functor sends right-exact sequences to left-exact sequences, which is pretty gnarly.

$$A \to B \to C \to 0 \text{ goes to } 0 \to \mathrm{Hom}(C, M) \to \mathrm{Hom}(B, N) \to \mathrm{Hom}(A, N)$$

Now let's talk tensor products.

Definition 3.7. For M, N R-modules, $M \otimes_R N$ is the R-module generated by elements of the form $m \otimes n$ with $m \in M, n \in N$ such that

- For $r \in R$, $(rm) \otimes n = m \otimes (rn) = r(m \otimes n)$
- $(m + m') \otimes n = m \otimes n + m' \otimes n$ and likewise $m \otimes (n + n') = m \otimes n + m \otimes n'$

The above relations are all we have, meaning that in general, elements of $M \otimes_R N$ look like finite sums $\sum_i m_i \otimes n_i$. It's often times hard to tell whether different elements are equal.

Example 3.8.
1) $R \otimes_R M \cong M$, since anything can be written $1 \otimes m$ by scaling appropriately using an element of R. Likewise, $M \cong M \otimes_R R$.
2) $R[x_1, \ldots, x_m] \otimes_R R[x_{m+1}, \ldots, x_n] \cong R[x_1, \ldots, x_n]$
3) $\mathbb{Q} \otimes_{\mathbb{Z}} \mathbb{Z}[x] \cong \mathbb{Q}[x]$
4) For $I, J \subseteq R$ ideals, $R/I \otimes_R R/J \cong R/(I + J)$
5) For M an R-module and S an R-algebra, then $S \otimes_R M$ is an S-module with $s(t \otimes m) = st \otimes m$

Again we'll find that its useful to equip ourselves with a universal property in order to prove properties of the tensor product. First note that the function (not morphism) $\otimes : M \times N \to M \otimes N$ defined by $(m, n) \mapsto m \otimes n$ is bilinear over R.

In fact, given another bilinear $f : M \times N \to P$, there exists a unique $\hat{f} : M \otimes N \to P$ such that $\hat{f} \circ \otimes = f$. This is the universal property of the tensor product.

The tensor product is a functor on both sides, and it's right-exact.

$$A \to B \to C \to 0 \text{ maps to } A \otimes M \to B \otimes M \to C \otimes M \to 0$$

Lemma 3.9. *The map $R[U^{-1}] \otimes M \to M[U^{-1}]$ defined $\frac{r}{u} \otimes m \mapsto \frac{rm}{u}$ is an isomorphism.*

Proof. Define $\phi : M[U^{-1}] \to R[U^{-1}] \otimes_R M$ by $\frac{m}{u} \mapsto \frac{1}{u} \otimes m$. First we need to check that this map is well-defined. Say $\frac{m}{u} = \frac{m'}{u'}$. Then $vu'm = vum'$ for some $v \in U$, meaning $vu' \otimes m = vu \otimes m'$, so $\frac{1}{u} \otimes m = \frac{1}{u'} \otimes m'$. This is the inverse to the above function. □

Since we've written localization as a tensor product, we know it's right-exact. We'll also show it preserves injections, meaning it straight up preserves exact sequences. This property is called flatness

Definition 3.10. An R-module F is *flat* if for every inject $M \to N$, $F \otimes M \to F \otimes N$ is also injective.

We want to show that tensoring by the localization of our ring is always flat.

Proposition 3.11. *$R[U^{-1}]$ is flat as an R-module. Thus, localization preserves exact sequences.*

Proof. Let $\phi : M' \to M$ be an injection of R-modules. We'd like to show that $R[U^{-1}] \otimes_R M' \to R[U^{-1}] \otimes_R M$ is injective. If $\frac{m'}{u} \mapsto \frac{\phi(m')}{)} u = 0$, then $v\phi(m') = 0$ for some $v \in U$, meaning $\phi(vm') = 0$. So $vm' = 0$ and $\frac{m'}{u} = 0$, as desired. □

As we've already mentioned, many properties of modules and rings can be verified by 'checking locally'. A geometric example of this is that a variety's smoothness is verified by checking smoothness at each point. There's an algebraic analogue we note state:

Lemma 3.12. *For R a ring and M an R-module,*

a) If $a \in M$, then $a = 0 \iff \frac{a}{1} = 0$ in M_m for each maximal ideal $m \subseteq R$.
b) $M = 0 \iff M_m = 0 \; \forall$ maximal ideals $m \subseteq R$.

Proof. a) $\frac{a}{1} = 0$ in $M_m \iff$ the annihilator I of a (the ideal I with $ra = 0 \forall r \in I$) is not contained in m. So $\frac{a}{1} = 0 \iff I = R \iff a = 0$ in M.
b) $M = 0 \iff a = 0 \forall a \in M \iff a/1 = 0$ in all M_m

□

Injectivity and surjectivity can also be checked locally.

Corollary 3.13. *A map $\phi : M \to N$ of R-modules is injective (resp. surjective) iff $\phi_m : M_m \to N_m$ is injective (resp. surjective) $\forall$ maximal ideals m.*

Proof. The forward direction follows from flatness. On the other hand, if $\ker(\phi_m) = (\ker \phi)_m = 0 \; \forall m$, then $\ker \phi = 0$. Likewise with cokernels. □

4. Lecture 4 — September 16, 2019

Let's talk about radical ideals. Last time we saw that the complement of a prime ideal is a multiplicative set. The converse, however, does not hold - there are multiplicative sets which do not arise as the complement of a prime ideal.

Example 4.1. $\{1, x, x^2, \dots\} \subseteq k[x]$ is multiplicatively closed, but its complement isn't an ideal (it doesn't contain 1).

However, there is a partial converse - ideals that are maximal in the complement of a multiplicatively closed set are prime. It usually turns out that the maximal ideals in some set of ideals are prime.

Proposition 4.2. *Suppose U is multiplicative and $I \subseteq R$ is an ideal not meeting U which is maximal amongst ideals which do not meet U. Then I is prime.*

Proof. Let's look at $IR[U^{-1}]$, which is maximal. Its preimage in R, call it P, is prime (preimage of prime is always prime). But $P \supseteq I$, so $I = P$. □

What does any of this have to do with radical ideals? Well, if $I \subseteq R$ is an ideal and $\exists a \notin I$ such that $a^n \notin I \; \forall n$. Then there's a prime ideal P containing I which does not a, by the previous result. On the other hand, if $a^n \in I$ for some n, then any prime P containing I contains a.

Corollary 4.3. *If $I \subseteq R$ is an ideal, then $\{f | f^n \in I \text{ for some } n\} = \bigcap_{P \supseteq I,\, P \text{ prime}} P$.*

Definition 4.4. The set $\{f | f^n \in I$ for some n$\}$ is called the *radical* of I, and denoted rad$I$ or $\sqrt{I}$.

Since we've witnessed the radical as an intersection of ideals, it is itself an ideal. The radical of 0 is the nilradical, the set of all nilpontent elements. One result is that $\text{rad}(0) = \bigcap P \text{ prime} P$, since all primes contain $(0) = 0$.

Definition 4.5. R is *reduced* if $\text{rad}(0) = (0)$.

Example 4.6. $k[x]/(x^2)$ isn't radical, because $\text{rad}(0) = (x)$

Remark 4.7. Note that $\text{rad}(0)$ is not in general prime. For instance, $\text{rad}(0)$ in $\mathbb{Z}/12\mathbb{Z}$ is generated by 6, which isn't prime.

More generally, if R is a UFD and $f_1, \ldots, f_n$ are irreducible elements generating distinct ideals and $g = f_1^{k_1} \ldots f_n^{k_n}$ with $k_i \geq 1$, then $\text{rad}(0)$ in $R/(g)$ is $(f_1 \ldots f_n)$.

There's a functor Spec that associates geometric objects to rings.

Definition 4.8. For R a ring, let $\text{Spec}(R)$ denote the set of prime ideals of R. It has the structure of a space when endowed with the *Zariski topology* - for any subset $I \subseteq R$, we define $V(I) := \{P \in \text{Spec}R | I \subseteq P\}$. The $V(I)$ are Zariski-closed.

Proof. a) $\bigcap_\lambda V(I_\lambda) = V(\sum_\lambda . I_\lambda)$

b) $V(I) \cup V(J) = V(I \cap J) = V(IJ)$

□

Since $V(I) = V((I))$, we restrict focus to ideals as inputs to V. In fact, amongst ideals we can restrict focus to radicals, as $V(I) = V(\text{rad}I)$. So what does Spec$R$ look like? Notice that a singleton $\{P\}$ in Spec$R$ is closed if and only if P is maximal. The subset of R's maximal ideals is written $\text{maxSpec}(R)$.

Example 4.9.

1) R = k[x]. Then Spec$R = \{f(x) | f \text{ irreducible}\}$. If k is algebraically closed, then these are in 1-to-1 correspondence with the elements of k. Using the fact that $k[x]$ is a PID and that irreducible polynomials are exactly those of the form $x - a$.
2) Again assuming $k = \bar{k}$, consider $\text{maxSpec}(k[x, y]) = \{(x - a, y - b) | a, b \in k\}$. Closed points are in bijection with k^2. The other points correspond to curves defined by irreducible polynomials $f(x, y)$. Looking at $\mathbb{A}^2 = \text{Spec}k[x, y]$ more generally, we have that the closure of a point like $f(x, y)$ includes all closed points $(x - a, y - b)$. such that $f(a, b) = 0$.

It turns out that Spec is a contravariant functor from **Ring** to **Top**. A morphism $\phi : R \to S$ induces a map $\text{Spec}(S) \to \text{Spec}(R)$ by preimaging. This map is continuous because pre-images of closed sets are closed. In particular, $(\text{Spec}\phi)^{-1}(V(I)) = V(\phi(I))$.

We've seen that prime ideals of R/I and $R[U^{-1}]$ are in correspondence with certain subsets of Spec$R$.

Proposition 4.10. *(1) The map $Spec(R/I) \to Spec(R)$ is a homeomorphism of $Spec(R/I)$ with $V(I) \subseteq Spec(R)$.*
(2) The map $Spec(R[U^{-1}]) \to Spec(R)$ is a homeomorphism of $Spec(R[U^{-1}])$ with $\{P | U \cap P = \emptyset\} \subseteq Spec(R)$.

Proof. Probably on PSet 2. □

Definition 4.11. An R-module M is *Artinian* if every strictly decreasing chain of submodules terminates.

The definition for rings is analogous. It turns out that the Artinian property for rings is stronger than the Noetherian.

Definition 4.12. Let $M = M_0 \supsetneq M_1 \supsetneq \cdots \supsetneq M_n$ be a chain of submodules of length n. The chain is a *composition series* if $M_n = 0$ and M_j/M_{j+1} is a nonzero simple module, meaning it has no nonzero proper submodules.

Definition 4.13. The *length* of an R-module M is the least length of a composition series, and ∞ if it has no finite composition series.

It'll turn out later that we can remove the word 'least' from the above definition, as all composition series for a module have the same length. Note that since M_i/M_{i+1} is simple, it's generated by any of its nonzero elements. So there's a map $R \to M_i/M_{i+1}$ sending 1 to a with kernel $\text{ann}(M_i/M_{i+1}) = \{r \in R | r(M_i/M_{i+1}) = 0\}$.

5. Lecture 5 — September 18, 2019

Recall that a composition series with respect to an R-module M is a chain $M = M_0 \supsetneq \cdots \supsetneq M_n = 0$ such that M_i/M_{i+1} is simple.

Theorem 5.1. *M has a finite composition series if and only if it is Artinian and Noetherian.*

Proof. If M is Noetherian, we can find a maximal proper submodule M_1, a maximal proper submodule $M_2 \supsetneq M_1$, and so on. Because M is Artinian, this procedure terminates in finitely many steps.

In other direction, we make use of the following claim: If M has a finite composition series of length n then every chain of submodules has length at most n and can be refined to a composition series. To see why, take $M' \subsetneq M$ a proper submodule. Then $M' = M_0 \cap M' \supset M_1 \cap M' \supset \cdots \supset M_n \cap M' = 0$. We can show by induction that if these are all proper containment, $M' \supset M_0$. Suppose $M = N_0 \supsetneq \cdots \supsetneq N_k$. We want to show $k \leq n$. If $n = 0$, then $M = 0$ and we're done. But length $N_1 <$ length$M$. By induction, $k - 1 < n - 1$ and we're done. □

Now let's look more at the Artinian property, and see what we can say about the geometry of rings that are Artinian.

Theorem 5.2. *For R a ring, the following are equivalent:*
a) R is Noetherian and all its prime ideals are maximal.
b) R is a finite length R-module
c) R is Artinian

Proof.

$a) \implies b)$ Suppose R of finite ideal. Let $I \subseteq R$ be an ideal maximal with respect to the property that R/I is not of finite length. 0 satisfies the property, and we can take such a maximum because R is Noetherian. We'd like to show that I is prime. Take $a, b \in R$ with $ab \in I$. Consider $I + (a) \supset I$. If $a \notin I$, then the containment is proper, so $R/I + (a)$ has finite length. So we have

$$0 \to I + (a)/I \to R/I \to R/I + (a) \to 0$$

Notice that $R/(I : a) \to I + (a)/I$ is an isomorphism. If $b \notin I$ then $(I : a) \supsetneq I$, so $R/(I : a)$ has finite length. Combining composition series, we have that R/I has finite length, producing contradiction. So I is prime and thus maximal, meaning R/I is a field and R has finite length.

$b) \implies c)$ Follows from previous theorem.

$c) \implies a)$ Suppose R is Artinian. Then we claim (0) is a product of maximal ideals. Choose a minimal ideal J with respect to the ideal being a product of maximal ideals - this exists by the Artinian property. Then for any maximal $m \subseteq R$, $mJ = J$. So $J \subseteq M$, and $J^2 = J$.

Now choose an ideal I minimal among ideals not annihilating J. Then $(IJ)J = IJ^2 = IJ \neq 0$. But $IJ \subseteq I$, so by minimality of I, $IJ = I$ (since IJ fails to annihilate J). Now choose $f \in I$ such that $fJ \neq 0$. By minimality, $(f) = I$. Since $IJ = I$, $\exists g \in J$ such that $f = fg$, meaning $f(1 - g) = 0$. g is in e very maximal ideal, so $1 - g$ is in none (you could add them and get 1, generating the whole ring). Then $1 - g$ is a unit, so $f = 0$ and $J = 0$.

So the claim is proven, and we have $(0) = m_1 \dots m_t$ for m_i maximal. For any s, $(m_1 \dots m_s)/(m_1 \dots m_{s+1})$ is a vector space over R/m_{s+1}. Any descending chain of subspaces corresponds to a chain of ideals in R, which is finite, so the vector space is finite-dimensional. Putting together the composition series for $m_1/m_1m_2, m_1m_2/m_1m_2m_3, \dots$ we get a finite composition series for R. So R has finite length, and it's Noetherian.

Now suppose that P is prime. Then it contains $0 = m_1, \dots, m_t$. So P contains one of these maximal ideals, and it's that maximal ideal itself. So every maximal ideal is one of the m_i, and there are only finitely many maximal ideals.

□

Corollary 5.3. *Artinian rings are Noetherian. In addition, R is Artinian $\implies$ specR is finite.*

Now what does this all mean geometrically? If we take R to be a k-algebra with $k = \overline{k}$ (e.g. $k[x_1, \dots, x_n]/I$). Then $R \cong k^\ell$ as k-vector spaces and ℓ equals the length of R, as well as the number of points of spec$R$ (up to multiplicity).

Example 5.4. (1) If $R = k[x,y]/(x,y)$, then spec$R = 0$ and R has length 1, corresponding to $R \supset (0)$.
(2) If $R = k[x]/(x(x-1))$, then spec$R = \{(x),(x-1)\}$. Here R is generated as a k-vector space by 1 and x. So $R \cong k^2$ and it has composition series $R \supsetneq (x) \supsetneq (0)$.
(3) Let $R = k[x,y]/(x,y^2)$. Then spec$R = \{(x,y)\}$, but $R \cong k^2$ (generated by 1 and y), and R has the composition series $R \supsetneq (y) \supsetneq (0)$.

The takeaway from the above examples is that spec doesn't tell us everything about the ring. Roughly speaking, spec$R$ corresponds to a "scheme-y" point.

6. Lecture 6 — September 23, 2019

Today we'll talk about associated primes. The motivation is that for $n \in \mathbb{Z}$, we can exhibit a prime factorization $n = \pm p_1^{d_1} \dots p_t^{d_t}$. In fact, in $\mathbb{Z}$, $(n) = (p_1^{d_1}) \cap \dots \cap (p_t^{d_t})$. The "associated primes" of the ideal (n) in this case are the (p_i) and the primary components are the $(p_i^{d_i})$. Over $\mathbb{Z}$, the Fundamental Theorem of Arithmetic tells us that the primes and primary components are unique. Over uglier rings, we don't always get unique factorization but we can hope to somehow extend this kind of thinking.

As always, let's try to pull this back to geometry. Take $R = k[x_1, \dots, x_n]$, $I \subseteq R$ an ideal.

Definition 6.1. $V(I)$ is *reducible* if it can be written $V(I) = V(I_1) \cup V(I_2)$ where $V(I) \neq V(I_i)$. Otherwise, it's *irreducible*.

Proposition 6.2. *$V(I)$ is irreducible if and only if $\sqrt{I}$ is prime.*

Proof. If $V(I) = V(\sqrt{I}) = V(I_1) \cup V(I_2)$, then primeness of $\sqrt{I}$ means it's in, say, $V(I_1)$. Then $V(I_1) \supset V(\sqrt{I})$, and in fact they're equal.

If $\sqrt{I}$ is not prime, then $fg \in \sqrt{I}$ for $f, g \notin \sqrt{I}$. For $P \in V(\sqrt{I})$, $f \in P$ or $g \in P$. Then $V(\sqrt{I}) = V(\sqrt{I}, f) \cup V(\sqrt{I}, g)$. Neither of the sets on the RHS equal $V(\sqrt{I})$, since $f, g \notin \sqrt{I} = \cap_{P \supset I \text{ prime}} P$. □

We'll see that $\sqrt{I}$ can be written as a finite intersection of primes uniquely, corresponding to writing $V(I)$ as the union of irreducible sets.

Example 6.3. Consider $I = (x^2, xy) \subseteq k[x,y]$. $V(I) = V(x^2) \cap V(xy)$. We'll see that the associated primes are (x) and (x,y). We also have that $I = (x) \cap (x^2, y) = I(x) \cap (x^2, xy, y^2)$. Note that we can't write I uniquely as the intersection of ideals generated by powers of primes, like we could over $\mathbb{Z}$.

Definition 6.4. Let R be a ring and M an R-module. A prime P of R is *associated* to M if there's some $x \in M$ such that $P = \text{ann}(x) = \{r \in R : rx = 0\}$.

The set of all primes associated to M is denoted $\text{Ass}_R(M)$ or Ass$M$ if the ring is clear. Sometimes the associated primes of R/I over R are called associated primes of I.

Remark 6.5. If $P \in \text{Ass}M$, then $P = \text{ann}(x)$ and the map $R \to M$ which multiplies by r has kernel P, so R/P is a sumbodule of M. Conversely, if P is prime such that there's an inclusion of modules $R/P \to M$, then P is the annihilator of the image of 1. In short, $P \in \text{Ass}M$ if and only if R/P is isomorphic to a submodule of M.

Theorem 6.6. *Let R be a Noetherian ring and $m \neq 0$ a finitely generated R-module. Then*

a) $AssM$ is finite and non-empty. It includes all primes minimal among those containing $annM$.
b) The union of all associated primes equals the zero divisors on M (including 0 itself).
c) Taking associated primes commutes with localizing. In particular,

$$Ass_{R[U^{-1}]}M[U^{-1}] = \{PR[U^{-1}] | P \in AssM, P \cap U \neq \emptyset\}$$

How do we know that we can find primes minimal over an ideal? Let $\{Q_i\}$ be a chain of prime ideals containing I. If $ab \in \cap Q_i$, then one of a or b is in all the Q_i, so $\cap Q_i$ is prime. So Zorn's lemma implies that there exist minimal primes over I. Note that this holds over arbitrary rings.

Definition 6.7. The primes in the associated primes that are not minimal are called *embedded* primes of M. If $M = R/I$, then if P is an embedded prime of M in R, $V(P)$ is called an *embedded component* of $\text{Spec}(R/I)$. If P is a minimal associated prime in R, then $V(P)$ is an isolated component of $\text{Spec}(R/I)$.

Example 6.8. $I = (x^2, xy) \subseteq R = k[x, y]$. What is $\text{Ass}(R/I)$? The only nonzero elements annihilated are multiples of x or y. So $\text{ann}(x) = (x, y)$ and $\text{ann}(y) = (x)$. Then $\text{Ass}_R(R/I) = \{(x), (x, y)\}$.

Theorem 6.9 (Prime avoidance)**.** *Let $J, I_1, \ldots, I_n$ be ideals in R. Suppose $J \subseteq \cup_j I_j$. If R contains an infinite fields or at most two of the I_j are not prime, then $J \subseteq I_j$ for some j.*

Proof. First suppose R contains an infinite field k. Then R is a k-vector space, so J is a k-vector space, and if it's contained in the union of finitely many subspaces it must be in one of them.

If at most two I_j are not prime, we induct on n. If $n = 1$, we're done. By induction, if J is in any smaller union of the I_j, we're set. So assume instead that J is in no smaller union. Then for each i, there exists $x_i \in J$ such that $x_i \in I_i$ but $x_i \notin I_j$ for any $j \neq i$. If $n = 2$, then $x_1 + x_2$ is not in I_1 or I_2, which is a contradiction. If $n > 2$, then at least one the I_j is prime, say it's I_1. Then consider $x_1 + x_2 x_3 \ldots x_n$. The second term is not in I_1, because none of its terms are, and it's also not in any of the I_j (because then $x_1 \in I_j$). So the term is not in any of the I_i, a contradiction. □

What's implied is that if I is not contained in any of a finite number of primes, there exists an $x \in I$ that 'avoids all of the primes' (i.e. it's not in their union).

Corollary 6.10. *Let R be Noetherian, $I \subseteq R$ an ideal, and $M \neq 0$ a finitely generated R-module. Either I contains a nonzero divisor on M or I annihilates an element of M.*

Proof. If I is in the union of associated primes, it's equal to an annihilator. Otherwise, it contains a nonzero divisor on M. □

Proposition 6.11. *Let R be a ring and $M \neq 0$ an R-module. If $I \subseteq R$ is maximal among ideals of R that are annihilators of elements of M, then I is prime. In particular, if R is Noetherian then $AssM \neq \emptyset$.*

Proof. Consider $ab \in I$. Say $I = \text{ann}(x)$. Suppose $b \notin I$. Then $bx \neq 0$, but $abx = 0$. So $(I, a) \subseteq \text{ann}(bx)$. By maximality, $a \in I$ so I is prime. □

This proves part b) of the theorem, because every zero divisor lives in some associated prime. Recall that we showed that $0 = x \in M$ if and only if $x \mapsto 0$ in M_m for all maximal ideals $m \subseteq R$. We can say something slightly stronger when R is Noetherian.

Corollary 6.12. *R Noetherian, M an R-module. If $x \in M$ then $x = 0$ if and only if $\frac{x}{1} = 0$ in each M_p for maximal associated primes P.*

Proof. We've proven the forward direction. Now suppose $x \neq 0$. Then since R is Noetherian, there exists a prime $P \in \text{Ass}M$ that's maximal among annihilators of elements containing $\text{ann}(x)$. Then $\frac{x}{1} \neq 0$ in M_p. □

7. Lecture 7 — September 25, 2019

We're interested in how associated primes behave in short exact sequences (SES), since SES can show up a lot.

Lemma 7.1. *Let R be Neotherian. If*

$$0 \to M' \to M \to M'' \to 0$$

is a SES of R-modules, then $AssM' \subseteq AssM \subseteq AssM'' \cup AssM'$.

Proof. The first containment is clear. For the second, let $P \in \text{Ass}M \setminus \text{Ass}M'$. Then $P = \text{ann}(x)$ for an $x \in M$ and $Rx \cong R/P$. For $0 \neq \overline{y} \in R/P$, $a\overline{y} = 0 \iff a \in P$, since P is prime. So every nonzero element of Rx has annihilator P. So $Rx \cap M' = 0$, and thus Rx is isomorphic to its image in M and $P \in \text{Ass}M$. □

Proposition 7.2. *If R is Noetherian and M a finitely generated R-module, then M has a filtration*

$$0 = M_0 \subseteq M_1 \subseteq \cdots \subseteq M_n = M$$

with each $M_{i+1}/M_i \cong R/P_i$ for some prime P_i.

Proof. Since R is Noetherian, if $M \neq 0$ then $\text{Ass}M \neq 0$. Let $P_1 \in \text{Ass}M$. There exists a submodule $M_1 \cong R/P_1$. Repeating with M/M_1 gives us M_2, and so on. The procedure terminates because N is Noetherian. □

Recall parts a) and c) of our big theorem from last time. Under the assumption that R is Noetherian and $M \neq 0$ a finitely generated R-module, we saw that

a) $\text{Ass}M$ is finite, non-empty, each containing $\text{ann}(M)$, and it includes all primes minimal among those containing $\text{ann}M$.
c) If U is multiplicatively closed, then $\text{Ass}_{R[U^{-1}]}M[U^{-1}] = \{PR[U^{-1}] | P \in \text{Ass}M, P \cap U \neq \emptyset\}$

Proof of c). If $P \in \text{Ass}M, P \cap U \neq \emptyset$, then $R/P \to M$ is an injection. Localizing, we get an injection $R[U^{-1}]/PR[U^{-1}] \to M[U^{-1}]$. We're using the fact that localization commutes with quotients. So it follows that $PR[U^{-1}]$ is prime and thus $PR[U^{-1}] \in \text{Ass}M[U^{-1}]$.

Conversely, if $Q \in \text{Ass}M[U^{-1}]$, we can write $Q = PR[U^{-1}]$ for some prime P of R with $P \cap U \neq \emptyset$. Agh I got lost here. At some point we used the fact that localization commutes with Hom. □

Proof of a). For finiteness, we can find $0 = M_0 \subseteq M_1 \subseteq \cdots \subseteq M_n = M$ with $M_{i+1}/M_i \cong R/P_i$ for some P_i prime. We induct on the length of the filtration. When $n = 1$, $M = R/P_1$ ... agh I also zoned out here :(□

Now we'll talk about primary decomposition, and look to bring some geometric intuition into things. Classically, primary decomposition is defined for ideals in rings, but it can be defined more generally for arbitrary modules (and that's what we'll do).

Definition 7.3. A submodule $N \subseteq M$ is *primary* if $\text{Ass}(M/N)$ consists of one element, P. In this caes, N is P-primary. On the other hand, M is *coprimary* if $0 \subseteq M$ is primary, i.e. $|\text{Ass}M| = 1$.

Proposition 7.4. *If $P \subseteq R$ is prime and $N_1, \ldots, N_t \subseteq M$ is a collection of R-modules, then if each N_i is P-primary in M, then $\cap N_i$ is P-primary.*

Proof. Induction allows us to assume $t = 2$ (whittle down the intersection in parts). Then $M/(N_1 \cap N_2) \hookrightarrow M/N_1 \oplus M/N_2$. So the associated primes of the LHS lives in those of the RHS. But those on the RHS are just the union of those associated to M/N_1 and to M/N_2. That comes out to just P. Since Ass of the LHS isn't empty, it's P. So $N_1 \cap N_2$ is P-primary. □

Proposition 7.5. *Let $P \subseteq R$ be prime. The following are equivalent.*

a) M is P-coprimary
b) P is minimal over ann$M$ and every element not in P is a nonzero zero-divisor on M
c) A power of P annihilates M and every element not in P is a non-zero zero divisor on M.

Proof. a) $\implies$ b): $\{P\} = \text{Ass}M$, so it must be minimal over ann$M$. Then P consists of all zero divisors on M, including 0. □

Note that if $M = R/I$ for some $I \neq 0$, then I is P-primary if and only if a power of P is in I and $\forall r, s \in R$ such that $rs \in I,\ r \notin P$ implies $s \in I$.

Example 7.6. (x^2, y) is (x, y)-primary, but it's not (x)-primary.

8. Lecture 8 — September 30, 2019

Last time we talked about what it means for a submodule to be primary. For the rest of the lecture, R is Noetherian and $M \neq 0$ is a finitely generated R-module. Recall that $N \subseteq M$ is P-primary if $\text{Ass}(M/N) = \{P\}$. We also saw that M is P-coprimary if $\text{Ass}(M) = \{P\}$. We showed that the the following are equivalent:

1) M is P-coprimary

2) P is minimal over $\text{ann}(M)$ and every element not in P is a non-zero divisor in M.
3) A power of P annihilates M and every element not in R is a non-zero zero divisor on M.

Notice that 2) implies that M is P-coprimary if and only if P is minimal over $\text{ann}(M)$ and $M \hookrightarrow M_p$. So if M is any module and P is minimal over $\text{ann}(M)$, then $M' = \ker(M \to M_p)$ is P-primary since $M/M' \hookrightarrow M_p = (M/M')_p$. In this case, M' is the P-primary component of 0 in M.

Example 8.1. $I = (x^2y) \subseteq k[x,y]$, $M = k[x,y]/I$. The minimal primes in $k[x,y]$ over $\text{ann}M = I$ are (x) and (y). And $\ker(M \to M_{(x)}) = \{\frac{r}{u} | vr = 0, v \notin (x)\} = (x^2)$. Similarly, $\ker(M \to M_{(y)}) = (y)$. And $(x^2y) = (x^2) \cap (y)$, though this won't always be the case.

Example 8.2. Take $I = (x^2, xy)$ and $M = k[x,y]/I$. The only minimal prime over I is (x), and $\ker(M \to M_{(x)}) = (x)$, but this time $I \neq (x)$.

Note that our theorem says that when I is P-primary, P is minimal over I and thus $\sqrt{I} \subseteq P$. We also have that I being P-primary means $P^n \subseteq I$ for some n, and $P \subseteq \sqrt{I}$. Then $P = \sqrt{I}$. However, our previous example demonstrates that the converse is false - I need not be primary only because its radical is prime.

Theorem 8.3. *Any proper submodule $M' \subsetneq M$ is the intersection of finitely many primary submodules. If $P_1, \ldots, P_n$ are prime and $M' = \cap_{i=1}^n M_i$ with M_i P_i primary, then*

a) Every associated prime of M/M' occurs among P_i.
b) If the intersection is irredundant (i.e. no M_i can be dropped), then the P_i are exactly the associated primes (perhaps repeated).
c) If the intersection is minimal (i.e. no intersection with fewer terms), then each associated prime of M/M' is equal to exactly one P_i.

And if P_i is minimal over the annihilator of M/M', then M_i is the P-primary component of 0 in M'.

Proof. $N \subseteq M$ is *irreducible* if N is not the intersection of two strictly larger submodules. By the ascending chain condition, every submodule can be written as the intersection of finitely many irreducible submodules.

So we can write $M' = \cap M_i$ with each M_i irreducible. If M_i isn't primary, then there exists P and Q distinct associated primes of M/M'. Then R/Q and R/P inject into M/M'. The annihilator of every element of R/P is P and of R/Q is Q.

Then the images of R/Q and R/P don't intersect in M/M_i (or rather they intersect only at 0). Then 0 is reducible and M_i is reducible and thus primary.

So we have a primary decomposition. To show a) through c), we factor out M' and assume $M' = 0$. For part a), we take $0 = \cap M_i$ a primary decomposition. Then $M = M/\cap M_i \to \oplus M/M_i$ is an injection since $m \mapsto 0$ if and only if $m \in M_i$ if and only if $m = 0$. So $\text{Ass}M \subseteq \cup \text{Ass}M/M_i = \{P_i\}$.

For b), we have $\forall j$, $\cap_{i\neq j} M_i \neq 0$. Then if $A \cap_{i\neq j}$ and $B = M_j$, $A \cap B = 0$. The second isomorphism theorem gives us that

$$A = A/A \cap B \cong (A+B)/B \subseteq M/B = M/M_j$$

So M_j is P_j-primary, and M/M_j is P_j-coprimary. We have that Ass$A \subseteq$ Ass$M$ and thus $P_j \in$ Ass$M$. We're making use of the fact that the set of associated primes can't be empty, and results about how associated primes behave in SES. The proof of c) is a bit of a pain. □

What do localizations tell us about primary decompositions? Suppose we have a minimal decomposition $M' = \cap_{i=1}^n M_i$ and $\{P_i\}$ are the corresponding primes. Let $U \subseteq R$ be a multiplicatively closed set and reindex so that $P_1, \ldots, P_t$ are the P_i not meeting U.

Proposition 8.4. *$M'[U^{-1}] = \cap_{i=1}^t M_i[U^{-1}]$ is a minimal primary decomposition over $R[U^{-1}]$.*

Proof. Again we factor out M' and reduce to the case $M' = 0$. If $U \cap P_i \neq \emptyset$ then Ass$(M/M_i)[U^{-1}] = \{P_i R[U^{-1}]\}$ so $M_i[U^{-1}]$ is $P_i R[U^{-1}]$-primary. If $U \cap P_i \neq \emptyset$, then $(M/M_i)[U^{-1}] = 0$ and $M_i[U^{-1}] = M[U^{-1}]$. Then $\cap_{i=1}^t M_i[U^{-1}] = 0$ is a primary decomposition. Since the associated primes of $M[U^{-1}]$ are those in Ass$M$ which don't meet U, this decomposition is minimal. □

9. Lecture 9 — October 2, 2019

We've seen that modules can be written as intersections of primary submodules. Now let's look at primary decomposition in UFDs.

Proposition 9.1. *Let R be Noetherian and an integral domain.*

a) If $f \in R$ and $f = u\prod p_i^{e_i}$ with u a unit and each p_i a prime generating distinct ideals, then $(f) = \cap(p_i^{e_i})$ is a minimal primary decomposition.
b) R is a UFD if and only if every prime ideal minimal over a principal ideal is principal.

Proof. a) First we show that $(p_i^{e_i})$ is (p_i)-primary. Clearly a power of (p_i) annihilates $R/(p_i^{e_i})$. If $r \in R \setminus (p_i)$ and $\overline{m} \in R/(p_i^{e_i})$ such that $r\overline{m} = 0$, then $p_i^{e_i} | rm$. Since p_i doesn't divide r, we have that $\overline{m} = 0$.

Clearly $(f) \subseteq \cap(p_i^{e_i})$. To show the opposite direction, we induction on the number of indices n. If $n = 1$, the result is clear. For the inductive step, we show $(g) \cap (p_1^{e_1}) \subseteq (f)$, where $g = u\prod_{i\neq 1} p_i^{e_i}$. Let $r = gq \in (p_1^{e_1})$ live in the intersection. Then, since p_1 doesn't divide g[1], $p_1 \mid q$, so $p_1^{e_1} \mid q$ and thus $r \in (f)$.

b) If $f = u\prod_i p_i$ is the prime factorization of f then, by part a), the associated primes of $R/(f)$ are (p_i). So every prime minimal over ann$(R/(f)) = (f)$ is principal. Conversely, suppose prime ideals minimal over principal ideas are principal. Then if all irreducibles are prime, factorizations are unique. If P is minimal over (f), then $P = (p)$ and $f = pu$. Since f is irreducible, u is a unit and $(f) = (p)$, meaning f is prime.

□

[1] We use the fact that the primes generate different ideals.

Now some geometric intuition behind the primary decomposition. In the following examples, we take k to be algebraically closed.

Example 9.2. Let $I = (x^2, y) \subseteq k[x, y]$. Then $V(I) = \{(x, y)\}$ – at the level of sets, it's just a point. Any $f = a_0 + a_1x + a_2y + a_3x^2 + \dots$ has residue $a_0 + a_1x$ mod I. So modding preserves $a_0 = f(0, 0)$ and $a_1 = \frac{\partial f}{\partial x}(0, 0)$.

If $J = (x^2, xy, y^2)$, we get the same $V(J)$, since $J \subseteq \sqrt{I}$ and $V(I) = V(\sqrt{I})$. But this time the residue of a polynomial f in $k[x, y]/J$ gives us the value of f at 0 and its derivatives in any direction. So $V(J)$ can be thought of as the whole first order infinitesimal neighborhood of the origin.

If $K = (x^2)$, then the residue of f in R/K gives us the value of f at every point on the line $x = 0$, along with values of the derivative in the horizontal direction.

If $L = (x^2, xy) = (x) \cap (x^2, xy, y^2)$, $V(L)$ corresponds to the union of the vertical line and the first order infinitesimal neighborhood at the origin. Since we have the vertical line, the only additional information from the neighborhood is that of the horizontal direction.

We'd like to generalize some results from linear algebra to modules. The first result we'll look at is Cayley-Hamilton.

Theorem 9.3 (Cayley-Hamilton (classic))**.** *A matrix A on a finite-dimensional vector space satisfies its characteristic polynomial $p(x) = \det(x\mathbf{1} - A)$.*

The more general result is the following:

Theorem 9.4 (Cayley-Hamilton (general))**.** *Let R be a ring, I an ideal, and M an R-module generated by n elements. Let $\phi : M \to M$ be a map with $\phi(M) \subseteq IM$. Then there exists a monic polynomial $p(x) = x^n + p_1x^{n-1} + \dots + p_n$ with $p_j \in I^j$ and $p \circ \phi = 0$ as an endomorphism on M.*

Proof. Let $m_1, \dots, m_n$ be generators for M. Then $\phi(m_i) = \sum a_{ij}m_j$ for $a_{ij} \in I$. Let $A = (a_{ij})$. Then we can treat M as an $R[x]$-module by setting $xa = \phi(a)$. Set $m = (m_1 \ \dots \ m_n)$. Then $(x\mathbf{1})m = Am$ and $(x\mathbf{1} - A)m = 0$. Recall that if B is a matrix of cofactors of $(x\mathbf{1} - A)$, then $B(x\mathbf{1} - A) = \det(x\mathbf{1} - A)\mathbf{1}$.

So $\det(x\mathbf{1} - A)\mathbf{1}m = 0$ and $\det(x\mathbf{1} - A)m_i = 0$ for all i. Then $\det(x\mathbf{1} - A)$ annihilates M, and $p(\phi) = 0$. Since the a_{ij} are in I, it's straightforward that the coefficients are in the correct powers of I. □

Definition 9.5. For R a ring, an R-module F is *free* with *free basis* $B \subseteq F$ if every element of F is uniquely an R-linear combination of elements of B. Equivalently, $F \cong \oplus_{b \in B} Rb \cong R^{|B|}$.

Corollary 9.6. *For R a ring and M a finitely generated R-module,*

a) If $\alpha : M \to M$ is surjective, it's an isomorphism.

b) If $M \cong R^n$, then any set of n elements generating M is a free basis. So the rank of M is well-defined.

10. Lecture 10 — October 7, 2019

We've been talking about primary decomposition and associated primes for a while - now we're going to shfit directions a bit. Last time we saw generalized Cayley-Hamilton for modules and talked about free modules. We states the following corollary, which we'll now prove.

Corollary 10.1. *For R a ring and M a finitely generated R-module,*

a) If $\alpha : M \to M$ is surjective, it's an isomorphism.
b) If $M \cong R^n$, then any set of n elements generating M is a free basis. So the rank of M is well-defined.

Proof. a) Let M be an $R[t]$-module where $tm := \alpha(m)$. If $I = (t)$, then α is surjective and $IM = M$. Applying Cayley-Hamilton with the identity, we see that there's a polynomial $p(x) = x^n + p_1 x^{n-1} + \cdots + p_n$ such that $p(\mathrm{id})M = 0$ and $p_i \in (t)^i$. So $p_i = a_i t^i$ for some $a_i \in R$, and

$$\begin{aligned}(1 + a_1 t + \cdots + a_n t^n)M &= 0\\ (1 + t(a_1 + a_2 t + \dots))M &= 0\\ (1 + q(t)t)M &= 0\\ (-q(\alpha))\alpha &= \mathrm{id}\end{aligned}$$

So $-q(\alpha)$ is an inverse to α and α is an isomorphism.

b) Choose generators $m_1, \dots, m_n$ for M. Define $\beta : R^n \to M$ by sending each basis element to an m_i. Choose an isomorphism $\gamma : M \to R^n$. Then $\beta\gamma : M \to M$ is surjective, so by (a) it's an isomorphism. Then $(\beta\gamma)\gamma^{-1} = \beta$ is an isomorphism, so the m_i are linearly independent and thus form a basis.

□

If $p \in R[x]$, we can think of $R[x]/(p)$ as isomorphic to $R[a]$ with $x \mapsto a$. We've sort of forced a to be a root of p in R. For instance, when we localize at $\{1, a, a^2, \dots\}$, this is the same as taking $R[x]/(ax - 1)$, because demanding that $ax = 1$ have a root amounts to giving a an inverse.

Proposition 10.2. *Let R be a ring and $J \subseteq R[x]$ an ideal. Let $S = R[x]/J$ and $s = x \in S$.*

a) S is generated by at most n elements as an R-module if and only if it contains a monic polynomial of degree at most n, in which case it is generated by $\{1, s, \dots, s^{n-1}\}$.
b) S is a finitely generated free module if and only if J is generated by a monic polynomial. And $\{1, s, \dots, s^{n-1}\}$ is a free basis.

Proof. Omitted. □

Definition 10.3. An *R-algebra S* is a ring along with a map $\phi : R \to S$.

The additional structure on S is that it admits scaling by R through ϕ. So in this way S is also naturally an R-module, and we can write rs to mean $\phi(r)s$. Often times we'll care about the case in which ϕ is an injection, so R naturally sits in S, or in which ϕ is a quotient map, so $S = R/I$.

Definition 10.4. S is *finitely generated* as an R-algebra if there exist $v_1, \dots, v_n \in S$ such that S is the ring generated by $\phi(R)$ and $v_1, \dots, v_n$.

Definition 10.5. $s \in S$ is *integral* over R if it's the zero of some monic polynomial in $R[x]$. If every element of S is integral over R, then we say S is integral over R.

Definition 10.6. The set of elements in S integral over R is called the *integral closure* of R in S.

If R is an integral domain, its integral closure (or normalization) is its integral closure inside of its field of fractions. Note that being finitely generated as an R-algebra is much weaker than being finitely generated as an R-module. We'll say that an R-algebra S is *finite over* R if it's finitely generated as an R-module.

Example 10.7.

1) $R[x]$ is a finitely generated R-algebra, but it's not finite or integral over R.
2) $R[x]/(x^2)$ is finite and integral over R.
3) $\mathbb{Q}[\sqrt{2}, \sqrt[3]{2}, \sqrt[4]{2}, \dots]$ is integral over $\mathbb{Q}$ but not finite over $\mathbb{Q}$.

Proposition 10.8. *An R-algebra S is finite over R if and only if S is generated as an R-algebra by finitely many integral elements.*

Proof. Suppose S is finite over R. Then for $s \in S$, multiplication by s is a map $S \to S$, and Cayley-Hamilton shows that s satisfies a monic polynomial. Conversely, if S is generated as an R-algebra by t elements, let $S' \subseteq S$ by the algebra generated by $t-1$ of them. By induction, we have that S' is finite over R. Say it's generated by some $\{s_i\}$. The remaining (algebra) generator of S, say s, is integral over R by assumption and thus integral over S'. So there's a surjection $S'[x]/(p) \to S \cong S'[x]/I$ with $x \mapsto x$ where p is monic and $p(s) = 0$. Since $p \in I$, there's a finite set of generators for S as an S' module, say $\{t_i\}$. Thus S is generated by $\{s_i t_j\}$ as an R-module. □

Proposition 10.9. *If S is an R-algebra and $s \in S$ then s is integral over R if and only if there exists an S-module N and a finitely generated R-module $M \subseteq N$ not annihilated by any nonzero element of S such that $sM \subseteq M$.*

We'll prove the proposition next time, but for now we'll examine a nice corollary assuming the proposition.

Corollary 10.10. *S is integral if and only if $R[S]$ is a finitely generated R-module.*

Proof. If S is integral, then $R[S]$ is finite over R. Set $N = R[S], M = R[S]$. If $I \in R[S]$ is not annihilated by any element of $R[S]$ then s is integral over R. □

11. Lecture 11 — October 9, 2019

Last time we stopped at the follow proposition:

Proposition 11.1. *If S is an R-algebra and $s \in S$ then s is integral over R if and only if there exists an S-module N and a finitely generated R-module $M \subseteq N$ not annihilated by any nonzero element of S such that $sM \subseteq M$.*

Proof. First assume that s is integral over R. Then let $N = S$ and $M = R[s] \subseteq S$. Then $M \cong R[x]/I$, since there's a surjection from $R[x]$ to M. I contains some monic polynomial satisfied by s, so M is finite over R.

For the converse, let $\phi : M \to M$ be multiplication by s. Applying Cayley-Hamilton with $I = R$, we have a monic polynomial $p(x)$ with coefficients in R such that $p(s)M = 0$. Then $p(s) = 0$ and s is integral over R. □

Theorem 11.2. *Let S be an R-algebra. Then the set of elements of S integral over R forms a subalgebra of S.*

Proof. We need to show closure under addition and multiplication. $R[a, b]$ is finite over R. If $s = ab$ or $a + b$, set $N = S$ and $M = R[a, b]$. M isn't annihilated by any element of S with $sM \subseteq M$ so s is integral over R. □

Corollary 11.3. *Let M be a finitely generated R-module and I an ideal of R such that $IM = M$. Then there exists an $r \in I$ acting as the identity on M, i.e. $(1 - r)M = 0$.*

Proof. Let $\phi = \mathrm{id}$. There exist $p_1, \ldots, p_n$ such that $p_j \in I^j \subseteq I$ such that $(1 + p_1 + \cdots + p_n)M = 0$. Set $R = p_1 + \cdots + p_n$. □

Definition 11.4. The *Jacobson radical* of a ring R is the intersection of all the maximal ideals in R.

So the Jacobson radical contains the nilradical, but in general they're not the same.

Lemma 11.5 (Nakayama's Lemma)**.** *Let I be an ideal contained in the Jacobson radical of R. Let M be a finitely generated R-module.*

a) If $IM = M$, then $M = 0$.
b) If $m_1, \ldots, m_n \in M$ have images in M/IM that generate it as an R-module then $m_1, \ldots, m_n$ are generators for M as an R-module.

Proof. a) By the previous corollary, we have that there exists an $r \in I$ such that $(1 - r)M = 0$. But r is in every maximal ideal, so $1 - r$ is in no maximal ideal. Then $1 - r$ is a unit, and $(1 - r)M = 0$ means $M = 0$.

b) Let $N = M/(\sum Rm_i)$. Then $N/IN = M/(IN + \sum RM_i) = 0$. $M = IN$ so $N = 0$ and $M = \sum Rm_i$.

□

Corollary 11.6. *If M and N are finitely generated R-modules and $M \otimes_R N = 0$ then $annM + annN = R$. If R is local, M or N is zero.*

Proof. First assume R is local and $M \neq 0$. If P is the maximal ideal, it equals the Jacobson radical and Nakayama gives us $M/PM \neq 0$, because $PM \neq M$. This is an R/P-vector space, so there's a surjection $M/PM \to R/P$. So $M \otimes N = 0$ and it surjects on to $R/P \otimes_R N \cong N/PN$. Then $N = PN$ and $N = 0$.

If R isn't local, suppose $\text{ann}M + \text{ann}N \neq R$. Find some prime P containing $\text{ann}M$ and $\text{ann}N$. Then $M_p \otimes_{R_p} N_p = 0$, and without loss of generality we may assume $M_p = 0$. Then there exists an element not in P which annihilates each generator of M. The product annihilates M, producing contradiction. □

Now recall that an integral domain is *normal* if it's integrally closed in its field of fractions. Interestingly, integrality and normality are connected to unique factorization. In particular, unique factorization implies normality.

Proposition 11.7. *R is a UFD implies R is normal.*

Proof. Consider $\frac{r}{s}$ in the field of fractions of R. We may assume they're relatively prime. Suppose

$$p(\frac{r}{s}) = (\frac{r}{s})^n + a_1(\frac{r}{s})^{n-1} + \cdots + a_n = 0$$

Then $r^n = s(-a_1 r^{n-1} - \cdots - a_n s^{n-1})$ so $s \mid r^n$. Then s is a unit in R and $\frac{r}{s} \in R$. □

A corollary to this is that the only rational solutions to monic polynomials over $\mathbb{Z}$ are in $\mathbb{Z}$.

Proposition 11.8. *If f factors in $S[x]$ as $f = gh$ for g and h monic, then the coefficients of g and h are integral over R.*

Proof. Let $R[x]/(g) = R[\alpha_1]$ via $x \mapsto \alpha_1$ for α_1 a root of g. Using long division, we have that $g = (x - \alpha_1)g_1$ over $R[\alpha_1]$. Repeating with g_1, we get a ring $T \supseteq S$ and elements α_i, β_j of T such that $g = \prod(x - \alpha_i)$ and $h = (x - \beta_j)$ in $T[x]$. So the α_i and β_j are integral over R, and their coefficients are also integral over R. □

Corollary 11.9. *If R is normal, then any monic irreducible polynomial is prime.*

Proof. Let Q be the field of fractions. If $f = gh$ in $Q[x]$ then $g, h \in R[x]$ and f is irreducible in $Q[x]$. Since Q is a field, $Q[x]$ is a UFD, so its irreducibles are prime and $(f) \subseteq Q[x]$ is prime. Then $R[x]/(f)$ is free over R and we have a map $R[x]/(f) \to Q \otimes R[x]/(f) = Q[x]/(f)$ via $g \mapsto 1 \otimes g$. This is the direct sum of maps $R \to Q \otimes_R R = Q$, since $Q \otimes_R R^{\oplus n} \cong \bigoplus(Q \otimes R)$. Then the map injects and $R[x]/(f)$ is an integral domain, meaning (f) is prime. □

12. Lecture 13 — October 21, 2019

Today we're going to prove the big theorem - Nullstellensatz. Recall that we've talked about Jacobson rings, which are rings in which all prime ideals are intersections of maximal ideals. It might be hard to see why that's a useful property, but today we'll connect it to localizations.

Lemma 12.1. *The following are equivalent:*

a) R is Jacobson
b) If $P \subseteq R$ is prime and $S = R/P$ contains $b \neq 0$ such that $S[b^{-1}]$ is a field, then S is a field.

Proof. If R is Jacobson, then S is Jacobson (lift, intersect, then project). S is an integral domain so (0) is prime. Then the Jacobson radical in S (intersection of all maximal ideals) is 0. Since $S[b^{-1}]$ is a field, only (0) is prime. So the only prime ideal in S avoiding the multiplicative set generated by b is (0). So any other prime ideal in S contains b. So 0 must be maximal in S, and S is a field.

In the other direction, let $Q \subseteq R$ be prime, and let I be the intersection of all maximal ideals containing Q. We'd like to show $I = Q$. Suppose not, so there exists $f \in I \setminus Q$. Now we select a prime P maximal among primes containing Q but not f (Zorn's). P isn't maximal in R, so R/P isn't a field. But by construction, $PR[f^{-1}]$ is maximal in $R[f^{-1}]$, and $R[f^{-1}]/PR[f^{-1}] = (R/P)[f^{-1}]$. So R/P is a field, producing contradiction. Then $I = Q$ and R is Jacobson. □

Now back to Nullstellensatz!

Theorem 12.2 (Nullstellensatz)**.** *Let R be a Jacobson ring.*

a) If S is a finitely generated R-algebra, then S is Jacobson.
b) If $N \subseteq S$ is maximal, then $M = N \cap R$ is maximal in R, and S/N is a finite extension of R/M.

Proof. The proof isn't so complicated, but it's pretty long. We first suppose that R is a field and $S = R[x]$. Then S is a PID (nonzero primes are maximal), so we just need to show that (0) is the intersection of prime ideals. Since no polynomial can have infinitely many irreducible factors, we just need to show that S has infinitely many prime ideals. If there are only finitely many irreducible polynomials $f_1, \dots, f_n$ then $\prod f_i + 1$ has positive degree (so it's not a unit) and it has no prime factors, giving us a new prime. So S has infinitely many nonzero prime ideals (which are maximal) so (0) is the Jacobson radical.

Now to part (b), again restricting to $S = R[x]$. If $N \subseteq S$ is maximal then $N = (f)$ for some irreducible, monic polynomial. Then $R \cap N = (0)$. The only maximal ideal of $S/(f)$ has dimension $\deg(f)$ over R so it's finite over R.

Now let R be a Jacobson ring and suppose S is generated (as an R-algebra) by a single element. We'll prove in this case and then induct over the size of the generating set. For (a), we want to show that if $P \subseteq S$ is prime and $S' = S/P$ contains $b \neq 0$ with $S'[b^{-1}]$ a field, then S' is a field. By the previous lemma, this will suffice to show that S is Jacobson. We now set $R' = R/R \cap P$. This injects into S'. Replace S by S' and R by R', an integral domain contained in S. We'd like to show that if $S[b^{-1}]$ is a field then so is S. In fact, we'll show that R is a field in this case too, and S is a finite extension of R.

For the second statement, we make the same reduction and assume S is a field. We then want that R is a field over which S is finite. So the same proof applies in both cases. S is generated by a single element T over R, and we write $S = R[x]/Q$ for some prime Q such that t is the image of x in S. We first claim $Q \neq 0$. Otherwise, there exists $b \in R[x]$ such that $R[x][b^{-1}]$ is a field, by hypothesis. If K is the field of fractions of R, then $(K[x])[b^{-1}]$ is also a field, meaning $K[x]$ must be a field. But it's not, producing contradiction.

So Q from earlier is not zero. $S[b^{-1}] = (R[x]/Q)[b^{-1}]$ is a field, so $S[b^{-1} = (K[x]/QK[x])[b^{-1}]$, but $K[x]/(QK[x])$ is already a field (since $K[x]$ is a PID), so $S[b^{-1}] = K[x]/(QK[x])$. And it's finite dimensional over K because Q has finite degree. Now take some $0 \neq p(x) \in Q$.

Since $S = R[x]/Q$, we have $p(t) = p_n t^n + \cdots + p_0 = 0$ in S. Inverting p_n, we get that $S[p_n^{-1}]$ is integral over $R[p_n^{-1}]$. b also satisfies an equation with coefficients in R: $q(b) = q_m b^m + \cdots + q_0 = 0$. We can assume $q_0 \neq 0$. Then $(\frac{1}{b})^m + (\frac{q_1}{q_0})(\frac{1}{b})^{m-1} + \cdots + (\frac{q_m}{q_0}) = 0$ by dividing by $q_0 b^m$.

Thus $S[b^{-1}]$ is integral over $R[(p_n q_0)^{-1}]$. Since $S[b^{-1}]$ is an integral domain, $R[(p_n q_0)^{-1}]$ is a field. Since R is Jacobson, it's is a field (by the lemma). So $S[b^{-1}]$ is integral over R, meaning S is, and thus S is a field (by corollary from a previous section). And S is finite over R since it's integral and generated by a single element as an R-algebra.

Finally, we induct on the number of generators of S as an R-algebra, r. We can assume $r > 1$ and that the statement holds for algebras generated by fewer than r elements. Let $S' \subseteq S$ be the algebra generated by $r-1$ of the generators. By induction, S' is Jacobson. S is generated by one element as an S' algebra, so S is Jacobson. If $N \subseteq S$ is a maximal ideal, then $N \cap S'$ is maximal, so $N \cap S' \cap R = N \cap R$ is by induction.

$R/(R \cap N) \subseteq S'/(S' \cap N)$ and $S'/(S' \cap N) \subseteq S/N$ are finite. So $R/(R \cap N) \subseteq S/N$ is finite by transitivity. □

13. Lecture 14 — October 23, 2019

Today we'll finish up Nullstellensatz by considering its geometric applications. In order to do that, we'll need to discuss some classical algebraic geometry.

Let k be a field.

Definition 13.1. If $\{f_i\} \subseteq k[x_1, \ldots, x_n]$, then $Z(\{f_i\}) = \{a = (a_1, \ldots, a_n) | f_i(a) = 0 \ \forall i\}$. This is called an *algebraic set* in k^n (written $\mathbb{A}^n$).

Definition 13.2. Let $X \subseteq k^n = \mathbb{A}^n$. Then $I(X) = \{f \in k[x_1, \ldots, x_n] | f(p) = 0 \ \forall x \in X\}$.

Some things to check:

- $Z(\{f_i\}) = Z(I) = Z(\sqrt{I})$ for $I = (f_i)_i$.
- $I(X)$ is a (radical) ideal, and $Z(I(Z(J))) = Z(J)$ for any ideal $J \subseteq k[x_1, \ldots, x_n]$.

For now we'll write $R = k[x_1, \ldots, x_n]$. Note that if $(a_1, \ldots, a_n) \in \mathbb{A}^n$, then the map $x_i \mapsto x_i - a_i$ is an isomorphism on R. So it induces an isomorphism $R/(x_1, \ldots, x_n) \to R/(x_1 - a_1, \ldots, x_n - a_n)$. The evaluation map $\mathrm{ev}_0 : R \to k$ which sends f to $f(0, \ldots, 0)$ is a surjection with kernel $(x_1, \ldots, x_n)$.

So $(x_1 - a_1, \ldots, x_n - a_n)$ is always a maximal ideal. Then there's a map of sets which injections $\mathbb{A}^n \to \mathrm{Spec}(R)$ with image contained in the set of maximal ideals. By definition, if $X = Z(I) \subseteq \mathbb{A}^n$ then $(a_1, \ldots, a_n) \in X$ if and only if $f(a_1, \ldots, a_n) = 0 \ \forall f \in I$. But this holds if and only if $(x_1 - a_1, \ldots, x_n - a_n) \in V(I)$. So the algebraic sets of $\mathbb{A}^n$ correspond to the closed sets of Spec$R$ intersected with the image of $\mathbb{A}^n$. In this way, $\mathbb{A}^n$ inherits the Zariski topology.

In fact, if $k = \bar{k}$ and $X \subseteq \mathbb{A}^n$ is an algebraic set, we'll see that there's a one-to-one correspondence between points of X and closed points (i.e. maximal ideals) in $\mathrm{Spec}(R/I(x))$. However, if k is not algebraically closed there can be additional maximal ideals in Spec$R$. For instance $R[x]/(x^2+1) \cong \mathbb{C}$ so (x^2+1) is a maximal ideal, but it's not of the previous form $(x - a)$.

Corollary 13.3. *Let $k = \bar{k}$. For each $p = (a_1, \ldots, a_r) \in \mathbb{A}^n$, define $m_p = (x_1 - a_1, \ldots, x_r - a_r) \subseteq k[x_1, \ldots, x_r]$. If X is an algebraic set, then every maximal ideal of $k[x_1, \ldots, x_r]/I(x)$ is of the form $m_p/I(x)$ for some $p \in X$. In particular, the points of X are in 1-to-1 correspondence with the maximal ideals of $k[x_1, \ldots, x_r]/I(x)$.*

Proof. This is a corollary to Nullstellensatz, which says that a finitely generated algebra over a Jacobson ring is Jacobson. Now let $S = k[x_1, \ldots, x_r]$ and suppose $n \subseteq S$ is a maximal ideal. Applying Nullstellensatz with $R = k$, we get that $0 = n \cap R$ and that S/n is finite (and thus algebraic over k). So $S/n = k$.

Now let a_i be the image of x_i under the map $S \to S/n = k$. Let $p = (a_1, \ldots, a_r)$. Then $m_p \subseteq n$. Since m_p is maximal, $m_p = n$. And we're done, since maximal ideals in $S/I(x)$ take the form $m_p/I(x)$. Thus $p \in Z(m_p) \subseteq X$. □

Now we can prove classical Nullstellensatz.

Theorem 13.4 (Nullstellensatz, classical)**.** *$k = \bar{k}$. If $I \subseteq k[x_1, \ldots, x_n]$ is an ideal, then $I(Z(I)) = \text{rad}I$. Thus, the correspondences $I \mapsto Z(I)$ and $X \mapsto I(X)$ induce a bijection between algebraic sets of $\mathbb{A}^n$ and radical ideals of $k[x_1, \ldots, x_n]$.*

Proof. By the previous corollary, the points of $Z(I)$ correspond to maximal ideals of $k[x_1, \ldots, x_n]$ which contains I. Thus $I(Z(I))$ is the intersection of the maximal ideals that contain I. By our Nullstellensatz, $S[k_1, \ldots, x_n]$ is Jacobson, so every prime containing I appears as the intersection of maximal ideals. So $I(Z(I)) = \bigcap \text{primes containing I} = \text{rad}I$.

On the other hand, $Z(I(X)) = X$ follows from the definition of algebraic set, and we just showed that if I is radical then $I(Z(I)) = I$. So I and Z are inverse maps between algebraic sets and radical ideals. □

Something worth pointing out is that in classical algebraic geometry, the only structure on algebraic sets occurs at the level of set theory and topology (via Zariski). Scheme-theoretic work imposes additional structure which further distinguishes things (agh idk if I got this right). Simply put, $Z(I) \cong Z(\text{rad}I)$ but if $I \neq \text{rad}I$ then $V(I) \ncong V(\text{rad}I)$.

A lot of the time, it's really nice to work with finitely-generated graded modules over graded rings. What we'll talk about now will give us a way of moving from local rings to graded rings and similarly of moving from a module over a local ring to a graded module over a graded ring.

Definition 13.5. A *multiplicative filtration* of a ring R is a sequence of ideals $R = I_0 \supseteq I_1 \supseteq \ldots$ such that $I_i I_j \subseteq I_{i+j}$. Usually we'll care about the case in which I is an ideal and $I_i = I^i$, referred to as the *I-adic filtration*.

If M is an R-module, then $M \supseteq IM \supseteq I^2M \supseteq \ldots$ is the I-adic filtration of M.

Definition 13.6. A filtration $M = M_0 \supseteq M_1 \supseteq \ldots$ is an *I-filtration* if $IM_n \subseteq M_{n+1}$. It is *I-stable* if $IM_n = M_{n+1}$ for $n >> 0$.

Definition 13.7. Let $I \subseteq R$ be an ideal. The *associated graded ring* of R with respect to I is $\text{gr}_I R = R/I \oplus I/I^2 \oplus \ldots$. If $\overline{a} \in I^m/I^{m+1}, \overline{b} \in I^n/I^{n+1}$ such that $a \in I^m$ and $b \in I^n$, we define $\overline{a}\overline{b} \in I^{m+n}/I^{m+n+1}$ to be the image of ab. You can check that this is well-defined.

Definition 13.8. If J is an I-filtration of M; $M = M_0 \supseteq M_1 \supseteq \dots$, we define $\mathrm{gr}_J M = M/M_1 \oplus M_1/M_2 \oplus \dots$. This is a $\mathrm{gr}_I R$-module with the following scaling: if $\overline{a} \in I^m/I^{m+1}$ and $\overline{b} \in M_n/M_{n+1}$, then $ab \in I^m M_n \subseteq M_{n+m}$. So we define $\overline{a}\overline{b} \in M_{n+m}/M_{n+m+1}$ to be the image of ab. Again, one can check that this is well-defined.

Proposition 13.9. *Let $I \subseteq R$ be an ideal and M a finitely generated R-module. If J ($M = M_0 \supseteq M_1 \supseteq \dots$) is an I-stable filtration with all the M_i finitely generated, then $gr_J M$ is a finitely generated $gr_I R$-module.*

Proof. Assume $IM_i = M_{i+1}$ for $i \geq n$. Then $(I/I^2)(M_i$ □

14. Lecture 15 — October 28, 2019

Recall that we've been talking about filtrations. In particular, for $I \subseteq R$ an ideal, $\mathrm{gr}_I R = R/I \oplus I/I^2 \oplus \dots$ with a well-define multiplication. And if M is an R-module with $\mathcal{J}$ a filtration $M = M_0 \supset M_1 \supset \dots$, then $\mathcal{J}$ is an I-filtration if $IM \subseteq M_{i+1}$. Finally, $\mathrm{gr}_{\mathcal{J}} M = M_0/M_1 \oplus M_1/M_2 \oplus \dots$ is a graded $\mathrm{gr}_I R$-module.

Definition 14.1. Let $f \in M$. If $\exists m$ such that $f \in M_m$ but $f \notin M_{m+1}$, we define the *initial formula* of f to be $\mathrm{in}(f) = \overline{f} \in M_m/M_{m+1} \subseteq \mathrm{gr}M$. If $f \in \cap M_m$, then $\mathrm{in}(f) = 0$.

The idea is that we're taking the smallest graded piece of what f is.

Example 14.2. Let $J = (xy + y^3, x^2) \subseteq R = k[x, y]$ and $I = (x, y) \subseteq R$. Then we define $\mathrm{in}(J)$ to be the ideal generated by $\mathrm{in}(j)$ for $j \in J$. We have $\mathrm{in}(x^2) = x^2 \in I^2/I^3$ and $\mathrm{in}(xy + x^3) = xy \in I^2/I^3$. Note $x(xy + y^3) - yx^2 - xy^3 \in \mathrm{in}(J)$ and thus $y^2(xy + y^3) - xy^3 = y^5 \in \mathrm{in}(J)$ despite the fact that y^5 is not generated by x^2 and xy.

Let $I \subseteq R$ be a maximal ideal for R Noetherian. Then $\mathrm{gr}_I(R) = R/I \oplus I/I^2 \oplus \dots$ and $I = (f_1, \dots, f_n)$. So for $a \in I/I^2$, $a = r_1 f_1 + \dots + r_n f_n$ where $r_i = 0$ or $r_i \notin I$. If $a \in I^m/I^{m+1}$, then $a = r_1 f_1 + \dots + r_n f_n$ where each $r \in R \setminus I^m$ or $r_i = 0$. So by induction, r_i is a polynomial in the f_i over k, i.,e. $\mathrm{gr}_I(R)$ is a finitely generated k-algebra.

Definition 14.3. IF R is a local ring with maximal ideal I, the *Hilbert function* of R is $H_R(n) = \dim_{R/I} I^n/I^{n+1}$. If M is a finitely generated R-module, define $H_M(n) = (I^n M)/(I^{n+1} M)$.

Since these are the Hilbert functions of $\mathrm{gr}_I R$ and $\mathrm{gr}_I M$, we're guaranteed that for sufficiently large n, they agree with polynomial of degree at most $H_R(1) - 1$.

Now we'll talk about the Blowup algebra. It's possible to understand this kind of stuff purely algebraically, but having an idea of the geometric picture is nice if that's your kind of thing.

Definition 14.4. R a ring, $I \subseteq R$ an ideal. Then the *blowup algebra* of I in R is the R-algebra $B_I R = R \oplus I \oplus I^2 \oplus \dots$.

Often times it's hard to keep track of where even homogeneous elements live (e.g. an element of I^3 also lives in R, I, and I^2). To keep track of the grading, we write elements of $B_I R$ as $f = a_0 + a_1 t + a_2 t^2 + \dots \in R[tI] \cong B_I(R)$. In words, we're just adding t's to keep track of which summand we're in. In this way, $B_I R$ is a subring of $R[t]$.

Remark 14.5. $B_I(R)/IB_IR = R/I \oplus I/I^2 \oplus \ldots \cong \mathrm{gr}_I R$.

Example 14.6. Set $R = k[x_1, x_2]$ and $I = (x_1, x_2)$. There's a natural map $k[x_1, x_2, y_1, y_2] \to k[x_1, x_2, t]$ with $x_i \mapsto x_i$ and $y_i \mapsto x_i t$. The image consists of elements of the form $a_0 + a_1 t + a_2 t^2 + \ldots$ with $a_0 \in R$ and $a_i \in I^i$. So the image is exactly the blowup algebra. The kernel is $(x_1 y_2 - x_2 y_1)$. The corresponding algebraic subset Z is the blowup of $\mathbb{A}^2$ at the origin.

Note that $R \hookrightarrow k[x_1, x_2, y_1, y_2] \to k[x_1, x_2, y_1, y_2]/(x_1 y_2 - x_2 y_1) \cong B_I R$. Thus there is a map $Z \to \mathbb{A}^2$. The y_i in $k[x_1, x_2, y_1, y_2]$ are homogeneous, which means the points correspond to ideals of the form $(x_1 - a_1, x_2 - a_2, b_1 y_1 - b_2 y_2)$, with the b_i not both 0. So for $(a_1, a_2) \in \mathbb{A}^2$ not the origin, the point in Z lying over it corresponds to $(x_1 - a_1, x_2 - a_2, a_2 y_1 - a_1 y_2)$. Over $(0,0)$ we have $(x_1, x_2, b_1 y_1 - b_2 y_2)$ with the b_i not both zero. So the fiber over (0,0) is one-dimensional, as there's one degree of freedom. In fact, it's a projective line $\mathbb{P}^1$. In this case, it's the exceptional set of the blowup, i.e. the pre-image of the origin corresponding to the ring $\overline{B_I R/IB_i R = \mathrm{gr}_I R}$.

If $R = k[x_1, \ldots, x_n]/J$ and $I = (x_1, \ldots, x_n)$ such that $J \subseteq I$, define $X = V(J) \subseteq \mathbb{A}^n$.

Definition 14.7. The *tangent cone* corresponding to $\mathrm{in}_I(J) \subseteq k[x_1, \ldots, x_n]$ is its $\mathrm{Spec}(\mathrm{gr}_I R/\mathrm{in}_I J)$ and $\mathrm{gr}_I R/\mathrm{in} J = \mathrm{gr}_I(R/J)$. We'll show this equality holds on the next homework.

The tangent cone consists of the limits of the secant lines to $V(J)$ through the origin. When blowing up $\mathbb{A}^2$ at the origin, each line in the tangent cone corresponds to a point in the fiber over the origin in the preimage of the curve.

Now back to pure algebra.

Lemma 14.8 (Artin-Rees Lemma)**.** *Let M be an R-module and $\mathcal{J} : M = M_0 \supset M_1 \supset \ldots$ be an I-filtration. Then $B_{\mathcal{J}} M = M \oplus M_1 \oplus M_2 \oplus \ldots$ is a graded $B_I R$-module.*

Proof. Assume each M_i is finitely generated as an R-module. Then $\mathcal{J}$ is I-stable if and only if $B_{\mathcal{J}} M$ is a finitely generated $B_I R$-module. To see why, note that if $B_{\mathcal{J}} M$ is finitely generated, its generators must be contained in the first n terms for some n. Now replace each generator with its homogeneous components. We get that $M_n \oplus M_{n+1} \oplus \ldots$ is generated by M_n so $M_{n+i} = I^I M_N$ for $i \geq 0$ and $\mathcal{J}$ is stable. On the other hand, if $\mathcal{J}$ is stable then $B_{\mathcal{J}} M$ is generated by the union of the generators for $M_0, \ldots, M_n$. □

Lemma 14.9 (Artin-Rees Lemma)**.** *Let R be Noetherian, $I \subseteq R$ an ideal and $M' \subseteq M$ both finitely-generated R-modules. If $\mathcal{J} : M = M_0 \supseteq M_1 \supseteq \ldots$ is I-stable, then so is $\mathcal{J}' : M' \supset M' \cap M_1 \supset M' \cap M_2 \supset \ldots$.*

Proof. Since I is finitely generated, $B_I R$ is a finitely generated R-algebra. Then, by Hilbert basis, it's Noetherian. $B_J M$ is a finitely generated $B_I R$-module, by our last result, so it's Noetherian and $B_{\mathcal{J}'} M' \subseteq B_{\mathcal{J}} M$ is finitely-generated and thus $\mathcal{J}'$ is I-stable. □

15. Lecture 16 — October 30, 2019

Today we'll prove the Krull intersection theorem.

Theorem 15.1 (Krull Intersection). *Let R be Noetherian and $I \subseteq R$ an ideal. If M is a finitely generated R-module, then $\exists\, r \in I$ such that $(1-r)(\cap_{j=1}^{\infty} I^j M) = 0$. If furthermore R is a domain or a local ring and I is a proper ideal, then $\cap I^j = 0$.*

Proof. Set $M' = \cap_{j=1}^{\infty} I^j M \subseteq M$. M' is finitely generated so we apply Artin-Rees and set $M_i = I^i M$. Then $M' \cap M \supset M' \cap IM \supset \dots$ is I-stable, so there's some P such that $M' \cap M_{p+1} = I(M' \cap M_p)$. This implies $M' = IM'$. It'd be nice to apply Nakayama, but we don't know that I is in the Jacobson radical of R. By a corollary of C-H, however, we get that there exists $r \in I$ such that $(1-r)M' = 0$.

For the second statement, take $M = R$. Then $M' = \cap I^j$. If R is a domain, then I being proper means $1 - r \neq 0$. Thus $1 - r$ is a nonzero divisor, implying $M' = 0$. Likewise, if R is local then $1 - r$ is a unit so $M' = 0$. □

Remark 15.2. The condition that R be a domain is necessary. To see why, take $R = k[x]/(x^2 - x)$ and $I = (x)$. Then $I^2 = (x^2) = (x)$ and thus $x \in \cap I^j$.

Corollary 15.3. *Let R be a Noetherian local ring and $I \subseteq R$ proper. If $gr_I R$ is a domain, then so is R.*

Proof. Say $f, g \in R$ and $fg = 0$. Then $\text{in}(f)\text{in}(g) = 0$, by this week's homework. So $\text{in}(f) = 0$ or $\text{in}(g) = 0$. By Krull, $\cap I^i = 0$ and thus f or g equal 0. □

Recall that if M is an R-module and $N \to N' \to N'' \to 0$ is exact, then $N \otimes M \to N' \otimes M \to N'' \otimes M \to 0$ is exact (i.e. tensoring is right-exact).

Definition 15.4. An R-module M is *flat* if $\forall N \subseteq N'$, the induced map $M \otimes_R N \to M \otimes_R N'$ is injective.

We've shown previously that $R[U^{-1}]$ is a flat R-module. We also know that free modules are flat. Now we'll talk about Tor, but in order to do that we first need to discuss free resolutions.

Definition 15.5. Let M be an R-module. A *free resolution* of M is a sequence

$$\dots \to F_1 \to F_0 \to M \to 0$$

such that each F_i is free and the sequence is exact.

It turns out that we can always construct a free resolution on M by being greedy. In particular, fix M a module and $\{m_i\}_{i \in J}$ a generating set for M. Then set $F_0 = \oplus_{i \in J} R$ and let e_i be the ith basis vector in F_0. We then have a map $F_0 \to M$ sending e_i to m_i. It surjects, giving us the first piece of our resolution.

We need the image of our next map to equal the kernel of this one, so we repeat the process. Take $M_0 = \ker(F_0 \to M)$ and repeat, arriving at $F_1 \to F_0 \to M \to 0$ exact. In this way we arrive at a free resolution of M.

Example 15.6. Let $M = k[x,y]/(x,y) \cong k$, thought of as a module over $R = k[x,y]$. This is generated by 1, giving us a surjection

$$R \to M \to 0$$

which sends $1 \in R$ to $\overline{1} \in M$. This has kernel (x,y). Then we can append to this diagram with a map $R^2 \to R$ by $(a,b) \mapsto ax + by$. This has kernel $(-y,x)$. We complete the resolution with an injection $R \to R^2$ defined by $f \mapsto (-fy, fx)$.

It's important to keep in mind that free resolutions are not unique.

Definition 15.7. Let M and N be R-modules and $\cdots \to F_1 \to F_0 \to M \to 0$ a free resolution. Then $\mathrm{Tor}_i^R(M,N)$ is the homology at $F_i \otimes N$ of the complex $\cdots \to F_1 \otimes N \to F_0 \otimes N \to 0$.

Facts about Tor:

1.) It's well-defined (with respect to choice of free resolution)
2.) It's symmetric. We could instead find a free resolution of N and tensor by M, and we'd get the same modules.
3.) $\mathrm{Tor}_0^R(M,N) = \mathrm{coker}(F_1 \otimes N \to F_0 \otimes N)$. Since tensoring is right-exact and the original $F_1 \to F_0 \to M \to 0$ were exact, that comes out to $M \otimes N$.

It turns out that Tor is the left derived functor tensor, which is how we'll be thinking about Tor.

16. Lecture 17 — November 4, 2019

Recall that for M, N two R-modules, $\cdots \to F_1 \to F_0 \to M \to 0$ is a free resolution of M and $\mathrm{Tor}_i^R(M,N) = H_i(F_\bullet \otimes N)$. Last time we mentioned the following facts:

1.) $\mathrm{Tor}_i(M,N)$ does not depend on choice of resolution.
2.) $\mathrm{Tor}_i)(M,N) = \mathrm{Tor}_i(N,M)$
3.) $\mathrm{Tor}_0(M,N) = \mathrm{coker}(F_1 \otimes N \to F_0 \otimes N) = M \otimes N$, since tensoring is right-exact and the original sequence was exact.
4.) If M is free, it has free resolution $0 \to M \to M \to 0$ so $\mathrm{Tor}_i(M,N) = 0$ for $i > 0$.
5.) Like tensoring, Tor is R-bilinear. So multiplication on M or N by $r \in R$ induces multiplication on $\mathrm{Tor}_i^R(M,N)$ by r.
6.) If R is Noetherian and M, N are finitely-generated, then $\mathrm{Tor}_i^R(M,N)$ is finitely-generated.
7.) If S is a flat R-algebra, then $S \otimes \mathrm{Tor}_i(M,N) = \mathrm{Tor}_i(S \otimes N, S \otimes N)$. This may be on the next homework.
8.) Tor solves the problem of tensoring not being exact (and only being right exact). Tor is the left derived functor of the tensor product. That is, if $0 \to M' \to M \to M'' \to 0$ is exact, then

$$\begin{aligned} \cdots \to \mathrm{Tor}_2(M'',N) \to \\ \mathrm{Tor}_1(M',N) \to \mathrm{Tor}_1(M,n) \to \mathrm{Tor}_1(M'',N) \to \\ M' \otimes N \to M \otimes N \to M'' \otimes N \to 0 \end{aligned}$$

is exact.

Example 16.1. Set $R = k[x]$ and $M = k[x]/(x)$. We have a free resolution

$$0 \to R \xrightarrow{\cdot x} R \to R/(x) \to 0$$

If N is any R-module, then we have that $\mathrm{Tor}_i(M,N) = H_i(0 \to N \xrightarrow{\cdot x} N \to 0)$ so $\mathrm{Tor}_0(M,N) = N/xN \cong R/(x) \otimes N$. $\mathrm{Tor}_1(M,N) = \{n \in N | xn = 0\}$, and the higher Tor are all zero.

In fact this holds more generally for any R and $x \in R$ a nonzero divisor (we need that x not be a zero divisor in order for the free resolution to be exact).

There's an immediate connection: if $\mathrm{Tor}_1^R(M,N) = 0$ for all N, then M is flat so tensoring by M is exact and it turns out that $\mathrm{Tor}_i^R(M,N) = 0$ for all $i > 0$ and all N. This will be on the next homework, but it's fairly straightforward: it comes down mostly to the fact that it's left derived to tensoring and that it comes from free resolutions.

Proposition 16.2. *Let R be a ring and M an R-module.*

a) If $I \subseteq R$ is an ideal, then $I \otimes_R M \to M$ is an injection if and only if $\mathrm{Tor}_1(R/I, M) = 0$.
b) M is flat if and only if (a) is satisfied for all ideals $I \subseteq R$.

Proof. For (a), consider the SES $0 \to I \to R \to R/I \to 0$. There's a LES

$$\cdots \to \mathrm{Tor}_1(R,M) \to \mathrm{Tor}_1(R/I,M) \to I \otimes N \to R \otimes M \to \dots$$

Note that $R \otimes M \cong M$ and $\mathrm{Tor}_1(R,M) = 0$ since R is free. Then, by exactness, $\mathrm{Tor}_1(R/I,M)$ is 0 if and only if the map $I \otimes M \to R \otimes M$ is an injection.

For (b), if M is flat then condition (a) is satisfied by definition. Assume now that it's satisfied for all ideals $I \subseteq R$ and let $N' \subseteq N$ be R-modules. Consider $N' \otimes M \to N \otimes M$. The condition of being an injection only involves finitely many elements of N, so replace N with the submodule generated by those elements. Then we may assume N is finitely generated, so N/N' is finitely generated. Let $N' = N_0 \subseteq N_1 \subseteq \cdots \subseteq N_p = N$ where N_{i+1}/N_i is simple. If $N_i \otimes M \to N_{i+1} \otimes M$ is injective for all i, then we're done. So assume N/N' is generated by one element. Then $R \twoheadrightarrow N/N'$ so $N/N/ \cong R/I$ for some ideal $I \subseteq R$. Then

$$\cdots \to \mathrm{Tor}_1(N/N', M) \to N' \otimes M \to N \otimes M \to \dots$$

is exact. The Tor is 0 by assumption, so $N' \otimes M \to N \otimes M$ is an injection and M is flat. □

Definition 16.3. An R-module M is *torsion-free* if for $r \in R$ a nonzero divisor in R and $m \in M$ nonzero, then $rm \neq 0$.

Corollary 16.4. *a.) If M is a flat R-module, it's torsion-free.*
b.) If R is a PID, then M is flat if and only if M is torsion-free.

Proof. For (a), let $a \in R$ be a nonzero divisor in R. Define $R \to R$ by $r \mapsto ar$. This is an injection, so since M is flat, $R \otimes M \xrightarrow{\cdot a} R \otimes M$ is an injection. This is just $M \xrightarrow{\cdot a} M$, so a is a nonzero divisor on M and M is torsion-free.

For (b), we see that the forward direction follows from (a). For the backward direction, assume M is torsion-free and $I \subseteq R$ is an ideal. Then $I = (a)$ for a a nonzero divisor in R.

We'd like to show that $\mathrm{Tor}_1^R(R/(a), M) = 0$. If $a = 0$, we're done since R is flat. If $a \neq 0$, then by a previous example $\mathrm{Tor}_1(R/(a), M) = \{m \in M | am = 0\} = 0$. □

Example 16.5. For $k = \bar{k}$, set $R = k[t]$ and $S = R[x]/(t(x-1))$. S has torsion, e.g. $t(x-1) = 0$, so S is not flat over R.

It turns out that flatness is a local property. Geometrically, this means it can be checked in neighborhoods around points, and algebraically this means that we can check the property at localizations at prime ideals.

Proposition 16.6. *M is flat over R if and only if M_P is flat over R_P for all primes (or maximal ideals) P*

Proof. If M is flat, then a SES of R_P modules $0 \to N' \to N \to N'' \to 0$ maps to the SES $0 \to M \otimes_R N' \to M \otimes_R N \to M \otimes_R N'' \to 0$. But $M \otimes_R N \cong M_P \otimes_{R_P} N$ as R_P-modules, via $m \otimes n/u \mapsto m/1 \otimes n/u$. So M_P is flat.

Now assume M is not flat. Then there exists some SES of R-modules $0 \to N' \to N \to N'' \to 0$ that's not exact when tensoring by M. Then $0 \to K \to M \otimes_R N' \to M \otimes_R N \to M \otimes_R N'' \to 0$ is exact, for K the kernel of the following map. Since $K \neq 0$, there exists a prime P such that $K_P \neq 0$. Thus localizing at P is exact and M_P isn't flat. □

Example 16.7. Set $M = k[x,t]/(t(x-1))$ and $R = k[t]$. The 'problem point' was (t). In fact, $M_{(t)} = k[x,t]_{(t)}/(t(x-1))_(t)$, which has torsion, so M is not flat at (t). At any other point, $M_{(t-a)} = k[x,t]_{(t-a)}/(x-1)$, since t is a unit in $M_{(t-a)}$. This is just $k[t]_{(t-a)}$, which is a free $R_{(t-a)}$-module and thus flat.

17. Lecture 18 — November 6, 2019

Now we'll start talking about completions - Eisenbud's chapter on completions is awfully long, and it's probably not as important as what will come afterwards (like dimension theory), so we'll devote two lectures to it. Today will be about construction and basic properties, and tomorrow we'll get into more sophisticated results, some of which we won't prove.

Here's the basic idea: if R is a ring and $M \subseteq R$ an ideal, the localization R_M tells us about Zariski open neighborhoods of M. The completion $\hat{R}_M$ tells us about 'analytic' open neighborhoods around M. Roughly speaking, the localization was not sufficiently expressive for tasks in differential topology and related areas.

Example 17.1. Set $R = k[x,y]/(y^2 - x - 1)$ for $k = \mathbb{C}$. $k[x] \hookrightarrow R$ induces a map which projects the graph of $y^2 - x - 1$ on the x axis via π. In standard topology, π has nonzero derivative at $(0,-1)$, so the inverse function theorem assures us of a neighborhood U of 0 such that there exists an analytic inverse $U \to V$, via $x \mapsto (x, -\sqrt{x+1})$. The problem is that our inverse map isn't algebraic - it's not a polynomial - so we don't have an algebraic inverse to π. However, $\sqrt{x+1}$ can be approximated using a power series expansion: $-\sqrt{x+1} = -1 - \frac{x}{2} + \frac{x^2}{3} - \dots$, which converges for $|x| < 1$.

Before we formally define completions, we'll first need to define inverse limits, which arise pretty frequently in math.

Definition 17.2. Let $\{A_i\}_{i \in J}$ be a collection of groups with J partially ordered such that if $i \leq j$ then $\exists \phi_{ij} : A_j \to A_i$ satisfying

1) $\phi_{ii} = \text{id}$
2) $\phi_{ik} = \phi_{ij} \circ \phi_{jk} \forall i \leq j \leq k$

These form an *inverse system*. The *inverse limit* of the inverse system is

$$\lim_{\leftarrow} A_i = \{\overline{a} \in \prod A_i | a_i = \phi_{ij}(a_j) \forall i \leq j\}$$

Now we're ready to define completions as inverse limits.

Definition 17.3. Let R be a ring and $M \subseteq R$ an ideal. Then $\{R/M^i\}$ is an inverse system with $\phi_{ij} : R/M^j \to R/M^i$ the natural quotient. This setup would make sense for any filtration of ideals. We define the *completion* with respect to M to be

$$\hat{R}_M = \lim_{\leftarrow} R/M^i = \{g = (g_1, g_2, \dots) \in \prod R/M^i | g_j = g_i \in R/M^i \text{ for } j > i\}$$

$\hat{R}_M$ is a ring equipped with coordinate-wise addition and multiplication. For each i, define $\hat{M}^i = \{g = (g_1, \dots,) \in \prod R/M^i | g_j = 0 \text{ for } j \leq i\}$. Each g_j is equivalent mod M^i, so $\hat{R}/\hat{M}^i \cong R/M^i$. And if $M \subseteq R$ is maximal, then $\hat{R}/\hat{M} = R/M$ so $\hat{m} \subseteq \hat{R}$ is maximal. If $g = (g_1, g_2, \dots) \in \hat{R}_M$ but not in $\hat{m}_j$, then $g_1 = 0$.

So each $g_i \notin M/M^i \subseteq R/M^i$ and each g_i is a unit. Since $g_j \equiv g_i \bmod M^i$, then $g_j^{-1} \equiv g_i^{-1} \bmod M^i$. So $h = (g_1^{-1}, g_2^{-1}, \dots) \in \hat{R}$ and it's the inverse of g, meaning g is a unit. We conclude that $\hat{R}$ is local if M is maximal in R.

Example 17.4. Set $R = S[x_1, \dots, x_n]$ and $M = (x_1, \dots, x_n)$. We want to show that $\hat{R} \cong S[[x_1, \dots, x_n]]$. Note $S[[x_1, \dots, x_n]]/M^i \cong R/M^i$, so we have a natural map

$$S[[x_1, \dots, x_n]] \to \hat{R}$$
$$f \mapsto (f + M, f + M^2, \dots)$$

In the other direction, if $(f_1 + M, f_2 + M^2, \dots,) \in \hat{R}$, then for $i > j$, $f_i = f_j +$ terms of degree $> j$. So we have a map $(f_1 + M, f_2 + M^2, \dots) \mapsto f_1 + (f_2 - f_1) + (f_3 - f_2) + \cdots \in S[[x_1, \dots, x_n]]$. This is well-defined.

Example 17.5. Let $p \in \mathbb{Z}$ be prime. The ring $\hat{Z}_{(p)}$, written $\mathbb{Z}_p$, is called the ring of p-adic integers. Let $(a_1 + (p), a_2 + (p^2), \dots) \in \mathbb{Z}_p$ where $0 \leq a_i < p^i$. For each i, $a_{i+1} \equiv a_i \pmod{p}^i$. So $a_{i+1} - a_i = b_i p^i$ for $b_i < p$. We write these as a power series, called a *p-adic expansion*: $a_1 + b_1 p + b_2 p^2 + \dots$. These partial sums recover the a_i. Note however, that when we add we need to carry over multiples of the p_i, in order to ensure that their coefficients be less than p. For instance, in $\mathbb{Z}_2$ we have $(1, 1, 1, 9, 9, \dots) + (1, 1, 1, 1, 1, 1, 1) = (0, 2, 2, 10, 10, \dots)$. The corresponding 2-adic expansions are

$$(1 + 0 \cdot 2 + 0 \cdot 2^2 + 1 \cdot 2^3) + (1 + 0) = (0 + 1 \cdot 2 + 0 \cdot 2^2 + 1 \cdot 2^3)$$

Note that $\mathbb{Z} \hookrightarrow \mathbb{Z}_p$. And since any p-adic expansion $a_0 + a_1 p + \dots$ with $0 \leq a < p$ corresponds to a unique element in $\mathbb{Z}_p$, $\mathbb{Z}_p$ is uncountable.

18. Lecture 19 — November 11, 2019

Definition 18.1. For R a ring and $M \subseteq R$ an ideal, if the natural map $R \to \widehat{R}_M$ is an isomorphism, R is *complete* with respect to M. When M is maximal, we say it's a *complete local ring*.

Note that the natural map will fail to inject when $\cap M^i \neq 0$, as $\cap M^i \mapsto 0 \in \widehat{R}_M$. From now on, we'll write $\widehat{R}$ to denote $\widehat{R}_M$. We have natural maps

$$\widehat{R} \to R/M^n$$
$$(f_1, \dots,) \mapsto f_n$$

Recall that $\widehat{M}_n = \{(f_1, \dots,) \in \hat{R} | f_i = 0 \ i \leq n\}$, and note that it's the kernel to the above map. Note also that the elements of $M^n \widehat{R}$ are generated by elements of the form $(ar_1, ar_2, \dots)$ for $a \in M^n$ and $(r_1, \dots,) \in \widehat{R}$. In particular, $ar_i \in M^n$, so it's 0 for $i \leq n$. Thus $M^n \widehat{R} \subseteq \widehat{M}_n$. If R is Noetherian, then this is an equality.

Example 18.2. For $R = \mathbb{C}[x_1, x_2, \dots]$ and $M = (x_1, x_2, \dots)$, you have that $(0, x_1, x_1 + x_2^2, x_1 + x_2^2 + x_3^3, \dots) \in \widehat{M}_1 - M\widehat{R}$.

Proposition 18.3. *$\widehat{R}$ is complete with respct to the filtration with the $\widehat{M}_i$.*

Proof. We saw last time that $\widehat{R}/\widehat{M}_n \equiv R/M^n$. So

$$\begin{aligned}\widehat{R} &= \varprojlim R/M^n \\ &= \varprojlim \widehat{R}/\widehat{M}_n \\ &= \text{completion of } \widehat{R} \text{ with respect to } \widehat{M}_1 \supset \widehat{M}_2 \supset \dots\end{aligned}$$

□

Theorem 18.4. *Let R be Noetherian and $\mathfrak{m} \subseteq R$ an ideal, $\widehat{R}$ the completion with respect to $\mathfrak{m}$. Then*

1. *$\widehat{R}$ is complete with resepct to $\mathfrak{m}\widehat{R}$.*
2. *$\widehat{R}$ is Noetherian.*
3. *$\widehat{R}$ is a flat R-module.*

Proof. See Eisenbud. □

You can think of completions as adding limits of certain sequences in the original ring, as with completions of metric spaces.

Example 18.5. In $R[x]$, the sequence $a_0, a_0 + a_1x_1, a_0 + a_1x_1 + a_2x^2$ "converges to" $\sum a_i x^i \in R[[x]]$.

In $\mathbb{Z}_2$, the sequence $1, 1+2, 1+2+2^2$ converges to $-1 = 1 + 2 + 2^2 + \dots \in \mathbb{Z}_2$.

Developing this idea requires a formal definition.

Definition 18.6. A sequence $a_1, a_2, \dots \in \widehat{R}$ *converges* to $a \in \widehat{R}$ if $\forall n \in \mathbb{N}$, $\exists i(n) \in \mathbb{N}$ such that $a - a_j \in \widehat{m}_n \ \forall j \geq i(n)$.

In words, convergence means that eventually the first n coordinates become the same and stay the same. This also gives rise to an intuitive definition of the Cauchy property.

Definition 18.7. A sequence $a_1, a_2, \dots \in \widehat{R}$ is *Cauchy* if $\forall n \in \mathbb{N}$ $\exists i(n) \in \mathbb{N}$ such that for $i, j \geq i(n)$, $a_i - a_j \in \widehat{M}_n$.

In this setting, it's pretty easy to see that a sequence is Cauchy if and only if it converges to an element of $\widehat{R}$, as one would hope. Next we'll talk about Hensel's lemma, which is motivated by the fact that in the p-adics, congruences are approximations: if $a \equiv b$ mod p^n, then they agree in their first n entries.

Example 18.8. $5 \equiv 1^2$ mod 2 and likewise mod 2^2, but not mod 2^3. And it's not the square of anything mod 8, so 5 isn't a square in $\mathbb{Z}_2$. Now, consider $7 \in \mathbb{Z}_3$. We have that $7 \equiv 1$ mod 3 and $7 \equiv (1+3)^2$ mod 9, and even $7 \equiv (1 + 3 + 3^2)^2$ mod 27. In fact, it turns out that we can continue indefinitely, so 7 is a square in $\mathbb{Z}_3$.

Hensel's lemma will give us conditions for determining when the root of a polynomial mod p can be lifted to a root in $\mathbb{Z}_p$. For instance, we've already seen that $x^2 - 5$ has no root in $\mathbb{Z}_2$, but that $x^2 - 7$ does have a root in $\mathbb{Z}_3$.

Lemma 18.9 (Hensel's lemma, version 1)**.** *If $f(x) \in \mathbb{Z}_p[x]$ and $a \in \mathbb{Z}_p$ satisfies $f(a) \equiv 0 \pmod{p}$ and $f'(a) \not\equiv 0 \pmod{p}$, then there's a unique $b \in \mathbb{Z}_p$ such that $f(b) = 0$ and $a \equiv b \pmod{p}$.*

Example 18.10. In the case $f(x) = x^2 - 5$ in $\mathbb{Z}_2$, $f'(x) = 2x \equiv 0 \pmod{p}$, so we can't find a square root this way. In $\mathbb{Z}_3$, $f(x) = x^2 - 7$ has $f(1) = 0 \pmod 3$ and $f'(1) = 2 \neq 0 \pmod 3$. So f has a root in $\mathbb{Z}_3$.

In general, which elements $c \in \mathbb{Z}_p$ are perfect squares? If we can write $c = p^n b$ with $n \geq 0$ and $p \nmid b$, then c is a square if and only if n is even and b is a square. Consider $f(x) = x^2 - b \in Z_p[x]$ and $f'(x) = 2x = 0$. If $p \neq 2$, then if b is a square mod p (say $b \equiv a^2 \mod p$), then $\overline{a}^2 = \overline{b}$

Lemma 18.11 (Hensel's lemma)**.** *Let R be a ring that's complete with respect to $\mathfrak{m}$. Let $f(x) \in R[x]$ be a polynomial with $f(a) \in f'(a)^2\mathfrak{m}$. Then $\exists$ a root b of f "near" a in the sense that $f(b) = 0$ and $b - a \in f'(a)\mathfrak{m}$. If $f'(a)$ is a nonzero divisor in R, then b is unique.*

Example 18.12. Let's go back to $\mathbb{Z}_2$ and $c = 2^n b$ for b odd. If b is a square, then $b = (1 + 2k)^2 = 1 + 4k + 4k^2 = 1 + 4(k + k^2)$. Since $k + k^2$ is even regardless of the parity of k, this tells us that $b \equiv 1 \mod 8$. If $f(x) = x^2 - b$, then $f'(x) = 2x$ and thus $f'(a)^2\mathfrak{m} \equiv 0 \mod 8$. Then take $a = 1$. That gives $a^2 - b \equiv 0 \mod 8$, so Hensel's lemma gives us that b is a 2-adic square.

We're done with completions - next time we'll talk about dimension theory!

19. Lecture 20 — November 13, 2019

Definition 19.1. The *Krull dimension* of a ring R, or just *dimension*, is $\dim R$, the supremum of lengths of chains of prime ideals in R, e.g. the chain $P_r \supsetneq P_{r-1} \supsetneq \cdots \supsetneq P_0$ has length r.

To see that this is a natural definition, note that it agrees with the dimension of finite-dimensional vector spaces when prime ideals are replaced with subspaces. If R is thought of as representing a scheme, its prime ideals are its subschemes and we arrive at an analagous definition. Unfortunately, it's pretty hard to perform computations with this definition.

Example 19.2. In $\mathbb{C}[x_1, \ldots, x_n]$, there's a chain $(x_1, \ldots, x_n) \supsetneq (x_1, x_{n-1}) \supsetneq \cdots \supsetneq (0)$. So the dimension is at least n, but it's not trivial to show that longer chains don't exist.

Definition 19.3. If $I \subsetneq R$ is an ideal, then the *dimension* of I is $\dim I = \dim R/I$. If I is prime, then we define the *codimension* of I to be the supremum of lengths of chains of primes descending from I. Then $\operatorname{codim} I = \dim R_I$. If I is an arbitrary ideal, define $\operatorname{codim} I = \min\{\operatorname{codim} P | P \supseteq I, P \text{ prime}\}$.

Definition 19.4. Let M be an R-module. Then $\dim M = \dim \operatorname{ann} M = \dim(R/\operatorname{ann} M)$.

Here's a question: if $I \subseteq R$ is an ideal, why can't we define $\operatorname{codim} I = \dim R - \dim I$? Even if I is prime, it's not obvious that you can choose a maximal chain of primes which contains I. The answer is that this is true in "nice" cases (e.g. if R is a domain which is finitely generated as a k-algebra), but it's not true more generally.

Example 19.5. Consider the following in $\mathbb{A}^3$: the plane defined by $x = 0$ and the x-axis defined by $y = z = 0$. In $k[x, y, z]$, this is cut out by the ideal $(x)(y, z) = (xy, xz)$. Let $R = k[x, y, z]/(xy, xz)$. There's the chain $(x) \subset (x, y) \subset (x, y, z)$, so $\dim R \geq 2$ (in fact, it equals 2). Setting $I = (x - 1, y, z) \subseteq R$, we have that $\dim I = \dim R/I = 0$ since R/I is a field. But $\operatorname{codim} I = \dim R_I = \dim k[x, y, z]_I/(y, z) = \dim k[x]_{(x-1)} = 1$.

The intuition of the mismatch is that dimension is global while codimension is local (it literally localizes). From here on out, we'll be using some of our earlier results regarding Artinian rings/modules. So we'll remind ourselves of them:

First recall that R is *Artinian* if every strictly decreasing chain of ideals is finite. We've already seen this next theorem.

Theorem 19.6. *Let R be a ring. Then R is Artinian if and only if R is Noetherian and all its prime ideals are maximal. Moreoever, if R is Artinian then it has only finitely many maximal ideals.*

Corollary 19.7. *If R is Noetherian, then R is Artinian if and only if $\operatorname{Spec} R$ is finite.*

Now we can translate these results in terms of dimension.

Corollary 19.8. *If R is Noetherian, then* $\dim R = 0 \iff$ *R is Artinian* $\iff$ *$\operatorname{Spec} R$ is finite.*

When we talked about the 'going up theorem', we saw that we can lift an increasing chain of prime ideals in R to a ring S integral over R. We also showed that if two primes in S, one contained in the other, have the same intersection in R then they must be equal.

Proposition 19.9. *Let $\phi : R \to S$ be a map of rings that makes S integral over R. Then any prime ideal of R that contains* $\ker \phi$ *is the pre-image of some ideal of S. Moreoever, if $I \subseteq S$ is some ideal, then* $\dim I = \dim \phi^{-1}(I)$.

Proof. If $I \subseteq S$ then $\ker \phi \subseteq \phi^{-1}(I)$, so $R/\phi^{-1}(I) \cong \phi(R)/\phi(R) \cap I$. So we can replace R with its image in S and assume $R \subseteq S$. Then the first statement follows from the going up theorem. For the second statement, consider a chain of primes containing $\phi^{-1}(I) \subseteq R$: $P_0 \subsetneq P_1 \subsetneq \ldots$. By going up, there exists a prime chain $Q_0 \subsetneq Q_1 \subsetneq \ldots$ in S containing I. So $\dim I \geq \dim \phi^1(I)$. On the other hand, going down means that chains of primes in S descend to chains of primes of equal length in R, so in fact the dimensions coincide. $\square$

Corollary 19.10. *Let $\phi : R \to S$ be a map of rings such that S is Noetherian and integral over R. Let $\psi : SpecS \to SpecR$ be the induced map. Then*

1.) *The fibers of ϕ over closed points (i.e. maximal ideals) are finite.*
2.) *If $X = V(I) \subseteq SpecS$ is closed, then $\psi(x) \subseteq SpecR$ is closed with the same dimension as X, i.e. $\psi(X) = V(J)$ and $\dim_S I = \dim_R J$.*

Proof. Kind of involved but not super exciting. □

20. Lecture 21 — November 20, 2019

Today we'll finish the principal ideal theorem (PIT) from last time. Again we'll be taking all rings to be Noetherian. Recall the statement of PIT: if P is a minimal prime over $(x_1, \ldots, x_c)$ then $\operatorname{codim} P \leq c$. The partial converse we'll prove today is as follows:

Corollary 20.1. *If P is a prime of codimension c, then P is minimal over an ideal generated by c elements.*

Proof. By induction, for $0 \leq r < c$, we can choose $x_1, \ldots, x_r \in P$ to generate an ideal of codimension r. The base case is $r = 0$. Any prime of codimension 0 is minimal over 0. Let $Q_1, \ldots, Q_n$ be the minimal primes contained in P. There are only finitely many minimal primes, as these are associated primes of 0 (of which there are only finitely many). By prime avoidance, $P \neq \cup Q_i$, so $\exists x_1 \in P$ with x_1 not in any Q_i. Then $P/(x_1)$ has codimension $\leq c - 1$.

So by induction, $P/(x_1)$ is minimal over an ideal generated by at most $c - 1$ elements. Let $(x_2, \ldots, x_d)$ be lifts of these elements in P. We have that P is minimal over $(x_1, \ldots, x_d)$. So $d \leq c$, but $c = \operatorname{codim} P \leq d$ by the PIT. Thus $d = c$. □

Recall that for R Noetherian, R is a UFD if and only if every prime minimal over a principal ideal is principal.

Corollary 20.2. *Let R be an integral domain. If every codimension 1 prime of R is principal, then R is a UFD.*

Proof. Primes minimal over principal ideals have codimension 1 or (because we're in a domain) are zero. □

> "Questions? You should have questions, because I have questions. I'm confused." - Dr. Ullery

The next thing we'll talk about is systems of parameters, continuing to assume that our rings are Noetherian.

Corollary 20.3. *If R is a local ring with maximal ideal $\mathfrak{m}$, then $\dim R$ is the smallest d such that $\exists$ elements $x_1, \ldots, x_d \in \mathfrak{m}$ with $\mathfrak{m}^n \subseteq (x_1, \ldots, x_d)$ for $n >> 0$.*

Proof. If $\mathfrak{m}^n \subseteq (x_1, \ldots, x_d) \subseteq \mathfrak{m}$, then $\mathfrak{m}$ is minimal over $(x_1, \ldots, x_d)$. So $\dim R \leq d$, by PIT. In the other direction, we can find $x_1, \ldots, x_\ell \in \mathfrak{m}$ with $\ell = \dim R$ such that $\mathfrak{m}$ is minimal over $(x_1, \ldots, x_\ell)$. Then $R/(x_1, \ldots, x_\ell)$ has a single prime. So $\mathfrak{m}_\mathfrak{m}$ is nilpotent and $\dim R = e \geq d$, since d is the minimal such number. □

Definition 20.4. For R a local ring, a sequence of elements $x_1, \ldots, x_d$ as in the corollary is called a *system of parameters* for R.

Proposition 20.5. *If $(R, \mathfrak{m})$ is a local ring of dimension d, TFAE:*

1.) $x_1, \ldots, x_d \in \mathfrak{m}$ is a system of parameters
2.) $rad(x_1, \ldots, x_d) = \mathfrak{m}$
3.) $\mathfrak{m}$ is minimal over $(x_1, \ldots, x_d)$

Recall that local rings have finite length if and only if they're Artinian. This is the case if and only if the ring's maximal ideal is the only prime ideal, and that's the case if and only if $\mathfrak{m}^n = 0$ for $n >> 0$. So for R a local ring, $\mathfrak{m}^n \subseteq q$ for $n >> 0$ if and only if R/q has finite length. Such an ideal q is said to have *finite colength*.

If M is a finitely generated module over a local ring R, then $q \subseteq \mathfrak{m}$ has *finite colength* on M if M/qM has finite length. Just like with rings, this is the case if and only if a power of $\mathfrak{m}$ annihilates M/qM.

Proposition 20.6. *If R is anything, M a finitely generated R-module, and $q \subseteq R$ an ideal, then $rad(ann(M/qM)) = rad(q + annM)$.*

Proof. It suffices to show that a prime P contains $\text{ann}(M/qM) \iff P$ contains $q + \text{ann}M$. Recall $P \supseteq \text{ann}(M/qM) \iff (M/qM)_P \neq 0$. By Nakayama, $M_P/q_PM_P \neq 0 \iff M_P \neq 0$ and $q_P \subseteq P_P$. And those conditions are satisfied exactly when $P \supseteq q$ and $P \supseteq \text{ann}M$. □

Proposition 20.7. *Let $(R, \mathfrak{m})$ be local ring and M a finitely generated R-module. Then* dim M *is the least number d such that there exists an ideal of finite colength on M generated by d elements.*

That's all for today - next time we'll keep talking about systems of parameters.

21. Lecture 22 — November 18, 2019

Today we'll talk about the principal ideal theorem, and we'll be supposing that all rings are Noetherian. Last time we talked about a ring's dimension, which is the maximum length of a chain of prime ideals in the ring. We saw that calculating dimension is pretty hard, and one of our goals is now to develop tools to calculate dimension. One class of tools makes use of the ring's generators.

If (a) is prime, then if $b = ra$ nonzero and prime then r is a unit so $(b) = (a)$. Thus $\text{codim}(a) \leq 1$. In fact, a stronger statement holds:

Proposition 21.1. *Any prime P properly contained in a principal ideal $(x) \neq R$ has codimension 0.*

Proof. Suppose $Q \subsetneq P \subsetneq (x)$ with Q prime. Then R/Q is an integral domain. Without loss of generality, we can replace R with R/Q and assume that $Q = 0$ and that R is a domain. If $y \in P$ then $y = ax$ for some a. Since $x \notin P$, it must be that $a \in P$. So $P = xP$. Then there must be a $b \in (x)$ such that $(1 - b)P = 0$. Since R is a domain, it must be that $b = 1$, producing contradiction. □

Theorem 21.2 (Krull's principal ideal theorem)**.** *If $x \in R$ and P is minimal among primes containing x, then* codim $P \leq 1$.

Before we can prove this, we recall a corollary about primes minimal over a given ideal - for R Noetherian and $I \subseteq R$ an ideal and $P \subseteq I$ a prime, TFAE:

a) P is minimal among primes containing I.
b) R_P/I_P is Artinian.
c) $P_P^n \subseteq I_P$ in R_P for $n >> 0$.

This is 2.19 in Eisenbud. We'll also need a new definition.

Definition 21.3. $Q \subseteq R$ prime. The nth *symbolic power* of Q is

$$\begin{aligned} Q^{(n)} &= Q^n R_Q \cap R \\ &= \{r \in R | sr \in Q^n \text{ for some } s \in R \setminus Q\} \end{aligned}$$

It's not hard to see that $Q^n \subseteq Q^{(n)} \subseteq Q$. It also turns out that $(Q^{(n)})_Q = (Q_Q)^n$.

Example 21.4. Let $R = k[x,y,z]/(xy - z^2)$ and set $P = (x,z)$. Then $y \notin P$ but $xy = z^2 \in P^2$, so $x \in P^{(2)} \setminus P^2$.

Now back to our original goal.

Proof of Krull's PIT. Let $x \in R$ and P be a minimal prime over (x). We'll show that if $Q \subsetneq P$ is prime, then $\dim R_Q = 0$, i.e. $\operatorname{codim} Q = 0$. This shows that $\operatorname{codim} P \leq 1$, since $\operatorname{codim} P = \operatorname{codim} P_P$. So we can assume that R is local and P is maximal. Since P is minimal over (x), the corollary says that $R/(x)$ is Artinian.

Thus the chain $(x) + Q \supset (x) + Q^{(2)} \supset (x) + Q^{(3)} \supset \dots$ stabilizes. Say $(x) + Q^{(n)} = (x) + Q^{(n+1)}$. Then $Q^{(n)} \subseteq (x) + Q^{(n+1)}$. So if $f \in Q^{(n)}$, we can write $f = ax + g$ for $g \in Q^{(n+1)}$. Thus $ax = f - g \in Q^{(n)} \subseteq Q$, and $axb \in Q^n$ for some $b \in R \setminus Q$. $x \notin Q$ by minimality of P, so $xb \in R \setminus Q$ and thus $a \in Q^{(n)}$. So $Q^{(n)} \subseteq (x)Q^{(n)} + Q^{(n+1)}$. The reverse inclusion is clear, so $Q^{(n)} = (x)Q^{(n)} + Q^{(n+1)}$. So, in $R/Q^{(n+1)}$, $\overline{Q^{(n)}} = \overline{(x)}\,\overline{Q^{(n)}}$.

Then, by Nakayama, $\overline{Q^{(n)}} = 0$ and thus $Q^{(n)} = Q^{(n+1)}$. Now recall that $(Q^{(n)})_Q = (Q_Q)^n$, thus in R_Q we have that $(Q_Q)^n = (Q_Q)^{n+1}$. Again using Nakayama, we have that $(Q_Q)^n = 0$. So R_Q is Artinian, by the corollary, and R_Q has dimension 0. □

Theorem 21.5. *If $x_1, \dots, x_c \in R$ and P is a minimal prime over $(x_1, \dots, x_c)$, then* $\operatorname{codim} P \leq c$.

Proof. Again we make use of the fact that $\operatorname{codim} P = \dim R_P$ to assume that R is local with maximal ideal P. By the corollary, $P^n \subseteq (x_1, \dots, x_c)$ for $n >> 0$. Let P_1 be a prime such that $P \supsetneq P_1$ with no primes in between. We'll show that P_1 is minimal over an ideal generated by $c-1$ elements. By induction, $\operatorname{codim} P_1 \leq c - 1$ and we're done.

By minimality of P, P_1 can't contain all x_i. Assume $x_1 \notin P_1$. Then P is a minimal prime over (x_1, P_1), meaning P is nilpotent in $R/(P_1, x_1)$. I spaced out for the rest of the proof. □

Corollary 21.6. *Let $P \subseteq R$ be a prime ideal (R Noetherian). Then any strictly decreasing chain of primes has length at most the number of generators of P.*

In particular, since $(x_1, \dots, x_c) \subseteq k[x_1, \dots, x_n]$ has descending chain $(x_1, \dots, x_c) \supset (x_2, \dots, x_c) \supset \cdots \supset 0$, we know that the codimension of $(x_1, \dots, x_c)$ is at least c. By the PIT it's at most c, so in fact $\operatorname{codim}(x_1, \dots, x_c) = c$.

22. Lecture 23 — November 25, 2019

Last time we were talking about systems of parameters, and we wanted to think about a local ring where the generators of the maximal ideal don't form a system of parameters. Here's a question for next time: what's an example of a local ring where the generators of the maximal ideal do not form a system of parameters.

Recall that if R is a local ring, then $q \subseteq R$ has finite colength $\iff$ R/q has finite length $\iff$ $m^n \subseteq q$ for $n >> 0$. We've also seen that if M is a finitely generated module over a local ring $(R, \mathfrak{m})$, then $q \subseteq \mathfrak{m}$ has finite colength on M if M/qM has finite length $\iff$ $\mathfrak{m}^n$ annihilates M/qM for $n >> 0$.

Proposition 22.1. *Let $(R, \mathfrak{m})$ be a local ring, M a finitely generated R-module, and $q \subseteq R$ an ideal. Then*

- *a.) q has finite colength on M $\iff$ $(q + annM) \supseteq \mathfrak{m}^n$ for $n >> 0$ $\iff$ q has finite colength on $R/annM$.*
- *b.) If $0 \to M' \to M \to M'' \to 0$ is a short exact sequence of R-modules, then q has finite colength on M $\iff$ q has finite colength on M' and M''.*
- *c.) $\dim M$ is the least number d such that there exists an ideal of finite colength on M generated by d elements.*

Proof. For a.), note that q has finite colength on $M \iff \mathrm{Rad}(q + \mathrm{ann}M) = \mathrm{rad}(\mathrm{ann}(M/qM)) = \mathfrak{m}$. And this holds $\iff \mathfrak{m}^n \subseteq q + \mathrm{ann}M$ for $n >> 0$. Note now that $(R/\mathrm{ann}M)/q(R/annM) \cong R/q + \mathrm{ann}M$, which has annihilator $q + \mathrm{ann}M$. So q has finite colength $R/\mathrm{ann}M$ $\iff$ $\mathrm{rad}(q + \mathrm{ann}M) = \mathfrak{m}$ $\iff$ q has finite colength on M.

For b.), note that if q has finite colength on M, then $\mathrm{ann}M \subseteq \mathrm{ann}M' \cap \mathrm{ann}M''$. So $q + \mathrm{ann}M \subseteq q + \mathrm{ann}M', q + \mathrm{ann}M''$. Since $\mathrm{rad}(\mathrm{ann}M/qM)$ is maximal, the radicals of $\mathrm{ann}(M'/qM/)$ and $\mathrm{ann}(M''/qM'')$ are as well. In the other direction, assume that q has finite colength on M' and M''. Tensoring by R/q, we have an exact sequence

$$M'/qM' \to M/qM \to M''/qM'' \to 0$$

which give us what we want.

For c.), note that $\dim M = \dim R/\mathrm{ann}M$, which equals the smlleast number d such that $q = (x_1, \ldots, x_d)$ has finite colength on $R/\mathrm{ann}M$ for $n >> 0$. By a.), q has finite colength on M if and only if it has finite colength on $R/\mathrm{ann}M$. □

The hope now is to get a result like PIT for dimension rather than codimension. We'd like to say something about how modding out by a single elements alters the dimension of a module.

Corollary 22.2. *If $(R, \mathfrak{m})$ is a local ring and M a finitely generated R-module, then for $x \in \mathfrak{m}$, we have $\dim M - 1 \leq \dim M/xM \leq \dim M$.*

Proof. Only the first inequality demands justification. If $d = \dim M/xM$, then there exists $q = (x_1, \ldots, x_d)$ of finite colength on M/xM. This means $M/(x, q)M = M/(x_1, \ldots, x_d, x)M$ has finite length. So $(x_1, \ldots, x_d, x)$ has finite colength on M. So $\dim M \leq d + 1$, and we're done. □

Proposition 22.3. *Let $(R, \mathfrak{m})$ be a local ring and S an R-algebra with $mS \neq S$. Then* $\mathrm{codim}\, \mathfrak{m}S \leq \mathrm{codim}\, \mathfrak{m}$.

Proof. If $x_1, \dots, x_d$ is a system of parameters in R, then any prime in S minimal over $\mathfrak{m}S$ is minimal over $I = (x_1, \dots, x_d)$. Suppose P is minimal over $\mathfrak{m}S$. Then let $I \subseteq Q, \mathfrak{m}S \subseteq P$ for Q prime. Then for $\psi : R \to S$ inducing the algebra, we have $(x_1, \dots, x_d) \subseteq \psi^{-1}(I) \subseteq \psi^{-1}(Q) \subseteq \mathfrak{m}$. So $\psi^{-1}(Q) = m$ and thus $\mathfrak{m}S \subseteq Q$ and $P = Q$. Our inequality follows from the PIT. □

What can we say when moreover S is local? It turns out that we can say quite a bit more.

Theorem 22.4. *Let $\psi : (R, \mathfrak{m}) \to (S, \mathfrak{n})$ be a map of local rings such that $\psi(\mathfrak{m}) \subseteq \mathfrak{n}$. Then* $\dim S \leq \dim R + \dim S/\mathfrak{m}S$.

Proof. Let $d = \dim R$ and $e = \dim S/\mathfrak{m}S$. Let $x_1, \dots, x_d \in \mathfrak{m}$ be a system of parameters for R and $y_1, \dots, y_e \in \mathfrak{n} \subseteq S$ with images in the quotient which are a system of parameters for $S/\mathfrak{m}S$. Then for $\alpha >> 0$, we have $\mathfrak{n}^\alpha \subseteq (y_1, \dots, y_e) + \mathfrak{m}S$. And for $\beta >> 0$, we have $\mathfrak{m}^\beta \subseteq (x_1, \dots, x_d)$. Then

$$\begin{aligned} n^{\alpha\beta} &\subseteq ((y_1, \dots, y_e) + \mathfrak{m}S)^\beta \\ &\subseteq (y_1, \dots, y_e) + \mathfrak{m}^\beta S \\ &\subseteq (x_1, \dots, x_d, y_1, \dots, y_e)S \end{aligned}$$

So $\dim S \leq d + e$, as desired. □

What's going on here geometrically is that for $X \to Y$ a map of varieties (or schemes), the dimension of X is at most the dimension of Y plus the dimension of a fiber.

Something that will be useful going forward is the going down theorem.

Theorem 22.5. *Let $\phi : R \to S$ be a map of rings such that S is a flat R-module. If $P \supset P'$ are primes of R and Q is a prime of S with $\phi^{-1}(Q) = P$, then there exists a prime Q' of S contained in Q such that $\phi^{-1}(Q') = P'$. In fact, Q' may be taken to be any prime of S which is contained in Q and minimal over $P'S$.*

Proof. Since $P'S \subseteq Q$, we can find a prime $Q' \subseteq Q$ minimal over $P'S$. I claim that $S \otimes R/P'$ is flat over R/P'. If $M' \subseteq M$ are R/P'-modules, then they're R-modules. So $S \otimes_R M' \hookrightarrow S \otimes_R M$. With some work, we can see that $S \otimes R/P' = S/P'S$ is flat over R/P'. So we can replace R with R/P' and S with $S/P'S$ and reduce to the case $P' = 0$. I lost track for the rest of this proof. □

23. Lecture 24 — December 2, 2019

Last time we saw that if $R \to S$ is such that S is a flat R-module then if $P_0 \supseteq P_1 \supseteq \cdots \supseteq P_n$ is a chain of prime ideals in R and Q_0 lies over P_0 then there exist $Q_0 \supseteq Q_1 \supseteq \cdots \supseteq Q_n$ in S such that Q_i lies over P_i. This was the going down theorem.

We also saw that if $\psi : (R, \mathfrak{m}) \to (S, \mathfrak{n})$ is a local map such that $\psi(\mathfrak{m}) \subseteq \mathfrak{n}$, then $\dim S \leq \dim R + \dim S/\mathfrak{m}S$. Geometrically, this is a statement somewhat like rank nullity: the dimension of the domain is at most the sum of that of the target and that of the fiber.

Corollary 23.1. *If R and S are as above and S is a flat R-module, then* $\dim S = \dim R + \dim S/\mathfrak{m}S$.

Proof. We need only show that $\dim S \geq \dim R + \dim S/\mathfrak{m}S$. This follows from the going down theorem. Let be $Q \subseteq S$ a prime minimal over $\mathfrak{m}S$ such that $\dim Q = \dim S/\mathfrak{m}S$. Then $\dim S \geq \dim Q + \operatorname{codim} Q = \dim S/\mathfrak{m}S + \operatorname{codim} Q$. So it remains to show $\operatorname{codim} Q \geq \dim R$. Since $Q \supseteq \mathfrak{m}S$ so $\psi^{-1}(Q) = \mathfrak{m}$. Let $\mathfrak{m} \supseteq P_1 \supseteq \cdots \supseteq P_d$ with $d = \dim R$. By going down, we have an analogous chain in Q. So $\operatorname{codim} Q \geq \dim R$, and we're done. □

Corollary 23.2. *If R is a ring, then $\dim R[x] = 1 + \dim R$. In particular, if k is a field then $\dim k[x_1, \ldots, x_n] = n$.*

Proof. Let $P_1 \subseteq \cdots \subseteq P_d$ be a chain of primes in R. Then in $R[x]$ we have the chain $P_1R[x] \subseteq \cdots \subseteq P_dR[x] \subseteq P_dR[x] + (x)$. Note that $P_dR[x] + (x)$ is prime because modding $R[x]$ by it gives R/P_d, a domain. So $\dim R[x] \geq 1 + \dim R$. For the other inequality, it suffices to show that the codimension of a maximal ideal in $R[x]$ is at most the codimension of its intersection with $R + 1$. This can be done, though it's slightly involved. □

For the rest of the class we'll talk about regular local rings. Let R be a local ring of dimension d with maximal ideal $\mathfrak{m}$. Then, by the PIT, $\mathfrak{m}$ can't be generated by fewer than d elements. $\mathfrak{m}$ is generated by exactly d elements if and only if it's generated by a system of parameters, by definition. In this case, R is called *regular* and $\mathfrak{m}$'s generators form a *regular system of parameters*.

Example 23.3. Let $R(\mathbb{C}[x,y]/(y^2 - x^3))_{(x,y)}$. (x, y) isn't principal in R, but $(x, y)^2 = (x^2, xy, y^2) \subseteq (x)$. So $\dim R$ is 1 (it's not 0 because it's a domain and has another prime ideal), and x is a system of parameters. Notably, this is a local ring that's not regular.

Geometrically, regular local rings correspond to smooth points on schemes and varieties.

Proposition 23.4. *If R is a regular local ring, it's an integral domain.*

Proof. Let $\mathfrak{m} \subseteq R$ be the maximal ideal. We induct on $\dim R$. If $\dim R = 0$, then $\mathfrak{m} = 0$ and R is a field. Assume $\dim R = d > 0$. We know $\mathfrak{m}^2 \neq \mathfrak{m}$, by Nakayama. By prime avoidance, we can find $x \in \mathfrak{m}$ that avoids the (finitely many) minimal primes of R and $\mathfrak{m}$. Now set $S = R/(x)$, and let $\mathfrak{n} = \mathfrak{m}S$ be the maximal ideal of S. x isn't in any minimal primes of R, so $\dim S > \dim R$. In order to induct, we need to show that S is regular. This is kind of a pain, but it can be done. □

Definition 23.5. A sequence $x_1, \ldots, x_d \in R$, not necessarily a local ring, is called a *regular sequence* if $(x_1, \ldots, x_d) \subsetneq R$ and $x_i + 1$ is always a nonzerodivisor in $R/(x_1, \ldots, x_i)$.

Example 23.6. In $\mathbb{C}[x, y, z]$, we have that $x, y(1 - x), z(1 - x)$ is a regular sequence but $y(1 - x), z(1 - x), x$ is not a regular sequence. So order matters. In a local ring it turns out that order doesn't matter.

Corollary 23.7. *If $x_1, \ldots, x_d$ is a regular system of parameters in a regular local ring, then $x_1, \ldots, x_d$ is a regular sequence.*

Proof. For each i, $R/(x_1, \ldots, x_i)$ is local of dimension at least $d - i$, by the PIT. The maximal ideal is generated by $x_{i+1}, \ldots, x_d$, so indeed the dimension equals $d - i$. Then the quotient is regular and therefore an integral domain. □