MATH 221: COMMUTATIVE ALGEBRA

RAY SHANG

Abstract. Notes for Harvard's Math 221 taught by Salim Tayou.

Contents

Date: Fall 2022.

1. Sept 1: prime and maximal ideal, integral domain, PID, nilradical, Jacobson radical

What is commutative algebra? Importance of commutative algebra. Last 50-60 years, proven to be a powerful tool to study other fields: algebraic geometry, number theory, algebraic topology, etc.

What does an algebraic notion of deformation look like?

Text: David Eisenbud. Commutative algebra with a view towards algebraic geometry. Roughly up to Chapter 13 of the book.

Conventions

- all rings are commutative with units
- $f : A \to B$ ring homomorphism, then $f(1_A) = 1_B$. units maps to units.

Let R be a ring. Recall an **ideal** of R is an abelian subgroup $I \subseteq R$, such that $\forall a \in R$, $b \in I$, $ab \in I$.

Definition 1.1. An ideal $p \subseteq R$ is a prime ideal if $p \neq R$, and $\forall x, y \in R$, $xy \in p \implies x \in p$ or $y \in p$.

Definition 1.2. An ideal $m \subseteq R$ is maximal if $m \neq R$ and for every ideal I such that any ideal I strictly containing m , we must have $I = R$.

Proposition 1.3. *If m is a maximal ideal, then m is a prime ideal.*

Proof. Wnat to prove if you have $xy \in m$, then one of them is in m. WLOG say $x \notin m$. Want to show $y \in m$. Look at the ideal generated by m and (x). Since $x \notin m$, by maximality, this ideal must be R. But it must contain 1. Then $1 = xu + v$, for $u \in R, v \in m$. So multiply by y, so $y = yxu + yv$. And $yv \in m$ and $yx \in m$, by assumption. So $y \in m$. So m is prime ideal. □

Definition 1.4. A **nilpotent element** $x \in R$ is an element such that there exist $n \geq 1$ s.t. $x^n = 0$.

A **unit element** $u \in R$ is an element which has multiplicative inverse: $uv = 1$.

A zero divisor $x \neq 0 \in R$ is an element s.t. there exist $y \neq 0$ s.t. $xy = 0$.

A ring with no zero-divisors is called an **integral domain**. (Note that the zero ring is not an integral domain.)

An ideal I is a **principal ideal** if $I = (a)$ for some $a \in R$. So generated by an element a.

A ring R is **principal ideal domain** or PID if it is an integral domain and every ideal is principal.

Proposition 1.5. *Let p, m be ideals of R.*

p is prime $\iff$ R/p is an integral domain.

p is maximal $\iff$ R/p is a field.

Proof. Assume that p is prime. Take element $\overline{x} \in R/p$ such that $\overline{x} \neq 0$. So $x \notin p$. If $\overline{y} \in R/p$ such that $\overline{xy} = 0$, then $xy \in p$ which means $y \in p$, which means $y\overline{y} = 0$.

Other direction.

Maximality statement. If m is maximal, then we need to show every element of R/m has a multiplicative inverse. Let $x \in R$, $\overline{x} \neq 0 \in R/m$. So $x \notin m$. Want to show there exist $\overline{y} \in R/m$ such that $\overline{xy} = 1 \in R/m$, so $xy + m = 1$.

□

Example 1.6. $p = (x - y) \subset k[x, y]$ is prime but not maximal.

The next theorem will utilize Zorn's lemma.

Lemma 1.7 (Zorn's Lemma)**.** *Let P be a nonempty, partially ordered set. Suppose every chain of P has an upper bound. Then there exist at least one maximal element of P.*

Theorem 1.8. *Let R be a nonzero ring. Then R has a maximal ideal.*

Proof. Consider $(0) \subset R$. If (0) is maximal, we're done. Otherwise, choose some $(0) \subset I \subset R$. If I is maximal, we're done. Otherwise:

Let $\mathcal{C} = \{I | I \neq R\}$ be the set of ideals $\neq R$. Since $(0) \in \mathcal{C}$, $\mathcal{C}$ is nonempty. Consider any chain of $\mathcal{C}$, with order relation given by inclusion. The chain is of the form $\{I_\alpha\}$. Then it has upperbound $I = \bigcup I_\alpha$. Furthermore, $I \in \mathcal{C}$ since if $I = R$, then $1 \in I \implies 1 \in I_\alpha$, which cannot happen.

By Zorn's lemma, $\mathcal{C}$ has a maximal element. This maximal element of $\mathcal{C}$ is then a maximal ideal of R.

□

Lemma 1.9. *The set n of nilpotent elements of R is an ideal, and R/n has no nonzero nilpotent elements.*

Proof. The product axiom is not hard to see. Only tricky thing to see is to prove abelian subgroup. Suppose $x, y \in n$. So $x^n = 0, y^m = 0$. Then show $(x + y)$ is nilpotent. Just raise it to $(x + y)^{n+m+1}$. By binomial identity, this is nilpotent.

Suppose R/n had some nilpotent element $\overline{x}$. So $\overline{x}^k = 0$. So $x^k \in n$. But then x^k is nilpotent. So $x \in n$. So $\overline{x} = 0$. □

Definition 1.10 (nilradical)**.** The nilradical of R is $\bigcap p$, the intersection of all prime ideals of R.

Definition 1.11 (Jacobson radical)**.** The Jacobson radical is $\bigcap m$, the intersection of all maximal ideals of R. Denoted $J(R)$¿

Proposition 1.12. *The nilradical is containd inside the Jacobson radical. Furthermore, the nilradical equals the ideal of all nilpotent elements.*

Proof. The first statement follows because we proved every maximal ideal is a prime ideal. Let's prove the second statement.

First, suppose x is nilpotent. Then $x^n = 0$ for some $n \geq 1$. Then $x^n \in p$ for all prime ideals p. Then $x \in p$.

For the other inclusion, we utilize Zorn's lemma once again. Suppose $x \in \bigcap p$, the nilradical. Assume FSOC that x is not nilpotent. Let $\mathcal{C} = \{I | x^n \notin I, \forall n \geq 1\}$. This is nonempty since $(0) \in \mathcal{C}$. It's easy to see every chain has an upperbound (take the union of elements of the chain). By Zorn's lemma, there exists a maximal element $I \in \mathcal{C}$.

We show that I is actually a prime ideal. If we prove this, then $x \in \bigcap p \subset I$, which would be a contradiction since $I \in \mathcal{C}$. Then x would have to be nilpotent.

So let's prove I is a prime ideal. Suppose $u, v \notin I$. Then $I \subset I + (u), I + (v)$, and by maximality of I in $\mathcal{C}$, we know that there exist $n_1, n_2 \geq 1$ such that $x^{n_1} \in (u) + I$ and $x^{n_2} \in (v) + I$. Then $x^{n_1+n_2} \in (uv) + I$. But $(uv) + I \notin \mathcal{C}$. So $uv \notin I$. Thus, I is prime, and we're done.

□

Proposition 1.13. *$x \in J(R) \iff 1 - xy$ is a unit for all $y \in R$.*

Proof. Hint: use fact that z is a unit $\iff$ for any maximal ideal m, $z \notin m$.

First we prove the hint. Suppose z is a unit. Then clearly z cannot be contained in any maximal ideal. Now suppose nonzero z is not in any maximal ideal. If $(z) = R$, then we're done. Suppose z was not a unit, so $(z) \neq R$. Let $\mathcal{C} = \{I \neq R | z \notin I\}$. Note $\mathcal{C}$ is nonempty, and every chain is bounded, so by Zorn's, there is at least one maximal element of $\mathcal{C}$. But this ideal is a maximal ideal. Contradiction. So z is a unit.

Prove the forward direction first. Suppose $x \in J(R)$. So x is in m for every maximal ideal m. Suppose for some y, we had $1 - xy$ is not a unit. By the hint, $1 - xy$ is contained in some maximal ideal. But if this were the case, since x is in that maximal ideal, $1 - xy + x = 1$ is in the maximal ideal, contradiction. So $1 - xy$ is a unit for every $y \in R$.

Suppose $1 - xy$ is a unit for all $y \in R$. Let m be some maximal ideal. Assume FSOC that $x \notin J(R)$. So x is not contained in some maximal ideal m. But then $(x) + m = R$. So $xy + (m) = 1$. Then $1 - xy \in (m)$. But by assumption $1 - xy$ is a unit, so $(m) = R$. Contradiction. □

2. Sept 6: radical, Noetherian rings, Hilbert's basis theorem

We begin with a useful bijection.

Proposition 2.1. *Let R be a ring, and $I \subset R$ an ideal. There is a one-to-one correspondence between ideals of R containing I, and ideals of R/I. This correspondence is given by the projection $\pi : R \to R/I$, and π^{-1}.*

Proof. It's easy to verify that if $I \subset R$ is an ideal, the $\pi(I)$ is an ideal of R/I, and if $J \subset R/I$ is an ideal, then $\pi^{-1}(J) \subset R$ is an ideal containing I. Surjectivity immediately holds by the latter.

For injectivity, suppose we had two ideals I_1, I_2 containing I that project to the same ideal $J \subseteq R/I$. We'll show that we must have $I_1, I_2 = \pi^{-1}(J)$. WLOG just consider I_1. Note we must have $I_1 \subset \pi^{-1}(J)$. Suppose there is some element $b \in \pi^{-1}(J)$ s.t. $b \notin I_1$. Since $\pi(I_1) = J$, there must be some element $a \in I_1$ such that $\pi(a) = \pi(b)$. So they map to the same element $b + I \in R/I$. But then $a - b \in I \subset I_1$. But if $a \in I_1$, this implies $b \in I_1$. So in fact, $I_1 = \pi^{-1}(J)$. □

We have a similar statement of 2.1 in the case of prime ideals. Namely, the prime ideals of R containing I are in bijection with the prime ideals of R/I. Same goes for maximal ideals.

For the rest of this section, it will be useful to also be familiar with basic operations of ideals, such as addition of ideals and multiplication of ideals.

Last time we defined the nilradical. We can generalize this to the notion of a radical.

Definition 2.2 (Radical)**.** Let $I \subseteq R$ be an ideal. Then the radical of I is $\sqrt{I} = \{a \in R | a^n \in I, \text{ for some positive n }\}$.

Example 2.3. $\sqrt{(0)} = n = \bigcap p$, the nilradical. The name makes sense now.

We have the following lovely theorem.

Theorem 2.4. *$\sqrt{I} = \bigcap p$, for all prime ideal p that contains I.*

Proof. Let $\pi : R \to R/I$ be the projection. Note $\sqrt{I} = \pi^{-1}(\sqrt{0})$. But by 1.12, we have $\sqrt{0}$ is the intersection of all prime ideals of R/I. But then the preimage of the intersection of all prime ideals of R/I is the intersection of the preimage of all prime ideals of R/I. This is the intersection of all prime ideals of R containing I. □

The idea is that, we already did the work in showing the interesection of all prime ideals is the same as all the nilpotent elements. We're merely appealing to the bijective correspondence between ideals of R containing I and ideals of R/I, to say that, really, the radical of I is the intersection of all prime ideals containing I.

Now that we have some insight into the radical, let's show that we can also do nice things with it.

Proposition 2.5. *(1) The radical ideal $\sqrt{I}$ is an ideal of R.*
(2) $\sqrt{IJ} = \sqrt{I \cap J} = \sqrt{I} \cap \sqrt{J}$
(3) $\sqrt{I^n} = \sqrt{I}$
(4) $\sqrt{I+J} = \sqrt{\sqrt{I} + \sqrt{J}}$.

Proof. Proof of (1): This follows from the fact that $\sqrt{I} = \pi^{-1}(\sqrt{0})$, and $\sqrt{0}$ the nilradical we already know to be an ideal of R/I.

Proof of (2): Let's prove that $\sqrt{IJ} = \sqrt{I \cap J}$. Note $IJ \subseteq I \cap J$. Then $\sqrt{IJ} \subseteq \sqrt{I \cap J}$ immediately. Prove reverse inclusion. Suppose $x \in \sqrt{I \cap J}$. Then $x^n \in I \cap J$ for some n. Then $x^{2n} = x^n x^n \in I \cap J$, which implies $x^n x^n \in IJ$. So $x \in \sqrt{IJ}$. Now let's prove that $\sqrt{I \cap J} = \sqrt{I} \cap \sqrt{J}$. Well, if $a \in \sqrt{I \cap J}$ then $a^n \in I \cap J \implies a^n \in I, J \implies a \in \sqrt{I} \cap \sqrt{J}$. Now if $a \in \sqrt{I} \cap \sqrt{J}$, there's some n such that $a^n \in I, a^n \in J \implies a^n \in I \cap J$. So $a \in \sqrt{I+J}$.

Proof of (3): $I^n \subseteq I$, so we immediately have $\sqrt{I^n} \subseteq \sqrt{I}$. If $a \in \sqrt{I}$, then $a^k \in I$, then $a^{kn} \in I^n \implies a \in \sqrt{I^n}$.

Proof of (4): First we show $\sqrt{I+J} \supseteq \sqrt{I} + \sqrt{J}$. Let $a \in \sqrt{I} + \sqrt{J}$. We can write $a = b + c$, where $b \in \sqrt{I}, c \in \sqrt{J}$. Suppose $b^n \in I, c^m \in J$. Then $a^{n+m+1} = (b+c)^{n+m+1}$ by the binomial theorem, we see is in $I+J$. So $a \in \sqrt{I+J}$. Now we show $\sqrt{I+J} \subseteq \sqrt{I} + \sqrt{J}$. It follows then that $\sqrt{I+J} \subseteq \sqrt{\sqrt{I} + \sqrt{J}}$. On the other hand, suppose $a \in \sqrt{\sqrt{I} + \sqrt{J}}$. So $a^k \in \sqrt{I} + \sqrt{J}$ for some k. Then $a^k = i + j$. Suppose $i^n \in I, j^m \in J$. Then $(a^k)^{m+n+1} = (i+j)^{m+n+1} \in I + J$ by binomial theorem. So $\sqrt{I+J} \supseteq \sqrt{\sqrt{I} + \sqrt{J}}$. □

The main point of today will be to talk about Noetherian rings, introduced by Emmy Noether. She proved in many foundational things in commutative algebra, among other things. In commutative algebra, what's really important is the properties of rings. This is the game. Introduce as little axioms as possible, and get as far as you can.

Chapter 1.4 of Eisenbud and Chapter 6 of Atiyah-McDonald are good references.

Let R be a ring.

Definition 2.6 (Noetherian)**.** R is said to be a **Noetherian ring** if one of the following equivalent conditions hold:

(1) Every ideal of R is finitely generated
(2) R has the ascending chain condition (ACC). In other words, every sequence $I_1 \subseteq I_2 \subseteq \cdots$ of ideals is stationary. So there exist $n_0 \geq 1$ such that $\forall n \geq n_0$, $I_n = I_{n_0}$.
(3) Every non-empty set of ideals has a maximal element.

Proof. First prove (1) $\implies$ (2). Assume every ideal of R is finitely generated. Show R has ACC. Let $I_1 \subseteq I_2 \subseteq \cdots$ be an ascendhing chain of ideals. Let $I = \bigcup I_n$, which is an ideal. By assumption, it is finitely generated. Let $a_1, \cdots, a_k$ be a set of generators. Then there exists $N_0 \geq 1$ s.t. $a_1, \cdots, a_k \in I_{N_0}$. Then the chain stabilizes at (at least) N_0.

Now (2) $\implies$ (3). Let $\mathcal{C}$ be a non-empty set of ideals. Assume FSOC that $\mathcal{C}$ does not have a maximal element. Since $\mathcal{C}$ is nonempty, we can find $I_1 \in \mathcal{C}$. But I_1 is not maximal. So there exist $I_1 \subset I_2$. But I_2 is not maximal. So by induction, get a chain $I_1 \subset I_2 \subset I_3 \subset \cdots$, which cannot satisfy ACC. Contradiction.

Now (3) $\implies$ (1). Let I be an ideal of R. Pick some $a_1 \in I$. Then pick some $a_2 \in I \setminus \langle a_1 \rangle$. Then pick some $a_3 \in I \setminus \langle a_1, a_2 \rangle$. We can form ideals of the form $\langle a_1, \cdots a_i \rangle$, since I is not finitely generated. But if it is not finitely generated, we won't have a maximal element of our set of ideals. Contradiction. So the ideal is finitely generated. □

Using the fact that R is Noetherian, we find other rings to also be Noetherian.

Proposition 2.7. *If R is Noetherian, then R/I is also Noetherian.*

Proof. Let J be an ideal of R/I. By the correspondence, there's an ideal in R that surjects onto it. So this ideal of R is generated by some $\langle g_1, \cdots, g_n \rangle$. Then J is generated by $\pi(g_1), \cdots, \pi(g_n)$. Since every ideal of R/I is finitely generated, it is Noetherian. □

Theorem 2.8 (Hilbert's Basis Theorem)**.** *Let R be a Noetherian ring. Then $R[X]$ is also Noetherian.*

Proof. We'll try to prove that every ideal of $R[X]$ is finitely generated. Let $I \subseteq R[X]$ be an ideal. Assume that I is not finitely generated. So I is nonzero. Let f_1 be an element of $I - \{0\}$ that is a polynomial of minimal degree. Since $\langle f_1 \rangle \neq I$, since I is not finitely generated, there exist $f_2 \in I \setminus \langle f_1 \rangle$ also of minimal degree. So $\langle f_1, f_2 \rangle \neq I$. Repeating the same process, by induction, there is $\langle f_1, \cdots, f_n \rangle \subset I$ and $f_{n+1} \in I \setminus \langle f - 1, \cdots, f_n \rangle$ of minimal degree.

Then we have degree of $f_n \leq$ degree of f_{n+1}. Then write $f_n = a_n X^{s_n} + \sum_{i<s_n} c_i X^i$, where degree of $f_n = s_n$, and we see $s_n \leq s_{n+1}$. Then look at $J = \langle a_1, a_2, \cdots \rangle \subseteq R$. Because R is Noetherian, then J is finitely generated.

So there exist $m \geq 1$ such that $J = \langle a_1, \cdots, a_m \rangle$.

The claim is that $I = \langle f_1, \cdots, f_m \rangle$. Here's why. Pick a_{m+1}. We can write $a_{m+1} = \sum_{i=1}^m \alpha_i a_i$. So $f_{m+1} = a_{m+1} X^{s_{m+1}} +$ lower degree terms . Then $a_{m+1} X^{s_{m+1}} = \sum_i^n \alpha_i a_i X^{s_i} X^{s_{m+1} - s_i}$. But $a_i X^{s_i}$ is the leading term in f_i. BLAH BLAH. All of this is to say, is that we can reduce the degree of f_{m+1}. Namely, $f - \sum_{i=1}^m a_i X^{s_{m+1} - s_i} f_i = g \in I$, where the degree of $g < s_{m+1}$. If $f_{m+1} \notin \langle f_1, \cdots, f_m \rangle$, then $g \notin \langle f_1, \cdots, f_m \rangle$. But f_{m+1} had minimal degree of elements not in $\langle f_1, \cdots, f_m \rangle$, contradiction.

□

As an immediate corollary, if R is Noetherian, then $R[X_1, \cdots, X_n]$ is Noetherian.

We should mention another important algebraic structure. S is a **R-algebra** if it is a ring equipped with ring homomorphism $R \to S$. This ring homomorphism gives S a R-module structure. So an R-algebra is an R-module that's also a ring.

An R-Algebra S is of finite type if there exist $e_1, \cdots, e_n \in S$ such that every element of S can be expressed as a polynomial of $e_1, \cdots e_n$ with coefficients in R.

Proposition 2.9. *If R is Noetherian, then any finite-type R-algebra is Noetherian.*

Proof. Another way of saying an R-algebra S is of finite type, is that there is a surjective ring homomorphism $R[X_1, \cdots, X_n] \to S$. But then $S \cong R[X_1, \cdots, X_n]/I$ where I is the kernel of the map. But R Noetherian $\implies$ $R[X_1, \cdots, X_n]$ is Noetherian, and it remains Noetherian after modding out by I. So S is Noetherian. □

3. Sept 8: Noetherian modules, localization

Today we're going to talk about Noetherian modules.

Definition 3.1. Let R be a ring, and M an R-module. M is said to be Noetherian if it has the ascending chain condition (ACC) for R-submodules. Equivalently, if every R-submodule is finitely generated. Equivalently, if every non-empty set of R-modules has a maximal element.

Proof. The proof of this is analagous to the proof of the equivalency of conditions for rings to be Noetherian. □

So if we have a sequence of R-submodules

$$N_0 \subseteq N_1 \subseteq \cdots$$

the chain will eventually stabilize. So there exist N_0 such that for all $n \geq N_0$, $N_n = N_{n+1}$.

Suppose N, M, P are R-modules. Then an **exact sequence** of R-modules is

$$0 \to N \to^f M \to^g P \to 0$$

such that at each step, the kernel of the morphism is equal to the image of the previous morphism. This is equivalent to f injective, g surjective, and $Im(f) = Ker(g)$.

Proposition 3.2. *Let*

$$0 \to N \to^f M \to^g P \to 0$$

be a short exact sequence of R-modules. Then M is Noetherian $\iff$ both N, P are Noetherian.

Proof. Assume M is Noetherian. Want to show N, P are Noetherian. So any R-submodule of M is Noetherian. But f identifies any R-submodule of N with an R-submodule of M, because f is injective. So N is a Noetherian module.

Let $P' \subseteq P$ be a R-submodule. Then $g^{-1}(P')$ is a R-submodule. But M is Noetherian, so this is finitely generated. Then P' is finitely generated. This proves P is Noetherian.

Now assume that N, P are Noetherian. We'd like to show that M is Noetherian. Let $M' \subseteq M$ be a R-submodule. We have $M' \cap N$ is finitely generated, since N is Noetherian. Let $e_1, \cdots, e_k$ be a set of generators of $M' \cap N$. Furthermore, the image of M' in P is finitely generated, since P is Noetherian. Call the generators $a_1 = g(b_1), \cdots, a_r = g(b_r)$. We claim that $e_1, \cdots, e_k$ and $b_1, \cdots, b_r$ generate M'. Let $x \in M'$, look at $g(x)$. Can decompose it as $\sum_{i=1}^{r} \alpha_i g(b_i)$. So $x - \sum_{i=1}^{r} \alpha_i b_i \in Ker(g) \cap M' = N \cap M'$. So $x - \sum_{i=1}^{r} \alpha_i b_i = \sum_{i=1}^{k} \beta_i e_i$. This proves that M' is finitely generated.

□

Proposition 3.3. *If R is Noetherian, then any finitely generated R-module M is Noetherian.*

Proof. If M is finitely generated, we have $M = \langle e_1, \cdots, e_k \rangle$ for some e_i. There is also a surjection $R^k \to M$. Let N be the kernel. Then we have a short exact sequence $0 \to N \to R^n \to M \to 0$. By the previous proposition, it's enough to prove that R^k is Noetherian. This is true by the following lemma. □

Lemma 3.4. *If R is Noetherian, then R^k is also Noetherian for any k.*

Proof. Proceed by induction. We have short exact sequence

$$0 \to R \to R^{n+1} \to R^n \to 0$$

The projection is $(\alpha_1, \cdots, \alpha_{n+1}) \mapsto (\alpha_1, \cdots, \alpha_n)$. The claim follows immediately, since R and R^n are Noetherian. □

There's another very useful notion in commutative algebra called localization. The reference for this material is Chapter 2.1 in Eisenbud, and Chapter 3 in Atiyah-McDonald.

Definition 3.5. A ring R is local if it has a unique maximal ideal.

Let R be a ring. A subset $S \subseteq R$ is a **multiplicative subset** if the following holds: $1 \in S, 0 \notin S$, and $S * S \subseteq S$.

Example 3.6. If $a \in R$, $a \neq 0$ and not nilpotent, then $S = \{1, a, a^2, \cdots\}$ is a multiplicative subset.

Example 3.7. The invertible elements of R, denoted $R^\times$, is a multiplicative subset.

Example 3.8. If p is a prime ideal, then $S = R \setminus p$ is multiplicative subset.

Definition 3.9 (Localization of Ring)**.** Let R be a ring, $S \subseteq R$ a multiplicative subset. The localization of R along S is the set of equivalence classes $S^{-1}R = \{\frac{a}{s} | a \in R, s \in S\}/\sim$, where $\frac{a}{s} \sim \frac{a'}{s'} \iff$ there exists $t \in S$ such that $t(as' - a's) = 0$.

Can also denote localization of ring R by S as $R[S^{-1}]$.

Proposition 3.10. *$R[S^{-1}]$ is a ring with the following operations:*

$$\frac{a}{s} + \frac{a'}{s'} = \frac{as' + a's}{ss'}$$

and

$$\frac{a}{s}\frac{a'}{s'} = \frac{aa'}{ss'}$$

Proof. Also want to check the operations are well-defined. This is a pretty menial task. □

So $R[S^{-1}]$ is a commutative ring with unit.

We also have a canonical ring morphism $R \to R[S^{-1}]$, where $r \mapsto r/1$.

Lemma 3.11. *The canonical map $R \to R[S^{-1}]$ is injective $\iff$ S contains no zero divisors.*

Proof. Suppose $a \neq b$, but $a/1 \sim b/1$. Then there exist $s \in S$ such that $s(b-a) = 0$. But since S doesn't contain any zero divisors, we must have $b = a$.

Now suppose $R \to R[S^{-1}]$ is injective. Suppose s did contain a zero divisor $s \in S$. We'd get an immediate contradiction on the injectivity of $R \to R[S^{-1}]$. □

Proposition 3.12 (Properties of Localization)**.** *1. If $S = R^\times$, then $R[S^{-1}] = R$*

2. If R is an integral domain, then $R[S^{-1}]$ is also an integral domain.

3. If R is an integral domain, then $S = R \setminus \{0\}$ is a multiplicative subset and $R[S^{-1}]$ is called the field of fractions of R.

Definition 3.13. If $p \subset R$ is a prime ideal, the localization of R at p is denoted $R_p = R[S^{-1}]$ where $S = R \setminus p$.

We also have that:

Proposition 3.14. *R_p is a local ring, with unique maximal ideal pR_p.*

Proof. We claim that $\frac{x}{y} \in R_p$ is a unit $\iff$ $x \in R \setminus p$. Suppose $\frac{x}{y} \in R_p$ is a unit. Then $\frac{x}{y}\frac{a}{b} = \frac{xa}{yb} = 1$. Note $y, b \in R \setminus p$. We have there exist $t \in R \setminus p$ such that $t(xa - yb) = 0$. But $0 \in p$, so we must have $xa = yb \in R \setminus p$. Then $x, a \in R \setminus p$.

Now suppose $x \in R \setminus p$. Consider any $y \in R \setminus p$. Then $\frac{y}{x}$ is in R_p, and $(x/y)(y/x) = 1$.

Now, we know that there must exist a maximal ideal of R_p by Proposition 1.8. We claim that it is uniquely pR_p. Suppose we had an ideal $pR_p \subset I \neq R$. Then it would have to contain some element $\frac{x}{y}$ where $x \in R \setminus p$. Because if all the $\frac{x}{y} \in I$ had $x \in p$, then it would be a subset of pR_p. Then I would contain a unit. So we see R_p is maximal. Furthermore if there were some $I \not\subseteq R_p$, it would still need to contain an element $\frac{x}{y}$ with $x \in p$. Thus, R_p is local and pR_p is the unique maximal ideal. □

We had a correspondence between prime ideals of R/p and prime ideals of R containing p. But how do we get the prime ideals of R that are contained in p?

Proposition 3.15. *We have a bijective correspondence between: the prime ideals of R_p and the prime ideals of R contained in p.*

Proof. Let $\phi : R \to R_p$ denote the canonical map.

Let I be a prime ideal of R_p. Note we must have $I \subseteq pR_p$. Then let f be the map sending prime ideals of R_p to prime ideals of R containined in p. Then let $f(I) = \phi^{-1}(I)$. This is a prime ideal.

Now let g denote the map from prime ideals of R contained in p to prime ideals of R_p. Define $g(I) = \phi(I)R_p$. This is indeed an ideal of R_p. We show it's prime. Suppose $\frac{a}{a'}, \frac{b}{b'} \in R_p$ such that $\frac{a}{a'}\frac{b}{b'} \in \phi(I)R_p$. Then there exist some $s \in S$ such that $s(ab) \in I$. So $ab \in I$. So either $a \in I$ or $b \in I$. So either $\frac{a}{a'} \in g(I)$ or $\frac{b}{b'} \in g(I)$.

It's easy to see that $f \circ g = Id$, and $g \circ f = Id$. □

We also have a notion of localization of modules:

Definition 3.16. If M is an R-module, and $S \subseteq R$ is a multiplicative subset, then $M[S^{-1}] = \{\frac{m}{s} | m \in M, s \in S\}$, so that $\frac{m}{s} \sim \frac{m'}{s'}$ if there exist $t \in S$ such that $t(ms' - m's) = 0$.

4. Sept 13: associated primes to module

One of the fundamental properties of $\mathbb{Z}$ is that you can decompose any $a \in \mathbb{Z}$ into a product of primes, up to ±.

In any factorial ring, any a is a product of irreducible elements, in a unique way. What happens for general rings? This question was tackled while thinking about Fermat's equation $x^n + y^n = z^n$. You can factor $x^n + y^n = \prod x + e^{2\pi i/n} y$, so you can consider the equation as $\mathbb{Z}[e^{2\pi i/n}]$. This ring however, is not factorial. Too bad.

Some lessons to take a way. There was a shift in point of view to ideals. Namely that $(a) = \prod (p_i^{n_i})$. Every ideal in a Noetherian ring we can write as a product specific types of ideals.

Our first objective is to define the notion of associated primes. Let R be a ring, and M an R-module.

Let R be a ring, and M an R-module.

Definition 4.1. A prime ideal $I \subseteq R$ is associated to M if $I = Ann(m) = \{r \in R | rm = 0\}$.

Let $Ass(M)$ denote the set of prime ideals associated to M. In this section, our main theorem is the following:

Theorem 4.2. *Let R be a Noetherian ring, and M a finitely generated R-module. (Assume M is nonzero). Then:*

- *$Ass(M)$ is nonempty and finite. Each associated prime ideal contains $Ann(M) = \{r \in R | rm = 0, \forall m \in M\}$. It contains all primes minimal among those containing $Ann(M)$.*
- *$\bigcup_{p \in Ass(M)} p = \{0\} \cup$ zero divisors of M $= Z(M)$*

Before we prove this statement, we state an important lemma and corollary:

Lemma 4.3 (Prime Avoidance)**.** *Let R be a ring, and $J \subseteq R$ an ideal. Suppose we have $I_1, \cdots, I_n$ such that $J \subseteq \bigcup_{k=1}^n I_k$. Suppose I_k are prime for $k \geq 3$ or R contains an infinite field. Then $J \subseteq I_k$ for some k.*

Proof. First, suppose R contains an infinite field F. Then J is an F-vector space. We claim if $|F| > n-1$, then any F-vector space cannot be expressed as the union of n proper subspaces. We prove this via contrapositive. So we show that if F-vector space J is the union of n proper subspaces, then $|F| \leq n-1$. Let $J \subseteq \bigcup_{i=1}^n V_i$. Furthermore, suppose each V_i is not contained by the union of the others. So there exist $v \in V_j$ such that $v \notin \bigcup_{i \neq j} V_i$. Furthermore, there exist $u \notin V_j$. Consider $v + Fu$. Note we have $v + Fu \notin V_j$. Since otherwise, $u \in V_j$. Also, for each $i \neq j$, we see at most one of $v + Fu$ is in V_i. Since if there were more than one, then we'd be able to get $v \in \bigcup_{i \neq j} V_i$, contradiction. So we have $|v + Fu| = |F| \leq n - 1$.

The above immediately implies our statement if R contains an infinite field.

Now suppose I_k prime for $k \geq 3$. In the case of $n = 1$, we're done. Suppose $n = 2$. So $J \subseteq I_1 \cup I_2$, and suppose they don't contain one another. Then we have

$x_1, x_2 \in J$ such that $x_1 \notin I_1, x_2 \notin I_2$. But $x_1 + x_2 \in J$, but $x_1 + x_2 \notin I_1, I_2$. This leads to a contradiction. So we need $J \subseteq I_1$ or I_2.

Now suppose $n \geq 3$. Note we can assume that none of the I_k are contained in the other ideals. Then for every I_ℓ, there exist x_ℓ such that $x_\ell \in I_\ell, x_\ell \notin \bigcup_{k \neq \ell} I_k$. Consider the element $x_3 + \prod_{k \neq 3} x_k$. This element cannot be in I_3. Since otherwise, $\prod_{k \neq 3} x_k \in I_3$, but I_3 is prime so one of the $x_k \in I_3$ for $k \neq 3$, contradiction. Furthermore, $x_3 + \prod_{k \neq 3} x_k \notin X_\ell$ for any $\ell \neq 3$. Otherwise, $x_3 \in X_\ell$ for $\ell \neq 3$, contradiction. This leads us to our claim. □

As a corollary, we have:

Proposition 4.4. *Let R be a Noetherian ring and $I \subseteq R$ an ideal. Let M be a finitely-generated R-module. Then either I contains a nonzero element that is not a zero divisor, or it annihilates an element of M.*

Proof. If I doesn't contain any non zero-divisors, so it contains only zero divisors, then $I \subseteq Z(M) = \bigcup_{p \in Ass(M)} p$. Then by the above lemma, we must have $I \subseteq p = Ann(m)$ for some $m \in M$. □

We're now ready to proceed with the proof of Theorem 4.2.

Proof. First, we show that $Ass(M)$ is nonempty. Let $\mathcal{A} = \{Ann(m) | 0 \neq m \in M\}$. This set is nonempty. Since R is Noetherian there exists at least one maximal element of $\mathcal{A}$. We claim any maximal element of $\mathcal{A}$ is a prime ideal of R. Suppose $Ann(m)$ is maximal in $\mathcal{A}$. Then suppose $xy \in Ann(m)$. So $xym = 0$. Suppose $xm \neq 0$. Then $Ann(m) \subseteq Ann(xm)$. But by maximality, $Ann(m) = Ann(xm)$. Then $y \in Ann(m)$. This shows $Ann(m)$ is prime, so $Ass(M) \neq \emptyset$.

Now we show that $\bigcup_{p \in Ass(M)} p = Z(M)$. Clearly, we have $\bigcup_{p \in Ass(M)} p \subseteq Z(M)$. Now suppose $x \in Z(M)$. So $xm = 0$ for some nonzero $m \in M$. Let $\mathcal{A}_m == \{Ann(m') | Ann(m) \subseteq Ann(m')\}$. This set is nonempty. Since R is Noetherian, we have at least one maximal element. Same idea as previous paragraph; this maximal element is prime. So $x \in Ann(m) \subseteq Ann(m') \in Ass(M)$. So we're done.

Now we prove that $Ass(M)$ is finite. First we prove the following two lemmas:

Lemma 4.5. *Let R be a Noetherian ring and M a finitely generated R-module. There exist filtration*

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

such that $M_i/M_{i-1} \cong R/p_i$ for prime ideal $p_i \subseteq R$.

Proof. Since R Noetherian + M finitely generated R-module, we know that $Ass(M)$ is nonempty. So there exist prime $p = Ann(m)$ for $m \in M$. Let $M_1 = \langle m \rangle$. Note $0 \to Ann(m) \to R \to M_1 \to 0$, where $R \to M_1$ maps $x \mapsto xm$. So $M_1 \cong R/p$. If $M_1 = M$, we're done. Otherwise, since M/M_1 is also finitely generated, we have $Ass(M/M_1)$ is nonempty, so there exist $p_2 = Ann([m_2])$, where $[m_2] \in M/M_1$ and $m_2 \in M$. We have $0 \to Ann([m_2]) \to R \to M_2/M_1 \to 0$. So $M_2/M_1 \cong p_2$. We can continue to build this chain $0 \to M_1 \subseteq M_2 \subseteq \cdots$. But since M is a Noetherian module, this chain must stabilize. □

Lemma 4.6. *Suppose $0 \to M' \to M \to^{\pi} M^{''} \to 0$ is an exact sequence of R-modules. Then $Ass(M) \subseteq Ass(M') \cup Ass(M^{''})$.*

Proof. Suppose $p \in Ass(M)$. So $p = Ann(m)$ for some $m \in M$. If $\pi(m) = 0$, then $m \in Ker(\pi)$, so $m \in M' \implies p \in Ass(M')$. If $\pi(m) \neq 0$, then $p \subseteq Ann(\pi(m))$. Let $t \in Ann(\pi(m))$. So $t\pi(m) = \pi(tm) = 0$. We see $p \subseteq Ann(tm)$. If $\mu \in Ann(tm)$, $\mu t \in Ann(m)$. So either $\mu \in Ann(m)$ or $t \in Ann(m)$. The former implies $Ann(m) = Ann(tm) \implies Ann(m) \in Ass(M')$, since $tm \in Ker(\pi) = M'$. The latter implies $Ann(m) = Ann(\pi(m)) \in Ass(M^{''})$. □

We're now ready to prove finiteness. We have that our R-module M filters as above. Then we have exact sequence

$$0 \to M_{n-1} \to M \to M/M_{n-1} \to 0$$

So $Ass(M) \subseteq Ass(M_{n-1}) \cup Ass(M/M_{n-1})$. Then note that

$$0 \to M_{i-1} \to M_i \to M_i/M_{i-1} \to 0$$

implies that $Ass(M_i) \subseteq Ass(M_{i-1}) \cup Ass(M_i/M_{i-1})$. Thus, we have $Ass(M) \subseteq \bigcup_{i=1}^{n} Ass(R/p_i)$.

But in fact, for prime p, $Ass(R/p) = \{p\}$. Because if a prime ideal $I \subseteq R$ was such that $I = Ann(m)$ for $m \in R/p$, we'd have $\forall r \in I$, $rm = 0 \implies r \in p$.

So $Ass(M) \subseteq \{p_1, \cdots, p_n\}$. So $Ass(M)$ is finite.

Finally:

Let p be a prime minimal over $Ann(M)$. We localize at p. So $S = R \setminus p$ is our multiplicative subset. So look at $R_p = R[S^{-1}]$ and $M_p = M[S^{-1}]$. So M_p is a R_p-module. On PSET2, we'll see that $Ass_{R_p}(M_p) = \{qR_p | q \in Ass(M), q \subseteq p\}$.

In fact, pR_p is the only prime containing $Ann(M_p)$ by minimality. And the set $Ass(M_p) \neq \emptyset$. Have to check that $M_p \neq 0$.

Note pR_P is maximal ideal of R_p. So $pR_p \in Ass(M_p)$, which implies $p \in Ass(M)$. □

5. Sept 15: p-rimary submodules, support

Last time we defined the associated primes to an R-module M. The goal is to find a decomposition of modules into ideals, similar to decomposition of integers into prime numbers.

We'll now introduce the support of a module.

Definition 5.1. Let M be a R-module. Then the support of M is the set of primes p such that $M_p \neq 0$.

Example 5.2. Take $M = \mathbb{Z}/p\mathbb{Z}$. Take $R = \mathbb{Z}$. Then $M_q = 0$ for any prime $q \neq p$. So $p \in \mathbb{Z} \setminus (q)$, so we are inverting p. But p is also zero, so we must have $M_q = 0$.

At least in this section, we won't be using the support of a module very often. But it's a useful notion, because under nice conditions of our ring and our modules:

Lemma 5.3 (PSET 2 Question 1.6)**.** *Suppose R is Noetherian and M is finitely generated R-module. Then $Supp(M) = V(Ann(M))$.*

Note that if $I \subseteq R$ is an ideal, then $V(I) := \{p | I \subseteq p,\ p \text{ is prime}\}$.

So in practice, when we're working with nice rings and modules, we'll appeal to the support to say something about primes containing $Ann(M)$.

Here is a very useful proposition:

Proposition 5.4.

- $Ass(M) \subseteq Supp(M)$

- *If R is Noetherian, M f.g. R-module, then the set of minimal elements of $Ass(M)$ and $Supp(M)$ coincide.*

Proof. We prove the first statement. Let $p \in Ass(M)$. Then $p = Ann(x)$ for some nonzero $x \in M$. We'd like to $M_p \neq 0$. It suffices to show that $x \in M_p$ is nonzero. Suppose it were zero. Then there would exist $t \in R \setminus p$ such that $tx = 0$. But then $t \in Ann(x) \implies t \in p$, contradiction. So $M_p \neq 0$, and $Ass(M) \subseteq Supp(M)$.

We prove the second statement. By assumption, R is Noetherian and M is f.g. R-module. By lemma 5.3, $Supp(M) = V(Ann(M))$. The set of minimal elements of $Supp(M)$ is the set of all primes minimal among those containing $Ann(M)$. But by Theorem 4.2, the primes minimal among those containing $Ann(M)$ are in $Ass(M)$. Thus, we must have the set of minimal elements of $Ass(M)$ and $Supp(M)$ coincide. □

Definition 5.5. The minimal primes in $Ass(M)$ are called the **isolated primes**. The non-minimal ones are called the **embedded primes**.

Example 5.6. Suppose R Noetherian, $M = R/I$ is finitely generated R-module. Then $Supp(R/I) = V(Ann(R/I))$, and $Ann(R/I) = I$. (If $r \in Ann(R/I)$, then $r * 1 \in I$). So the isolated associated primes of R/I are primes minimal over I.

We arrive to a very important (for reasons we'll see later on) definition:

Definition 5.7 (Primary Submodule)**.** We say $N \subseteq M$ is a **primary submodule** of M if $Ass(M/N)$ consists of exactly one element p. We say then that N is p-primary.

Example 5.8. $Ass(R/p) = \{p\}$. If $I \subseteq R$ is an associated prime of R/p, then $I = Ann(x)$ for some nonzero $x \in R/p$. Then $rx \in p$ for every $r \in I$. This implies $r \in p$. So $I \subseteq p$. But $I \supseteq Ann(R/p) = p$. So we conclude that $p \subseteq R$ is p-primary.

When working with nice rings and modules, if we have a p-primary submodule but don't know what either $\sqrt{Ann(M/N)}$ or p looks like, we can appeal to:

Lemma 5.9. *Assume R is Noetherian, and M f.g R-module. If N is p-primary, then $p = \sqrt{Ann(M/N)}$.*

Proof. Since N is p-primary, we have $Ass(M/N) = \{p\}$. By Theorem 2.4, $\sqrt{Ann(M/N)} = \bigcap_{p \supseteq Ann(M/N)} p = \bigcap_{\text{minimal } p \supseteq Ann(M/N)} p$. But since R is Noetherian and M f.g. R-module, by Proposition 5.4, the set of minimal elements of $Ass(M/N)$ and the set of primes minimal among those containing $Ann(M/N)$ coincide. Namely, it's just p. So $\sqrt{Ann(M/N)} = p$. □

How can we identify when a submodule is p-primary? Under nice rings and modules, we have some equivalent conditions we can check:

Proposition 5.10. *Let R be Noetherian and M a finitely generated R-module. Let $N \subseteq M$ be a sub-module. The following are equivalent:*

- *N is primary.*
- *For every $a \in R$: if there exist $m \in M$, $m \notin N$, but $am \in N$, then there exists $k \geq 1$ s.t. $a^k M \subseteq N$.*
- *$Z(M/N) = \sqrt{Ann(M/N)}$.*

Proof. First we show that (2) $\implies$ (3). Let $a \in Z(M/N)$. So $am \in N$, but $m \notin N$. Then by assumption of (2), there exist k such that $a^k M \subseteq N$. Then $a^k \in Ann(M/N) \implies a \in \sqrt{Ann(M/N)}$. So $Z(M/N) \subseteq \sqrt{Ann(M/N)}$. To see the reverse, suppose $a \in \sqrt{Ann(M/N)}$. So $a^k \in Ann(M/N)$ for some k. Assume also $M/N \neq 0$ (otherwise we'd be done). So there exist nonzero $m \in M/N$. Then there is some least i such that $a^i m = 0$. Then $a^{i-1}m \neq 0$. So $a(a^{i-1}m) = 0 \implies a \in Z(M/N)$.

Now we show (3) $\implies$ (1). Note since R Noetherian, $Ass(M/N)$ is nonempty, and $Z(M/N) = \bigcup_{p \in Ass(M/N)} p$. If this is unclear, see proof of Theorem 4.2. Then we have $\sqrt{Ann(M/N)} = \bigcup_{p \in Ass(M/N)} p$. But $\sqrt{Ann(M/N)} = \bigcap_{p \supseteq Ann(M/N)} p$. Let $p \in Ass(M/N)$ be minimal. Then $\bigcap_{p \supseteq Ann(M/N)} p \subseteq p \subseteq \bigcup_{p \in Ass(M/N)} p$. But we have an equality. So $\bigcup_{p \in Ass(M/N)} p = p$, and by minimality of p, we must have $Ass(M/N) = \{p\}$. So N is p-primary.

Now we show (1) $\implies$ (2). By assumption, $Ass(M/N) = \{p\}$. Then since R Noetherian, M f.g. R-module, by the previous lemma we have $p = \sqrt{Ann(M/N)}$. Furthermore, $Z(M/N) = p$. So $Z(M/N) = \sqrt{Ann(M/N)}$. So for $a \in R$, if there exist $m \in M, m \notin N$ such that $am \in N$, then $a \in Z(M/N) \implies a \in \sqrt{Ann(M/N)}$. So there exist k such that $a^k \in Ann(M/N) \implies a^k M \subseteq N$. □

Example 5.11. Suppose R Noetherian. Clearly R/I is finitely generated R-module. We have $I \subseteq R$ is p-primary $\iff Ass(R/I) = \{p\} \iff$ for every $a, b \in R$ we have $ab \in I \implies a \in I$ or $b \in \sqrt{I}$ (because $p = \sqrt{Ann(R/I)} = \sqrt{I}$) $\iff$ every zero divisor in R/I is nilpotent.

Example 5.12. In $\mathbb{Z}$, primary ideals are (0) and (p^n).

A prime ideal is a primary ideal. And $\sqrt{I}$ is a prime ideal. None of the reverse implications are true in general.

Lemma 5.13. *Let $I \subseteq R$ be any ideal, and $m \subseteq R$ a maximal ideal. Suppose $\sqrt{I} = m$. Then I is m-primary.*

Proof. We have $\sqrt{I} = \bigcap_{I \subseteq p} p = m$. So any prime containing I contains m. This means the only prime ideal containing I is m. Note $Ann(R/I) = I$. We have $Ass(R/I) \subseteq V(Ann(R/I)) = V(I) = m$. So we must have $Ass(R/I) = \{m\}$. OOPS, I THINK THIS IS ACTUALLY NOT CORRECT. IM ASSUMING R NOETHERIAN HERE. □

A property p-primary submodules enjoy is that they're closed under finite intersection.

Lemma 5.14. *If p is prime, $N_1, \cdots, N_k \subseteq M$ are p-primary, then $N_1 \cap \cdots \cap N_k$ is also p-primary.*

Proof. We have $Ass(M/N_i) = \{p\}$. We prove this by induction on k. $k = 1$ is fine. Now assume it's true for k. Show $k+1$. We have a short exact sequence

$$0 \to N_1 \cap \cdots \cap N_k / N_1 \cap \cdots \cap N_{k+1} \to M/N_1 \cap \cdots \cap N_{k+1} \to M/N_1 \cap \cdots \cap N_k \to 0$$

So $Ass(M/N_1 \cap \cdots \cap N_{k+1}) \subseteq Ass(M/N_1 \cap \cdots \cap N_k) \cup Ass(N_1 \cap \cdots \cap N_k/N_1 \cap \cdots \cap N_{k+1})$. The first is $\{p\}$ by induction. So just need to show that $Ass(N_1 \cap \cdots \cap N_k/N_1 \cap \cdots \cap N_{k+1}) = \{p\}$ or $\emptyset$.

Look at $N_1 \cap \cdots \cap N_k \to M/N_{k+1}$.

$$\begin{tikzcd}
N_1 \cap \cdots \cap N_k \arrow[rr] \arrow[dr] & & M/N_{k+1} \\
& \frac{N_1\cap\cdots\cap N_k}{N_1\cap\cdots\cap N_{k+1}} \arrow[ur, "g"'] &
\end{tikzcd}$$

but g is injective. Because it is injective, any associated prime of $\frac{N_1\cap\cdots\cap N_k}{N_1\cap\cdots\cap N_{k+1}}$ is an associated prime of $\frac{M}{N_{k+1}}$. So $Ass(\frac{N_1\cap\cdots\cap N_k}{N_1\cap\cdots\cap N_{k+1}})$ is either $\emptyset$ or $\{p\}$.

□

6. Sept 20: primary decomposition existence

Last time we defined the notion of a primary submodule, and if you take a finite intersection of p-primary submodules, then the finite intersection is also p-primary.

Today, we'll finally talk about primary decomposition.

Definition 6.1 (Primary Decomposition)**.** Let M be an R-module, and N a submodule. Then a **primary decomposition** of N is an expression

$$N = N_1 \cap \cdots \cap N_i$$

where N_i is a primary submodule and $Ass(M/N_i) = \{p_i\}$.

The decomposition is reduced if all the p_i are distinct. So $p_i \neq p_j$ for $i \neq j$ and N is not the intersection of a proper subset of the N_i's.

Starting from any primary decomposition, one can get a reduced one.

First, discard all the redundant N_i's.

Then, if some of the p_i are equal to p, then you can just replace them by their intersection.

Example 6.2. In PSET 2, if you had a finitely generated abelian group M, which is a finitely generated Z-module, we found the associated primes of M. Namely, if $M = \mathbb{Z}^r \oplus \bigoplus \mathbb{Z}/p_i^{n_i}$.

Definition 6.3. A submodule $N \subsetneq M$ is called **irreducible** if it cannot be written as

$$N = N_1 \cap N_2$$

where N_1, N_2 are submodules of M that are not equal to N.

Example 6.4. If $M = \mathbb{Z}, R = \mathbb{Z}$, the irreducibles submodules of M are $I = (p^n)$. Meanwhile, an ideal of the form $(p^n q^m) = (p^n) \cap (q^m)$.

Lemma 6.5. *Let R be Noetherian ring, and M f.g. R-module. Then any irreducible submodule N of M is primary.*

Proof. Suppose N is irreducible. Assume FSOC that N is not primary, then there exist two prime ideals $p_1, p_2 \in Ass(M/N)$ s.t. $p_1 \neq p_2$. Then $p_1 = Ann([x_1]), 0 \neq [x_1] \in M/N, x_1 \in M$. Same with $p_2 = Ann([x_2])$. This means that $x_1, x_2 \notin N$. So N is strictly contained in (N, x_1), and N is strictly contained in (N, x_2). Then $N \subseteq (N, x_1) \cap (N, x_2)$. Let's show this is an equality. If $z \in (N, x_1) \cap (N, x_2)$, then in M/N, $[z] = \alpha[x_1] = \beta[x_2]$ for some $\alpha, \beta \in R$. WLOG suppose p_1 not contained in p_2. Let $t \in p_1, t \notin p_2$. Then $t[z] = t\alpha[x_1] = \alpha t[x_1] = 0$, and $0 = t[z] = t\beta[x_2]$, so $t\beta \in Ann[x_2] = p_2$. But $t \notin p_2 \implies \beta \in p_2$. So $[z] = \beta[x_2] = 0$, which implies $z \in N$. So $N = (N, x_1) \cap (N, x_2)$. Then N is not irreducible, contradiction. So we must have that N is primary. □

Theorem 6.6 (existence of primary decomposition)**.** *Let R be Noetherian, M f.g. R-module. Then every proper submodule of M has a primary decomposition.*

Proof. Let

$$\mathcal{C} = \{N \neq M | N \text{ can be written as a finite intersection of irreducible submodules.}$$

Assume FSOC that $\mathcal{C}$ is nonempty. Since M is Noetherian module, it has at least one maximal element, call it N. Since $N \in \mathcal{C}$, this implies N itself cannot be an irreducible submodule. So it can be written as $N = N_1 \cap N_2$, where $N \neq N_1, N_2$. By maximality, $N_1, N_2 \notin \mathcal{C}$. This implies they can be written as the finite intersection of irreducible elements. Then N can be as well, contradiction. So $\mathcal{C}$ is empty, and every proper submodule is the finite intersection of irreducible submodules. But by our given and the previous lemma, this means every proper submodule admits a primary decomposition. □

Example 6.7. Let $R = \mathbb{Z}$, pick any ideal $I = (a)$. The associated primes are $p \setminus a$. Can write $I = (p_1^{n_1}) \cap \cdots \cap (p_k^{n_k})$, where $a = \prod p_i^{n_i}$.

Example 6.8. Consider $I = (x^2, xy) \subseteq k[X, Y]$. Look at $\{(x, y) \in k^2 | x^2 = 0, xy = 0\}$. The set where $xy = 0$ is the coordinate axis, and $x^2 = 0$ is just the x-axis. But if you just look at the picture, you lose the x^2. But if you remember the ideal, you remember the x^2.

$\sqrt{I} = (x)$ but $(x^2) \subsetneq I \subseteq (x)$. Moreover, I is not (x)-primary, because $xy \in I$ but $x \notin I$, $y \notin \sqrt{I}$. Can write $I = (x) \cap (x, y)^2$. The radical of $(x, y)^2$ is (x, y), which is maximal. Then we know $(x, y)^2$ is (x, y)-primary. And (x) is (x)-primary.

Geometrically, what you're obtaining. The vanishing set of (x) is

Example 6.9. Let $\mathbb{Z}[i]$ be the gaussian integers $= \{a + ib, a, b \in \mathbb{Z}, i^2 = -1\}$. We have an extension $\mathbb{Z} \to \mathbb{Z}[i]$. Any prime number $p \in Z$, what is the primary decomposition of $I = (p)$ in $\mathbb{Z}[i]$. If $p \cong 1 \mod 4$, then p is the sum of two squares $p = a^2 + b^2 = (a + ib)(a - ib)$. So $p = (p, a - ib) \cap (p, a + ib)$. If $p \cong 3 \mod 4$, then $I = (p)$ is prime. If $p \cong 2 \mod 4$. Then $(2) = (1 + i)^2$.

7. Sept 22: primary decomposition uniqueness theorems, hom and tensor

Last time we showed the existence of primary decomposition for nice enough rings and modules. Now we'll establish some nice uniqueness statements.

Theorem 7.1 (First uniqueness theorem)**.** *Let R be Noetherian and M f.g. R-module. Suppose $N \neq M$ has reduced primary decomposition $N = N_1 \cap \cdots \cap N_r$, where N_i is p_i-primary. Then $Ass(M/N) = \{p_1, \cdots, p_r\}$.*

Proof. WLOG we can assume $N = 0$. This is because if we prove it for the case $N = 0$, if we have the original statement, we can replace M with M/N. The images of N_i in M/N will still be p_i-primary modules.

First we show $Ass(M/N) \subseteq \{p_1, \cdots, p_r\}$. Note we have the SES

$$0 \to N_1 \to M \to M/N_1 \to 0$$

which implies $Ass(M) \subseteq \{p_1\} \cup Ass(N_1)$ by lemma 4.6. Then consider the SES

$$0 \to N_1 \cap N_2 \to N_1 \to N_1/N_1 \cap N_2 \to 0.$$

Note $N_1/N_1 \cap N_2$ injects into M/N_2, so $Ass(N_1/N_1 \cap N_2) \subseteq \{p_2\}$. Continuing in this fashion, we obtain the claim.

Now we show $Ass(M/N) \supseteq \{p_1, \cdots, p_r\}$. WLOG, we show $p_1 \in Ass(M/N)$. Since the primary decomposition is reduced, $N_2 \cap \cdots \cap N_r \neq 0$. Then there exists nonzero $x \in N_2 \cap \cdots \cap N_r$ such that $x \notin N_1$. Since N_1 is primary, R Noetherian, M f.g. R-module, we have by lemma 5.9, $p_1 = \sqrt{Ann(M/N_1)}$. Since R Noetherian, there exist k s.t. $p_1^k \in Ann(M/N_1)$. Choose minimal k s.t. $p_1^k x \in N_1$, so $p_1^{k-1}x \notin N_1$. Then there is $t \in p_1^{k-1}$ s.t. $tx \notin N_1$.

Consider $Ann(tx)$. Note $p_1 tx \in N_1$, so $p_1 tx \in N_1 \cap N_2 \cap \cdots \cap N_r = 0$. So $p_1 \subseteq Ann(tx)$. But if $z \in Ann(tx)$, $ztx = 0 \in N_1 \cap N_2 \cap \cdots \cap N_r$, but $tx \notin N_1$. Since N_1 is primary, by Proposition 5.10, $z \in \sqrt{Ann(M/N_1)} = p_1$. Thus, $p_1 = Ann(tx) \implies p_1 \in Ass(M)$.

□

Now proof of the second uniqueness theorem.

Theorem 7.2 (Second uniqueness theorem). *Let R be Noetherian ring, and M f.g. R-module. Suppose $N \neq M$, and $N = N_1 \cap \cdots \cap N_k$ a reduced primary decomposition, with N_i being p_i-primary.*

If p_i is minimal in the set $Ass(M/N)$, then N_i is uniquely determined by N (in any primary decomposition of N, the N_i must appear).

Proof. WLOG we can assume that $N = 0$. Let N_i be a module with minimal p_i.

Note that

$$\psi : M \to M/N_i \to (M/N_i)_{p_i}$$

can be factored through $M \to M_{p_i} \to (M/N_i)_{p_i}$, where $m/s \in M_{p_i} \mapsto \psi(m)/s \in (M/N_i)_{p_i}$. Note that $M_{p_i} \to (M/N_i)_{p_i}$ is surjective, and the kernel is N_{p_i}, so it factors through $M_{p_i} \to M_{p_i}/N_{p_i} \cong (M/N_i)_{p_i}$. In other words, the diagram

$$\begin{tikzcd}
M \arrow[r] \arrow[dr] & M/N_i \arrow[r] & (M/N_i)_{p_i} \\
 & M_{p_i} \arrow[ur] \arrow[r] & M_{p_i}/N_{p_i} \arrow[u, "\cong"]
\end{tikzcd}$$

commutes. We can simplify our findings with this square:

$$\begin{tikzcd}
M \arrow[r, "\alpha"'] \arrow[d, "\iota"'] & M_{p_i} \arrow[d, "b"'] \\
M/N_i \arrow[r, "j"] & (\frac{M}{N_i})_{p_i} \cong \frac{M_{p_i}}{N_{p_i}}
\end{tikzcd}$$

We claim that j is injective. Suppose $[x] \in M/N_i$ is mapped to zero. Then there exist $t \in R \setminus p_i$ s.t. $tx \in N_i$. Then since N_i is p_i-primary module, by proposition 5.10, we have $Z(M/N_i) = \sqrt{Ann(M/N_i)} = p_i$. Since $t \notin p_i$, we must have $x \in N_i$, so $[x] = 0$.

We also claim that $b : M_{p_i} \to M_{p_i}/N_{p_i}$ is injective. Note $M \to \oplus M/N_i$ is injective since the kernel is $\cap N_i = 0$. Then $M_{p_i} \to \oplus(M/N_i)_{p_i}$ is injective as well. But in fact, $(M/N_j)_{p_i} = 0$ for $i \neq j$. To see why, note p_i is minimal, and $p_i \neq p_j$, so $p_j \not\subseteq p_i$. Then there exist $t \in p_j, t \notin p_i$. Then t is invertible in R_{p_i}. Furthermore, $t \in p_i \implies t \in \sqrt{Ann(M/N_j)} = p_j$. So there exist k s.t. $t^k(M/N_j) = 0$, which implies $t^k(M/N_j)_{p_i} = 0$. But t is invertible, so $(M/N_j)_{p_i} = 0$.

Together, these facts show $\ker M \to M_{p_i} = N_i$.

□

Thats the end of our discussion of primary decomposition.

We will now talk about Hom and tensor products. This is chapter 2 in Atiyah Macdonald, or 2.2 in Eisenbud.

Let M, N be two R-modules. Then

$$Hom_R(M,N) := \{ \text{ morphisms of } R\text{-modules } f : M \to N\}$$

The object $Hom_R(M,N)$ itself is an R-module.

Proposition 7.3. *Some properties:*

- $Hom_R(\oplus M_i, N) = \prod Hom_R(M_i, N)$
- $Hom_R(M, \prod N_j) = \prod_j Hom(M, N_j)$
- $Hom_R(R,N) = N$*, where* $\phi \mapsto \phi(1)$.
- *The functor* $Hom_R(M,-) : Mod_R \to Mod_R$ *is left-exact. If* $0 \to N \to P \to U$ *is exact, then* $0 \to Hom(M,N) \to Hom(M,P) \to Hom(M,U)$ *is exact.*

  The functor $Hom_R(-,M)$ *is right-exact. So if* $C \to B \to A \to 0$ *is exact, then* $0 \to Hom(A,N) \to Hom(B,N) \to Hom(C,N)$ *is exact.*
- *There is a natural isomorphism* $Hom_R(M \otimes N, C) \cong Hom_R(M, Hom(N,C))$.
- $(\oplus M_i) \otimes_R N \cong \oplus(M_i \otimes N)$
- $M \otimes_R R \cong M$
- *Tensor product is right exact. So if* $A \to B \to C \to 0$ *is exact, then* $A \otimes_R M \to B \otimes_R M \to C \otimes_R M \to 0$ *is exact.*

Proposition 7.4 (base change)**.** *If M is R-module, $R \to S$ ring homomorphism (which makes S an R-algebra) then $M \otimes_R S$ is a S-module.*

Proposition 7.5. *$S \subseteq R$ multiplicative subset, M R-module, then $M \otimes_R R[S^{-1}] \cong M[S^{-1}]$ and if $I \subseteq R$ is an ideal then $M \otimes_R R/I \cong M/IM$.*

Proof. We have a bilinear map $R[S^{-1}] \times M \to M[S^{-1}]$, where $(\frac{a}{s}, m) \mapsto \frac{ma}{s}$. So we get a map $R[S^{-1}] \otimes_R M \to M[S^{-1}]$. Other direction, $M[S^{-1}] \to R[S^{-1}] \otimes_R M$. Map $m/s \mapsto \frac{1}{s} \otimes m$. Have to check well-defined. These compose in both directions to give identities. So we have isomorphism.

□

Definition 7.6. Let R be a ring. Spec$R$:= { prime ideals of R }. If $i \subseteq R$, then $V(I) \subseteq Spec(R)$, where $V(I) = \{$ p prime and $I \subseteq p\}$.

8. Sept 27: spectrum, zariski topology

We're going to start by talking about the spectrum of a ring. Some motivation for this object:

If X is a compact "nice" topological space, say $(0,1)$. If you look at the ring R of continuous functions on X, a classical theorem from functional analysis is that if X is nice enough, there is a correspondence between the maximal ideals of R and the points on X.

So the idea is that if you have a ring R, you'd like to see it as a ring of functions on some topological space.

Definition 8.1. Let R be a ring. Then the spectrum of R is the set of all prime ideals.

Example 8.2. If $R = k$ is a field. Then $Spec(R) = \{(0)\}$.
If $R = \mathbb{Z}$, then $Spec(\mathbb{Z}) = \{(0)\} \cup \{(p)|$ prime p $\}$.

Now we'll make $Spec(R)$ a topological space by declaring $V(I) = \{p \in Spec(R) | I \subseteq p\}$ to be closed, for any ideal $I \subseteq R$. (In other words, take the coarsest topology such that the $V(I)$ is closed.

To see that this indeed generates a topology, one can verify that:

$$\cap V(I_\alpha) = V(\sum I_\alpha)$$

and

$$\bigcup_{finite} V(I_\alpha) = V(\cap_{finite} I_\alpha).$$

This is called the **Zariski topology**. We leave verification that it is a topology to the reader.

Example 8.3. What are the closed subsets in $Spec(\mathbb{Z})$? You take any ideal $I = (\alpha) = (p_1^{n_1} \cdots p_r^{n_r})$. Then $V(I) = \{p_1, \cdots, p_r\}$.

What about $\mathbb{A}^1_{\mathbb{C}} = Spec\mathbb{C}[X]$? One can show by division algorithm or weak nullstellensatz that $Spec(\mathbb{C}[X]) = \{0\} \cup \{X - \alpha | \alpha \in \mathbb{C}\} = \{(0)\} \cup \mathbb{C}$.

If $S \subseteq Spec(R)$, we denote $I(S) = \bigcap_{p \in S} p$. This is a radical ideal of R.

Lemma 8.4. *Let $S \subseteq Spec(R)$.*

- $V(I(S)) = \overline{S}$.
- $I(V(J)) = \sqrt{J}$

Proof. For any $p \in S$, we have $I(S) = \bigcap_{p \in S} p \subseteq p$. So $p \in V(I(S))$. So $S \subseteq V(I(S))$. Then $\overline{S} \subseteq V(I(S))$.

Now suppose $\overline{S} = V(J)$. Then for every $p \in S$, $J \subseteq p$ which implies $J \subseteq \bigcap_{p \in S} p = I(S)$. Then $V(J) = \overline{S} \supseteq V(I(S))$. So we have $V(I(S)) = \overline{S}$.

The second statement is a restatement of what we already know. □

As a corollary:

Proposition 8.5. *We have an inclusion-reserving bijection between radical ideals of R, and closed subsets of $Spec(R)$.*

The bijection maps radical ideal $I \mapsto V(I)$, and maps closed subset $J \mapsto I(J)$.

In particular, $\overline{[p]} = V(p) = \{q | p \subseteq q\}$. Note a point $[p] \in Spec(R)$ is closed $\iff$ $p \subseteq R$ is a maximal ideal.

If R is integral, then $\overline{\{0\}} = Spec(R)$. So (0) is a dense point in $Spec(R)$.

If you look at $\mathbb{C}[X_1, \cdots, X_n]$ and look at $\mathbb{A}^n_{\mathbb{C}} := Spec(\mathbb{C}[X_1, \cdots, X_n])$, Hilbert's Nustellensatz tells you that the maximal ideals of $\mathbb{A}^n_{\mathbb{C}}$ are exactly those of the form $(X_1 - \alpha_1, \cdots, X_n - \alpha_n)$ for $\alpha_i \in \mathbb{C}$.

So we have our set $Spec(R)$ and have endowed it with the Zariski topology. Let's talk about some topological properties that we may observe. We'll begin with irreducibility.

Definition 8.6. A topological space is irreducible if it not empty and not a union of two strict closed subsets.

Proposition 8.7. *Let $X \neq \emptyset$ be a topological space. TFAE:*

- *X is irreducible*
- *Every finite intersection of nonempty open subsets is non-empty*
- *Every nonempty open subset is dense.*

Proof. Let's show (1) $\implies$ (2). Take $U_1, U_2 \subseteq X$ open, non-empty. Then take their complements F_1, F_2. We have $F_1 \cap F_2 \neq X$, where $F_1, F_2 \neq X$. So $U_1 \cap U_2$ is nonempty. The general statement then follows from this.

Let's show (2) $\implies$ (3). This immediately holds.

Show (3) $\implies$ (1). Well, assume FSOC that X could be written as the union of two proper closed subsets. Then their complements are opens that do not intersect. Contradiction. □

Here are a few exercises to jog your brain:

Proposition 8.8. *Let $Y \subseteq X$. Then Y endowed with the subspace topology is irreducible $\iff \overline{Y}$ is irreducible.*

Proposition 8.9. *If $f : X \to Y$ is continuous, then X irreducible $\implies f(X)$ is irreducible.*

An irreducible maximal subset (w.r.t inclusion) in X is called an **irreducible component.** An irreducible maximal subset is automatically closed since its closure is irreducible, but it is maximal, so it equals its closure.

By Zorn's lemma, every point is contained in an irreducible component. This tells you that X is union of its irreducible components.

Example 8.10. If $X = Spec(R)$: if X has a dense point, then X is irreducible. In fact, if R is an integral domain, then (0) is dense in $Spec(R)$, so $Spec(R)$ is irreducible.

Proposition 8.11. *Let R be a ring. We have a bijection between the set of primes of R and the set of irreducible subsets of $Spec(R)$.*

Proof. Take the prime p, note R/p is integral domain. There's a continuous inclusion $Spec(R/p) \to Spec(R)$, induced by $R \to R/p$. Since $Spec(R/p)$ is irreducible, it's image in $Spec(R)$ is irreducible. The image is exactly $V(p)$.

Now let $V(I) \subseteq Spec(R)$ be irreducible. We can assume I is radical. Send it to $I \subseteq R$. Prove I is prime. Let $fg \in I$, st. $f, g\ /inI$. Claim that $V((I, f)) \cup V((I, g)) = V(I)$. If $p \in V((I, f)) \cup V((I, g))$, then clearly $p \in V(I)$. Now suppose $p \in V(I)$. Since $fg \in I$, this implies $fg \in p$. So $f \in p$ or $g \in p$. Then p contains either (I, f) or (I, g). So $p \in V((I, f)) \cup V((I, g))$.

Since $V(I)$ is irreducible, $V(I) = V(I, f)$ or $V(I, g)$. So $\sqrt{(I, f)} = \sqrt{I} = I$ or $\sqrt{(I, g)} = \sqrt{I} = I$. So either $f, g \in I$. So I is prime.

We see that composition in either direction gives identity. So these two maps give us our bijection. □

9. Sept 29: noetherian, cayley-hamilton, nakayama's lemma, integral extensions

Last time we proved a bijection between the primes of R and the closed irreducible subsets of $Spec(R)$.

Lemma 9.1. *Let X be a Noetherian topological space. Then every closed subset of X can be uniquely expressed as a finite union of irreducible subsets.*

Proof. Let $\mathcal{C} = \{S \subseteq X |$ S not expressible as finite union of irreducible subsets $\}$. We'll show that S is empty. Assume FSOC that S is nonempty. So suppose $A_1 \in X$. Suppose there is a proper subset A_2 of A_1 that is in $\mathcal{C}$. We can continue to take proper subsets to get a chain $A_1 \supsetneq A_2 \supsetneq A_3 \supsetneq \cdots$. But since X is Noetherian, this chain must stabilize at some A_n. But A_n itself cannot be irreducible, and since the chain stabilizes, A_n must not have any subsets in $\mathcal{C}$. So $A_n = B \cup C$ for proper closed B, C, which are properly contained in A_n. So B, C can be expressed as a finite union of irreducibles. Thus, so can A_n, contradiction. So $\mathcal{C}$ is empty.

Exercise to reader to verify uniqueness. □

Proposition 9.2. *If R is Noetherian, then $Spec(R)$ has finitely many irreducible components and $Spec(R)$ is the union of the irreducible components.*

Proof. The latter statement is true by Zorn's lemma. So let's show that $Spec(R)$ has finitely many irreducible components. But by the previous lemma, since R is Noetherian, so is $Spec(R)$. So $Spec(R)$ is a finite union of irreducible closed subsets. Choose a minimal union $Spec(R) = \bigcup_{i=1}^{n} Y_k$. Let Y be an irreducible component of $Spec(R)$. Since Y is closed, $Y = \bigcup_{i=1}^{n} Y \cap Y_i$, so there must exist i s.t. $Y = Y \cap Y_i$. So $Y \subseteq Y_i$. So $Y = Y_i$ by maximality. □

Let's connect this back to primary decomposition.

Last time we saw that if R is Noetherian ring, and $I \subseteq R$, then I can be expressed as a decomposition $I = I_1 \cap \cdots \cap I_k$ s.t. I_ℓ is p_ℓ-primary.

Note $V(I) = \cup V(I_j) = \cup V(\sqrt{I_j}) = \cup V(p_\ell)$. And $V(p_\ell)$ is closed and irreducible.

So in the decomposition of $V(I)$, you only really see the p_ℓ. The reduced structure.

Example 9.3. Take $k[X]$ and the ideal $I_1 = (x)$ and $I_n = (x^n)$. Note $V(I_1) = V(I_n)$. So the multiplicity of x^n in I_n does not appear in geometry.

Example 9.4. Take $k[X, Y]$. Let $I = (X^n Y^m) = (X^n) \cap (Y^m)$. The vanishing set of I is the union of the X and Y axis.

If you look at the examples, you see that when you look at the geometry, you do lose some information.

We're going to start a something new now. Today we'll talk about **integral extensions**.

First, we discuss some very important and useful commutative algebra theorems, namely the Cayley-Hamilton theorem and Nakayama's lemma. The former will be used to prove the latter.

We have

Theorem 9.5 (Cayley-Hamilton)**.** *Let R be a ring and N f.g. R-module. Let $\{e_1, \cdots, e_n\}$ generate N, and $f : N \to N$ an R-module homomorphism. Then*

$$f(e_j) = \sum_{i=1}^{n} \alpha_{ij} e_i$$

and let $M = (\alpha_{ij})_{1\leq i,j\leq n}$ be our matrix representing f. Let $P(X) = \det(M - XI_n) \in R[X]$.

Then $P(f) = \det(M - fI_n) : N \to N$ is the zero map.

Proof. Now we can equip N with $R[X]$-module structure, namely by letting R act in the obvious way on N and X act on N via f.

Now we have

$$f(e_j) = \sum_{i=1}^{n} \alpha_{ij} e_i$$

which can be rewritten as

$$\begin{aligned} 0 &= \sum_{i=1}^{n} \alpha_{ij} e_i - \delta_{ij} f(e_i) \\ &= \sum_{i=1}^{n} \alpha_{ij} e_i - \delta_{ij} X e_i \\ &= [M - XI]e_j \end{aligned}$$

Multiplying by the adjoint of $[M - XI]$, we have $\det(M - XI)e_j = 0$. This is true for every j. So $\det(M - fI) = 0$. □

Theorem 9.6 (Nakayama's)**.** *Let M be a finitely generated R-module, $I \subseteq R$, st. $IM = M$. Then there exist $a \in I$ s.t. $(1 + a)M = 0$.*

Proof. Let $\Phi = Id_M$. Let $(e_1, \cdots, e_n)$ be a family that spans M as an R-module. Note since $e_j \in M = IM$, each e_j can be written as a finite sum of elements in IM, i.e as $\sum cm$ where $c \in I, m \in M$. Each of these m can be written as a finite sum of the e_i. If we plug in the linear combination in terms of e_i for each m, we'll get an expression $\Phi(e_j) = \sum \alpha_{ij} e_i$ where $\alpha_{ij} \in I$.

Then let $M = (\alpha_{ij})$, so M is a matric with entries in I. Cayley-Hamilton tells us that if $P(X) = \det(M - XI) \in I[X]$, then $P(\Phi) = 0$. Write $P(X) = X^n + \sum_{i=1}^{n-1} b_i X^i$ where $b_i \in I$. Then $P(\Phi)(m) = 0 \implies m + \sum_{i=0}^{n-1} b_i m = 0$. So let $a = \sum_{i=0}^{n-1}$.

□

As a corollary:

Proposition 9.7. *With the same assumptions as above, if $I \subseteq J(R)$ the jacobson radical, then $M = 0$.*

Proof. If $I \subseteq J(R)$, and $a \in I$, then by proposition 1.13, $1 - a$ is a unit. But by Theorem 9.6, there exist an element $b \in I$ s.t. $(1 + b)M = 0$. So $M = 0$. □

Another corollary:

Proposition 9.8. *Assume $I \subseteq J(R)$, and M f.g. R-module. If $N \subseteq M$ and $M = N + IM$, then $M = N$.*

Proof. If $M = N + IM$, then quotienting by N gives $M/N = I(M/N)$. Then since $I \subseteq J(R)$, this implies $M/N = 0$. So $M = N$. □

Let's look at some applications.

Theorem 9.9. *Let (R, I) be a local ring (has unique maximal ideal). Note the jacobson radical is I, and every ideal is contained in I. Let M be a finitely generated R-module.*

- *Then M/IM is a finite dimensional vector space over $R/I = k$.*
- *A set $\{\overline{x_1}, \cdots, \overline{x_n}\}$ is a basis of $M/IM \iff \{x_1, \cdots, x_n\}$ is minimal set of generators of M over R.*
- *Any minimal set of generators of M have the same cardinality.*

Proof. (1) is immediate since M is finitely generated, I is maximal, so M/IM must be a finite dimensional vector space.

Note (3) follows immediately from (2). The cardinality of any minimal set of generators must equal the dimension of M/IM.

So let's prove (2). Let's prove the forward direction. let $N = Rx_1 + \cdots + Rx_n$. Then $M = N + IM$. Then by Nakayam's lemma, $M = N$. Note $\{x_1, \cdots, x_n\}$ must be minimal. If it weren't, then we'd have WLOG $x_1, \cdots, x_i$ spanning M, which means $\overline{x_1}, \cdots, \overline{x_i}$ span M/IM.

The reverse direction: suppose $\{x_1, \cdots, x_n\}$ is minimal set of generators of M over R. Then $\overline{x_1}, \cdots, \overline{x_n}$ span M/IM. Suppose this wasn't a basis. So WLOG there is some subset $\{\overline{x_1}, \cdots, \overline{x_i}\}$ that spans M/IM. Then let $N = Rx_1 + \cdots + Rx_i$. We have $M = N + IM$. So $M = N$, contradiction on the minimality of $\{x_1, \cdots, x_n\}$. □

Proposition 9.10. *If M is a finitely generated R-module, and $f : M \to M$ surjective endomorphism, then f is in fact an isomorphism.*

Proof. Consider M as a $R[X]$-module, where the action of X on M is defined by $X \mapsto f$. Since $f : M \to M$ is surjective, if $I = (X)$, then $M = IM$. Note it is still a finitely generated $R[X]$-module. Then by Nakayam's lemma (9.6), there exist $a = Xg(X) \in I$ s.t. $(1 - Xg(X))M = 0$. So $(1 - g(X)X)m = 0 \implies m = g(X)Xm$. This implies that the action of X on M, namely $f : M \to M$, is injective. □

Definition 9.11. Let $R \to S$ be ring extension. An element $\alpha \in S$ is said to be integral over R if there exist unitary (monic) polynomial $P \in R[X]$ s.t. $P(\alpha) = 0$.

Example 9.12. Consider $R \to R$. Then $\alpha \in R$ is integral over R. Just take $X - \alpha \in R[X]$.

Example 9.13. If $K \to L$ is a field extension, then $\alpha \in L$ is integral over $K \iff \alpha$ is algebraic over K.

Example 9.14. $\mathbb{Z} \to \mathbb{Z}[i]$. We have $i \in \mathbb{Z}[i]$ is integral over $\mathbb{Z}$, via $x^2 + 1$.

Or $\mathbb{Z} \to \mathbb{Z}[\sqrt{n}]$, look at $x^2 - n$.

Example 9.15. $\mathbb{Z} \to \mathbb{Q}$. Any $\alpha \in \mathbb{Q}$ is integral over $\mathbb{Z}$.

In general, if R is UFD, $R \to Frac(R) = K$. We have $\alpha \in K$ integral over $R \implies \alpha \in R$.

Theorem 9.16. *Let $R \to S$ be a ring extension, $\alpha \in S$. TFAE:*

- *α is integral over R.*
- *$R[\alpha]$ is a finitely generated R-module.*
- *$R[\alpha] \subseteq R'$, R' f.g. R-module.*
- *There exist $R[\alpha]$-module M such that $Ann(M) = \{0\}$ (in the ring $R[\alpha]$), and M is a f.g. R-module.*

Proof. For (1) $\implies$ (2): there exists monic $P \in R[X]$ s.t. $P(\alpha) = 0$, and $P(X) = X^n + \sum a_k X^k$. So $\alpha^n \in Span_R(1, \cdots, \alpha^{n-1})$. So in fact, $\forall k \geq n$, $\alpha^k \in Span_R(1, \cdots, \alpha^{n-1})$. So $R[\alpha]$ is a finitely generated R-module.

For (2) $\implies$ (3): just take R' to be $R[\alpha]$.

For (3) $\implies$ (4) : take $M = R'$. If $x \in R[\alpha]$, and $xM = 0$. Then $1 \in M \implies x * 1 = 0 \implies x = 0$.

For (4) $\implies$ (1): consider multiplication map by α from $M \to M$. This is an R-endomorphism. By Cayley-Hamilton, there exist a monic polynomial $P \in R[X]$ s.t. $P(f_\alpha)(m) = 0$, which means $P(\alpha)m = 0$. So $P(\alpha) \in Ann(M) = 0$, so α is integral over R. □

Definition 9.17 (/lemma)**.** Let $R \to S$ be a ring extension.

- The set of elements of S that are integral over R form a ring $\widetilde{R}$. This is called the integral closure of R in S.
- If R is a integral domain, $S = Frac(R)$. We say that R is normal (integrally closed) if $R = \widetilde{R}$, the integral closure in $Frac(R)$.

Note you need to justify $\widetilde{R}$ is a ring.

10. Oct 4: integral closure is ring, normality, dimension

Recall if we have injection $R \to S$, we say that $x \in S$ is **integral** over R if there is some unitary polynomial

$$x^n + c_{n-1}x^{n-1} + \cdots + c_0 = 0$$

where $c_i \in R$.

Example 10.1. Consider $\mathbb{Z} \to \mathbb{Q}$. If $\frac{a}{b}$ was integral, and you cleared denominators, you'd find the $b|a$, so $\frac{a}{b}$ must be an integer. So the integral closure of x is

Definition 10.2. Let $R \to S$ be ring extension. The integral closure $\widetilde{R} = \{s \in S|$ s integral over R $\}$.

This is what the integral closure looks like as a set. Let's verify that it's also a ring.

Proposition 10.3. *Let $R \to S$ be a ring extension. The integral closure $\widetilde{R}$ is a ring.*

Proof. Obviously $0, 1 \in \widetilde{R}$.

Let $x, y \in \widetilde{R}$. So by Proposition 9.16, we know $R[x]$ and $R[y]$ are finitely generated R-modules. Want to show $R[x + y]$ is finitely generated. Note that

$R[x+y] \subseteq R[x,y]$. So it suffices to show $R[x,y]$ is f.g. R-module. Find n s.t. $x^n \in R\langle 1, x, \cdots, x^{n-1}\rangle$, and m s.t. $y^m \in R\langle 1, y, \cdots, y^{m-1}\rangle$. So $x^n y^m \in R\langle x_i y_j\rangle$ for $1 \leq i \leq n-1, 1 \leq j \leq m-1$. Thus, $R[x,y]$ is f.g. R-module, so $R[x+y]$ is f.g. R-module.

Note $R[xy] \subseteq R[x,y]$, so $xy \in \widetilde{R}$ as well. Finally, $-x \in \widetilde{R}$ since if $R[x]$ is f.g. R-module then obviously $R[-x]$ is as well. □

Proposition 10.4. *Suppose you have $R \to S \to T$ where $R \to S$ is an integral extension, and $S \to T$ is an integral extension. Then $R \to T$ is integral extension.*

Proof. S is integral over R, so S is a f.g. R-module. So let $S = R\langle g_1, \cdots, g_k\rangle$. Also T is f.g. over S. So $T = S\langle e_1, \cdots, e_n\rangle$. So we see that T is f.g. as an R-module as well, via $T = R\langle g_i e_j\rangle$. This is all implicitly using proposition 9.16. □

Definition 10.5. An integral domain R is normal if the integral closure $\widetilde{R}$ in $K = Frac(R)$ is itself, i.e. $\widetilde{R} = R$.

Example 10.6. If you take $R = K[X^2, X^3]$. Then R is not integrally closed. The integral closure is just $\widetilde{R} = k[X]$. So R is not normal.

Example 10.7. In algebraic geometry example: $k[x^2, x^3]$ is given by $x^3 - y^2 = 0$. A result of Zariski is: taking integral closure for curves removes singularities.

Here's some handwavy reason why you should believe the next theorem is true: if you believe that normality say something about how geometrically a space doesn't have too much crazy singularities, then the space times your field shouldn't have crazy singularities either.

Theorem 10.8. *If R is normal, then $R[x]$ is normal.*

Proof. Want to show $R[x]$ is integrally closed. Note that $Frac(R[X])$ is $k(X)$ where $k = Frac(R)$. Note $k(X) = \{f/g | f, g \in k[X]\}$.

Let $t \in k(X)$ be integral over $R[X]$. Then $t^n + \alpha_{n-1}t^{n-1} + \cdots + \alpha_0 = 0$, where $t = \frac{P}{Q}$ where P, Q are coprime. So plugging in this fraction into the equation, we get $P^n + cQP^{n-1} + \cdots + c_0 Q^n = 0$. This implies $Q|P$. So we must have $t \in R[X]$. □

Sidenote: UFD is not "geometric," more of a number theory fact. Normality is indeed a geometric fact. UFD implies normality.

Lemma 10.9. *Let R be normal. Let $A(x) \in R[X]$, where $B(x), C(x) \in K[X]$. Say $A = BC$, BC monic. Then either B or $C \in R[X]$.*

Proof. The equation $A = BC \implies A$ is monic. So all roots of $A(x)$ are integral. So $A(x) = \prod(x - \alpha_i)$ are integral over A. (We're implicitly taking the algebraic closure of k here). Then the roots of B, C are integral too. So $B(x) = \prod(x_{b_i})$, the coefficients are in terms of the b_i, so the coefficients of B are integral. These coefficients are in k, so they're integral over R. Then they're contained in R because R is normal. □

Suppose we have $P(x) \in k[X]$ is integral over $R[X]$. Then $P^n + \alpha_{n-1}P^{n_1} + \cdots + \alpha_0 = 0$. Then $\alpha_0 = -P(\alpha_1 + \alpha_2 P + \cdots + P^{n-1})$. But we need α_0 and P and the latter sum to be monic. So the trick is to replace P with $P(x) + X^N$ for N sufficiently large. This is still integral. Plugging this in, we see that we can assume P and α_0 is monic.

Now we're going to talk about Noether's Normalization.

How do you define dimension? Intuitively, we think of $k[X]$ being dimension 1. And $k[X,Y]$ being dimension 2. But what about $k[X,Y]/(X^2-Y^3) \cong k[X^2,X^3]$? (Turns out this is dimension 1).

Philosophy of Dimension of a k-Algebra: its the "number of independnet algebraic variables it can have."

Definition 10.10. We say $r_1, \cdots, r_n \in R$ are algebraically independent if $P(r_1, \cdots, r_n) = 0 \iff P = 0$ for $P \in k[X_1, \cdots, X_n]$.

Definition 10.11. If $k \subseteq L$ is a field extension, the transcendence degree $trdeg_k(L) = \text{ maximal number of algebraic independent elements }$.

Its a fact that any maximal set of algebraic indepednent elements are of the same size.

Proof sketch: say $\{y_1, \cdots, y_n\}$ is maximal alg independent set and $\{x_1, \cdots, x_m\}$ is maximal alg independent set. WLOG assume $n > m$. look at $\dim_k$

Definition 10.12. If R is an integral domain and a k-Algebra, then $\dim(R) = trdeg_k(Frac(R))$.

What if R is not an integral domain? For example $k[X,Y]/(xy)$. Geometrically this looks like the union of $k[X,Y]/(x)$ and $k[X,Y]/(y)$. You can define the dimension as the dimension of the bigger of the two. So in general, you can do something like find a primary decomposition then find the dimension of each (something like that?)

We won't prove but only state:

Theorem 10.13 (Noether Normalization)**.** *If R is a k-algebra, there exist algebraically independent elements $x_1, \cdots, x_n \in R$ s.t. $k \to k[x_1, \cdots, x_n] \to R$ s.t. R is f.g. $k[x_1, \cdots, x_n]$-module and R is integral over $k[x_1, \cdots, x_n]$.*

11. Oct 6: noether's normalization

Let's dive into Noether's Normalization theorem today. Emmy Noether (a prolific, underrated mathematician) proved this for infinite fields k in 1926, and Nagata proved it generally in 1962. You'll notice that Nagata and Nakayama are both Japanese mathematicians. Grothendieck coined the name "Japanese rings" in honor of the Japanese school of mathematics, which has seen great contributions to commutative algebra and algebraic geometry.

Note that in a k-algebra A, we say $\alpha_1, \cdots, \alpha_n$ are algebraically independent if for any $P \in k[X_1, \cdots, X_n]$ we have $P(\alpha_1, \cdots, \alpha_n) = 0$, then $P = 0$.

We say that A is a finite type k-Algebra if every element of A can be expressed as a polynomial in terms of $\alpha_1, \cdots, \alpha_n$, with coefficients in k. In other words, there's a surjective ring homomorphism $k[X_1, \cdots, X_n] \to A$, where $X_i \mapsto \alpha_i$.

Theorem 11.1 (Noether Normalization)**.** *Let k be a field, A a finite type k-algebra. Then there exist $a_1, \cdots, a_n \in A$ algebraically independent over k s.t. $k[a_1, \cdots, a_n] \to A$ is finite integral extension.*

Proof. By lemma 11.3, since A is a finite type k-algebra, there exist elements $a_1, \cdots, a_n$ s.t. $A = k[a_1, \cdots, a_n]$. Induct on n, the number of generators. If they're algebraically independent, then we're done. Otherwise, they're algebraically dependent, so by the lemma, there are elements $y_1, \cdots, y_{n_1} \in A$ and $A' = k[y_1, \cdots, y_{n-1}]$ and $A' \to A'[a_n] = A$ is finite integral extension. If the $y_1, \cdots, y_{n-1}$ are algebraically independent, you're done. Otherwise, continue to apply lemma 11.3. So there would exist algebraically independent $b - 1, \cdots, b_k \in A$ s.t. $k[b_1, \cdots, b_k] \to \cdots \to A' \to A$, and the composition of a finite number of finite integral extensions is a finite integral extension. □

Lemma 11.2. *If $R \to S$ ring extension, and $\alpha_1, \cdots, \alpha_n \in S$ are integral over R. Then $R[\alpha_1, \cdots, \alpha_n]$ is a finitely generated R-module.*

Proof. For clarity, consider first showing $R[\alpha_1, \alpha_2]$ is f.g. R-module. Since α_1, α_2 are integral over R, we have $R[\alpha_1]$ is finitely generated by $\{g_1, \cdots, g_n\}$ and $R[\alpha_2]$ is finitely generated by $\{e_1, \cdots, e_m\}$. Then for $\alpha_1^i \alpha_2^j$, we have it is expressible in terms of the $\{g_i e_j\}$.

So if we have $\alpha_1, \cdots, \alpha_n \in S$ integral over R, take the generating set G_i for $R[\alpha_i]$ for each i, then $R[\alpha_1, \cdots, \alpha_n]$ is spanned by all the possible multiplication of some elements in the G_i. □

Lemma 11.3. *Let A be a k-algebra generated by $a_1, \cdots, a_n$ which are algebraically dependent. Then there exist $y_1, \cdots, y_{n-1}$ in A s.t. a_n is integral over $A' = k[y_1, \cdots, y_{n-1}]$ and $A = A'[a_n]$.*

Proof. Since $a_1, \cdots, a_n$ is algebraically dependent, there exist $P \in k[X_1, \cdots, X_n]$ s.t. $P \neq 0$ and $P(a_1, \cdots, a_n) = 0$. We're going to set $y_i = a_i - a_n^{e^i}$ where $1 \leq i \leq n-1$ and e is a positive integer to be determined later. Note that for whatever integer e we pick, we have $A = k[y_1, \cdots, y_{n-1}, a_n]$. So now we show that a_n is integral over $k[y_1, \cdots, y_{n-1}]$. The integer e we pick will be one that guarantees this.

Note we have

$$\begin{aligned} 0 &= P(a_1, \cdots, a_m) \\ &= P(y_1 + a_n^e, \cdots, y_{n-1} + a_n^{e^{n-1}}, a_n). \end{aligned}$$

We can view this polynomial as $Q(y_1, \cdots, y_{n-1}, a_n)$, and also as $\widetilde{Q}(z) = Q(y_1, \cdots, y_{n-1}, a_n) \in (k[y_1, \cdots, y_{n-1}])[a_n]$.

Expanding P as a polynomial of the X_i, we have $P(X) = \sum \alpha_I X_1^{r_1} \cdots X_n^{r_n}$, where $\alpha_I \in k$. We have for each tuple $(r_1, \cdots, r_n)$ that

$$X_1^{r_1} \cdots X_n^{r_n} = (\prod_{i=1}^{n-1} (Y_i + X_n^{e^i})^{r_i}) X_n^{r_n}.$$

if we expand this polynomial out as well, we'll get something that looks like

$$Y_1^{r_1} \cdots Y_{n-1}^{r_{n-1}} X_n^{r_n} + \cdots + X_n^{r_1 e + \cdots + r_{n-1} e^{n-1} + r_n}.$$

Choose integer e that is greater than all integers that appear in all the tuples $(r_1, \cdots, r_n)$. Then note that $r_1 e + \cdots + r_{n-1} e^{n-1} + r_n$ is a conversion from base e to base 10. So if e is greater than all the integers that appear in all tuples, then each tuple $(r_1, \cdots, r_n)$ gives a unique $r_1 e + \cdots + r_{n-1} e^{n-1} + r_n$.

This means that when viewing P as a polynomial in terms of X_n with coefficients in $k[Y_1, \cdots, Y_{n-1}]$, we have a leading power of X_n whose coefficient is $\alpha_{(r_1, \cdots, r_n)}$ for the tuple $(r_1, \cdots, r_n)$ that has maximum $r_1 e + \cdots + r_{n-1} e^{n-1} + r_n$.

Thus, we have a monic polynomial with coefficients $k[Y_1, \cdots, Y_{n-1}]$ with root a_n.

□

As a corollary, we have the deep theorem:

Suppose you have a finite field extension $K \to L$, and you take the integral closure $\widetilde{A} \subset L$ of a ring $A \subset K$ over L. Is this still a finite extension? In general this is not true. But under certain hypothesis, it is. Before we state this theorem, we discuss some Galois Theory prerequisites:

A **normal** field extension $K \to L$ is a field extension s.t. if $f(x) \in K[X]$ is irreducible and has a root in L, then f splits completely in L (i.e. L contains all the other roots of f).

If $K \to L$ is a field extension, $\alpha \in L$ is **separable** if the minimal polynomial of α over K is separable (i.e no multiple roots).

We say that the extension $K \to L$ is **separable** if every element of L is separable over K. So for every $\alpha \in L$, the minimal polynomial of α over K is a separable polynomial. This implicitly means that $K \to L$ is also an algebraic extension.

We also discuss something called the **field trace**. Given a field extension $K \to L$, we can consider L as a K-vector space. For $\alpha \in L$, $m_\alpha : L \to L$ given by $v \mapsto \alpha v$ is a K-linear transformation. Then $Tr_{L/K}(\alpha)$ is defined to be the trace of this linear transformation.

Concretely, we have the following formula: if $\alpha \in L$, and $\sigma_1(\alpha), \cdots \sigma_n(\alpha)$ are the roots of the minimal polynomial of α over K, then

$$Tr_{L/K}(\alpha) = [L : K(\alpha)] \sum_{i=1}^{n} \sigma_i(\alpha).$$

Then if L/K is separable, for every α, each root appears only once.

In fact, when L/K is separable, we have a nondegenerate, symmetric bilinear form called the **trace form**. It's the map $L \times L \to K$ sending $(x, y) \mapsto Tr_{L/K}(xy)$.

Theorem 11.4. *Let k be a field, A k-algebra that is integral domain and finite type. Let $k_A = Frac(A)$, and $k_A \to L$ finite field extension. Let $\widetilde{A}$ denote the integral closure of A over L. Then $A \to \widetilde{A}$ is a finite ring extension.*

Proof. By Noether normalization, we know that $k[a_1, \cdots, a_n] \to A$ finite integral extension, and $k[a_1, \cdots, a_n] \cong k[X_1, \cdots, X_n]$. This is Noetherian and integrally closed. And $k(a_1, \cdots, a_n) \to k_A$ finite extension (exercise).

So L is also a finite extension of $k(a_1, \cdots, a_n)$. We have $k(a_1, \cdots, a_n) \to^{finite} k_A \to^{finite} L$ and looking at $k[a_1, \cdots, a_n] \to A \to \widetilde{A}$, in this tower of extensions $\widetilde{A}$ is integral closure of $k[a_1, \cdots, a_n]$ in L. If $char(k) = 0$, then $k(a_1, \cdots, a_n) \to L$ is separable.

This implies that $k_A \to L$ is also a separable extension.

We finish off the proof of this theorem by the next lemma. □

Lemma 11.5. *We have $k_A = Frac(A)$, and $k_A \to L$ is finite separable extension. Then $\widetilde{A}$ = integral closure of A in L is Noetherian and thus a finite extension of A.*

Proof. Any element $x \in L$ satisfies the equation $x^n + \lambda_{n-1}x^{n-1} + \cdots + \lambda_0 = 0$, where $\lambda_i \in K_A$. Then there exist $a \in A$, s.t. $a\lambda_i \in A$ for every i. So $(ax)^n +$

$a\lambda_{n-1}(ax)^{n_1} + \cdots + a^n\lambda_0 = 0$. So $ax \in \widetilde{A}$. Hence, we can find a k_A-basis of L given by elements of $\widetilde{A}$. So $(b_1, \cdots, b_n)$ is k_A-basis of L, $b_i \in \widetilde{A}$.

Let $N = \{x \in L | Tr_{L/K}(xb_j) \in A \forall j \in \{1, \cdots, r\}\}$. Then N is an A-module containing $\widetilde{A}$. This is because for any $x \in \widetilde{A}$, we have $Tr_{L/K}(x) \in A$. Note $Tr_{L/K}(x) \in K$ and it is a sum of integral elements over A which implies it is in A.

We have $Tr_{L/K} : L \times L \to K$ is non degenerate. So there exist $(x_1, \cdots, x_n)$ is k-basis of L such that $Tr_{L/K}(x_i b_j) = \delta_{ij}$. Then $N = Ax_1 + \cdots + Ax_n$. To see $\subseteq$, note if $x \in N$, then $x = \sum_{i=1}^r \alpha_i x_i$ where $\alpha_i \in K$. So $\alpha_i = Tr_{L/K}(xb_i) \in A$. Thus, N is a f.g. A-module which implies N is Noetheiran. Since $\widetilde{A} \subseteq N$ is a sub A-module. So $\widetilde{A}$ is noetheiran and a f.g. A-module. Thus $A \to \widetilde{A}$ is finite.

□

12. Oct 11 hilbert's nustellensatz

For a brief review of Galois theory notions, see chapter 4 of Chambertloir. In the bibliography section on Canvas.

Lemma 12.1. *Ring extension $R \to S$ is finite $\iff$ S is finite type R-algebra and integral over R.*

Last time we were trying to prove the following corollary:

Theorem 12.2. *Let k a field, A a finite type k-algebra. $K_A \to L$ is a finite extension, and $\widetilde{A}$ is the integral closure of A in L. Then $\widetilde{A}$ is finite extension of A, which implies $\widetilde{A}$ is a finite-type k-algebra, Noetherian, and integral domain.*

Proof. Last time, we proved this when $k_A \to L$ is separable.

We can assume that $A = k[a_1, \cdots, a_n] \cong k[x_1, \cdots, x_n]$ using Noether normalization.

Then replace L by its normal closure. If $L = k_A(B_1, \cdots, B_n)$, then the normal closure $L' = K_A(B_1, \cdots, B_n)$ plus all other roots in the minimal polynomials of each B_i. If you prove that in the tower $k_A \to L \to L_{norm}$, if $B \subset L_{norm}$ is finite over A, then $\widetilde{A}$ finite over A. Then we can assume $k_A \to L$ normal extension.

Let $G = Gal(L/K_A)$. Let $L' = L^G$, the fixed field of G.

Artin's lemma: L/L' is galois extension with Galois group G. Where $k_A \to L' \to L$, and $k_A \to L'$ is purely inseparable, and $L' \to L$ is separable. So in $k_A \to L' t \emptyset L$ and we have $A \to B' \to \widetilde{A}$, where $B', \widetilde{A}$ is integral closure of A. From last time, we already know $B' \to \widetilde{A}$ is finite. So enough to show $A \to B'$ is finite.

Let $y_1, \cdots, y_n$ be generators of the extension $K_A \to L'$. Since $k_A \to L'$ is purely inseparable, there exist $r > 0$ s.t. $y_i^{p^r} \in k_A$ and $y_i^{p^r} = \frac{p_i}{q_i}$.

Let $t_1, \cdots, t_r \in k$ be the nonzero coefficients of p_i, q_i. Let $K' = K(t_1^{p^{-r}}, \cdots, t_s^{p^{-r}}) =$ splitting field of $x^{p^r} - t_i$ for every i. Note K' is finite extension of K and also a purely inseparable extension of K.

Char$(k) = p > 0$. Let $L' = k_A(y_1, \cdots, y_m) \subseteq k_A(P_1^{p^{-r}}, Q_1^{p^{-r}}, \cdots, P_m^{p^{-r}} \subseteq k(t_1^{p^{-r}}, \cdots, t_s^{p^{-r}}, a_1^{p^{-r}}, \cdots, a_n^{p^{-r}})) = k'(a_1^{p^{-r}}, \cdots, a_n^{p^{-r}}) =: L''$.

Call the integral closure of B' in L" to be $\widetilde{B'}$. Note $K \to K'$ is finite, and $A = k[a_1, \cdots, a_n] \to k'[a_1, \cdots, a_n]$ is finite. Note $k'[a_1, \cdots, a_n] \to k'[a_1^{p^{-r}}, \cdots, a_n^{p^{-r}}]$.

So $A = k[a_1, \cdots, a_n] \to k'[a_1^{p^{-r}}, \cdots, a_n^{p^{-r}}]$. Note the $a_i^{p^{-r}}$ are still algebraically independent. $L^{"} \cong k'(x_1, \cdots, X_n)$. and this $L^{"} \supseteq k'[a_1^{p^{-r}}, \cdots, a_n^{p^{-r}}]$ integrally closed in L.

So we have $A \to B' \to \widetilde{B'}$ finite implies $A \to B'$ finite so $A \to \widetilde{A}$ is finite.

□

WARNING: The above was poorly written and likely not very clear. Will have to go back and fix it at some point.

We're moving on now to Hilbert's zero theorem (Nullstellensatz).

Lemma 12.3. *Let $R \to S$ be integral ring extension of domains. Then R is a field $\iff$ S is a field.*

Proof. Assume R is a field. Let $0 \neq y \in S$. Since y is integral, we have an equation $y^n + a_{n-1}y^{n-1} + \cdots + a_1 y + a_0 = 0$, where $a_i \in R$. If $a_0 \neq 0$, then $y(y^{n-1} + a_{n-1}y^{n-2} + \cdots + a_1) = -a_0$. This shows y is invertible with inverse $\frac{y^{n-1}+a_{n-1}y^{n-2}+\cdots+a_1}{-a_0}$. If $a_0 = 0$, since S is an integral domain we can factor out a y and repeat the process. Since $y \neq 0$, at some point we must have a constant term that is nonzero, and thus find an inverse.

Now suppose S is a field. Let $x \in R$. There exist $y \in S$ s.t. $xy = 1$, and y is integral over R, so $y^n + a_{n-1}y^{n-1} + \cdots + a_1 y + a_0 = 0$ for some $a_i \in R$. Multiply by x^{n-1} to get $y + a_{n-1} + \cdots + a_1 x^{n-2} + a_0 x^{n-1} = 0$. Since $a_i \in R$ and $x \in R$, this implies $y \in R$. □

Theorem 12.4 (Hilbert's Nullstellensatz)**.** *Let $K \to L$ be an extension of fields such that L is a finite type K-algebra. Then L is a finite extension of K.*

Proof. Noether's normalization implies that since L is finite type k-algebra, you can find extension $k \to k[a_1, \cdots, a_n] \to L$ s.t. $k[a_1, \cdots, a_n] \to L$ is finite and integral. By the lemma since L is a field, then $k[a_1, \cdots, a_n]$ is a field. But a ring of polynomials can only be a field only if there are no formal variables. So $K \to L$ is a finite, integral extension. □

As a corollary, if $K = \bar{k}$ is algebraically closed then we have:

Theorem 12.5 (Hilbert's Weak Nullstellensatz)**.** *The maximal ideals of $k[X_1, \cdots, X_n]$ are exactly $m = (x_1 - a_1, \cdots, x_n - a_n)$ for $(a_1, \cdots, a_n) \in K^n$.*

Proof. First note that all of the $(x_1 - a_1, \cdots, x_n - a_n)$ are maximal. This is because $0 \to (x_1 - a_1, \cdots, x_n - a_n) \to k[x_1, \cdots, x_n] \to K \to 0$ is an exact sequence, and since the quotient is a field, we have maximality.

Now suppose m be a maximal ideal of $k[x_1, \cdots, x_n]$. Then the extension $k \to k[x_1, \cdots, x_n]/m = L$ is a field extension s.t. L is a finite type k-algebra. So by Hilbert's zero theorem, $K \to L$ is finite. So $L \cong K$ as a field because K is algebraically closed. Then via this isomorphism, the elements $X_i \in L$ map to some $a_i \in K$, so $X_i - a_i \in m$. So $(X_1 - a_1, \cdots, X_n - a_n) \subseteq m$, but by maximality of the former, we must have equality. □

As a cute corollary of Hilbert's Weak Nullstellensatz:

Proposition 12.6. *if $K = \bar{k}$ is algebraically closed. A system of equations $F_1(x_1, \cdots, x_n) = 0, \cdots, F_n(x_1, \cdots, x_n) = 0$ does not have a solution in k^n $\iff$ there exist $G_i \in k[X_1, \cdots, X_n]$ s.t $\sum F_i G_i = 1$.*

Proof. The reverse direction is easy. If we had $\sum F_i G_i = 1$, then if we had a solution $(x_1, \cdots, x_n)$ to all the F_i, then $\sum F_i(x_1, \cdots, x_n) G_i = 0 = 1$, which is impossible. So there are no solutions.

On the other hand, suppose $F_1, \cdots, F_n$ had no solutions. Assume FSOC that $(F_1, \cdots, F_n) \neq k[X_1, \cdots, X_n]$. Then it is contained in a maximal ideal m. But by Theorem **??**, m is of the form $(x_1 - a_1, \cdots, x_n - a_n)$. This would imply $(a_1, \cdots, a_n)$ is a solution to the F_i, contradiction. So $(F_1, \cdots, F_n) = k[X_1, \cdots, X_n]$, in particular $1 \in (F_1, \cdots, F_n)$.

(Sidenote: a result of Kollar gives a bound on the degree of the G_i in terms of the data you have) □

Another corollary (so many corollaries today):

Proposition 12.7. *Let k field. Let $I \subseteq k[x_1, \cdots, x_n]$ be an ideal. Then $\sqrt{I} = \bigcap_{maximal} m = J(I)$.*

If $F \subseteq Spec(A)$ is a closed subset

Proposition 12.8. *Let A be a finite-type k-algebra, then $F \subseteq Spec(A)$ is closed subset. Then $\overline{\text{closed points of } F} = F$.*

Proof. gives one line proof of showing $A[[X]]$ is not finite type k-algebra. □

13. Oct 13: Top to Down! Going Clown!

We prove a corollary from last time:

Proposition 13.1. *Let k be a field. Let $I \subseteq k[X_1, \cdots, X_n]$. We show $\sqrt{I} = \bigcap_{maximal} m$.*

Proof. We have the obvious inclusion $\sqrt{I} = \bigcap_{prime} p \subseteq \bigcap_{maximal} m$. Now we show the reverse inclusion. To show $\sqrt{I} \supseteq \bigcap_{maximal} m$, we prove by contrapositive. Suppose $P \notin \sqrt{I}$. We construct a maximal ideal containing I but not P.

Let $J \subseteq k[X_1, \cdots, X_{n+1}]$ be $J = (PX_{n+1} - 1, I)$. Assume FSOC that $J = k[X_1, \cdots, X_{n+1}]$. Then we have

$$1 = (PX_{n+1} - 1)A + \sum_{j=0}^{m} X_{n+1}^j F_j(X_1, \cdots, X_n)$$

where $F_j \in I$. Consider the map $k[X_1, \cdots, X_{n+1}] \to k(X_1, \cdots, X_n)$ defined by $X_i \mapsto X_i$ for $1 \leq i \leq n$ and $X_{n+1} \mapsto \frac{1}{P}$. Under this map, our above equation becomes $1 = \sum_{j=0}^m \frac{1}{P^j} F_j$. So $P^m = \sum_{j=0}^m P^{m-j} F_j$. So $p \in \sqrt{I}$, contradiction.

So $J \neq k[X_1, \cdots, X_{n+1}]$. Then it is contained in a maximal ideal $\widetilde{m} \subseteq k[X_1, \cdots, X_{n+1}]$. Let $m = \widetilde{m} \cap k[X_1, \cdots, X_n]$. Note m is prime. We show that m is also maximal.

Note we have a tower of extensions

$$k \to k[X_1, \cdots, X_n]/m \to k[X_1, \cdots, X_{n+1}]/\widetilde{m}.$$

Since $k[X_1, \cdots, X_{n+1}]/\widetilde{m}$ is a finite type k-Algebra, by Theorem 12.4, the extension $k \to k[X_1, \cdots, X_{n+1}]/\widetilde{m}$ is a finite extension. Thus, $k \to k[X_1, \cdots, X_n]/m$ is finite extension $\implies$ an integral extension. Since we have an extension of domains, since k is a field this means $k[X_1, \cdots, X_n]/m$ is a field as well, meaning m is maximal.

Note $p \notin m$. Otherwise $p \in \widetilde{m}$ together with $PX_{n+1} - 1 \in m \implies 1 \in m$, which is impossible. Thus, we have constructed a maximal ideal m containing I but not p. □

Another way of looking at this is that inside $Spec(k[x_1, \cdots, x_n])$, we have $\underline{V(I) = V(\sqrt{I}) = \{p \supseteq I\} \supseteq} \{m \supseteq I|$ maximal m $\}$. This is really saying that $V(\sqrt{I}) = \{m \supseteq I|$ maximal m $\}$.

Proposition 13.2. *If A is a finite type k-Alegebra, then closed points are dense in any closed subset of $Spec(A)$.*

What this means is that for every $I \subseteq A$, we have $\sqrt{I} = \bigcap_{I \subseteq m} m$.

Proof. We have $A = k[X_1, \cdots, X_n]/J$. The ideals of A are in bijection with the ideals of $k[X_1, \cdots, X_n]$ containing J. So this is true by what we proved above. □

Hint for pset: if the closure of all the closed points is not the entire $Spec(A)$, then A is not a finite k-algebra.

Definition 13.3 (Jacobson Ring)**.** A ring A is a Jacobson ring if the closed points are dense in any closed subset of $Spec(A)$.

Suppose we have $R \to S$ integral extension. We want to study what happens to $Spec(S) \to Spec(R)$. We want to study surjectivity, and also going-up and going-down theorems. These are very useful for comparing the dimension of R and the dimension of S.

We begin with the following lemma:

Lemma 13.4. *Let $R \to S$ be integral extension.*

- *If S domain, then R is a field $\iff$ S is a field.*
- *If $p \subseteq R$, $q \subseteq S$ prime ideals s.t. $q \cap R = p$, then p is maximal in R $\iff$ q maximal in S.*

Proof. We showed (1) before. We'll utilize it to prove (2). Take $R/p \to S/q$. This is integral, and since these are domains, R/p is a field $\iff$ S/q is a field. □

Proposition 13.5. *Let $R \to S$ be an integral extension. Let $p \subseteq R$ be a prime ideal.*

- *(Lying over) There exist prime $q \subseteq S$ s.t. $q \cap R = p$. This is asking whether in the map $Spec(S) \to Spec(R)$, $p \in Spec(R)$ is in the image.*
- *(Incomparability) If $q_1, q_2 \subseteq S$ primes both lying over p, then $q_1 \subseteq q_2 \implies q_1 = q_2$.*

Proof. Let $p \subseteq R$ be a prime ideal. Consider the map $R_p \to S_p$, where we localize S to be a R_p-module. This map is integral and also injective. Note we also have

$$\begin{tikzcd}
R \arrow[r] \arrow[d] & S \arrow[d] \\
R_p \arrow[r] & S_p
\end{tikzcd}$$

commutes. There exist a maximal ideal q of S_p. Then $q \cap R_p = pR_p$ by the previous lemma. Then the preimage of q in $S \to S_p$ is a prime which lies over p.

Now suppose we have $q_1 \subseteq q_2 \subset S$ lying over $p \subseteq R$. Both of these primes do not intersect with $R \setminus p$, so they have corresponding primes in S_p. These primes intersecting R_p give pR_p, which is maximal. Then by the previous lemma, they must also be maximal. Since $q_1 \subset q_2$, this means $q_1 = q_2$. □

Definition 13.6 (Going-Up Property)**.** An extension $R \to S$ satisfies the going-up property if given primes $p_1 \subseteq p_2 \subseteq R$ with $q_1 \subseteq S$ lying over p_1, there exist $q_2 \supseteq q_1$ lying over p_2.

Theorem 13.7. *An integral extension satisfies the going-up property.*

Proof. Let $R \to S$ be our integral extension. Note we have an induced map $R/p_1 \to S/q_1$ which is still integral. Furthermore, p_2/p_1 is a prime ideal of R/p_1. Thus, by proposition 13.5, there exist q_2/q_1 lying over p_2/p_1. □

Definition 13.8 (Going-Down Property)**.** An extension $R \to S$ satisfies the going down property if given prime ideals $p_1 \subseteq p_2$ and $q_2 \subseteq S$ s.t. q_2 lies over p_2, there exist q_1 lying over p_1.

Theorem 13.9 (Going-Clown Property)**.** *If $R \to S$ integral extension, and S is domain and R is integrally closed in S. Then $R \to S$ satisfies the going-down property.*

14. Oct 18: going-down, krull dimension

chapter 13 proposition 13.10 is proof of going down.

Definition 14.1 (Going-Down Property)**.** A ring extension $R \to S$ satisfies the going-down property if given $p_1 \subseteq p_2 \subseteq R$, and $q_2 \subseteq R$ lying over p_2, there exist $q_1 \subseteq q_2$ lying over p_1.

Proposition 14.2. *Let $S \to R$ be an integral extension, R domain, and S integrally closed. Then $S \to R$ satisfies the going down property.*

Proof. A mostly Galois-free proof: `https://peeps.unet.brandeis.edu/~igusa/Math205bS10/Math205b_S10_53.pdf` □

Now we'll discuss some dimension theory.

Definition 14.3 (Krull Dimension)**.** Let R be a ring. The krull dimension $\dim R := \sup\{r \in \mathbb{N} | \exists p_0 \subset p_1 \subset \cdots \subset p_r$ chain of prime ideals $\}$.

Note that even a Noetherian ring can have infinite dimension. This is because we are taking a supremum over the length of all proper chains of prime ideals.

Definition 14.4. If $p \subseteq R$ is a prime ideal, then the height of p is $\sup\{r | p_0 \subset p_1 \subset \cdots \subset p_r = p\}$.

So the height is the supremum over the length of all the proper chains of prime ideals that end at p.

Definition 14.5. The coheight of $p \subseteq R$ is $\sup\{r | p = p_0 \subset \cdots \subset p_r\}$

The coheight of p is the supremum over the length of all proper chains of prime ideals that start at p.

Some immediately corollaries:

Proposition 14.6. *Given prime $p \subseteq R$*

- *Height + coheight* $\leq \dim R$.
- *Coheight of p equals* $\dim R/p$. *Height of p is* $\dim p$ *(if you consider p a ring without identity)*

- *(R,m) local ring then* $\dim R =$*height of* m.

Example 14.7. If K is a field then $\dim K = 0$.

IF R domain, then $\dim R = 0 \implies R$ is a field.

$\dim \mathbb{Z} = 1$.

Any PID that is not a field has dimension 1.

A ring is artinian if

Definition 14.8. A ring R is Artinian if it satisfies the descending chain condition.

Proposition 14.9. *An Artinian ring R has dimension* 0*.*

Example 14.10. If k is a field, $\dim k[x_1, \cdots, x_n] = n$. We have $(0) \subset (x_1) \subset (x_1, x_2) \subset \cdots (x_1, \cdots, x_n)$. So the dimension is at least n. To show it is $\leq n$, utilize Noether normalization.

Example 14.11. Dimension of a topological space X. Then $\dim X = \sup\{F_n \subset \cdots \subset F_0, F_i \subset X$ all irreducible closed subsets $\}$.

Note $\dim(R) = \dim(Spec(R))$.

If $Y \subseteq X$, we have $\dim Y \subseteq \dim X$. If $X = \bigcup_{i=1}^n X_i$ where $X_i \subseteq X$ irreducible closed. Then $\dim X = \max \dim X_i$. If $X = \bigcup U_i$, U_i open then $\dim X = \max \dim U_i$.

15. Oct 20: transcendence basis

Definition 15.1 (Transcendence Basis)**.** $K \subseteq L$ fields. Subset $B \subseteq L$ is a transcendence basis if

- the elements of B are algebraically independent over K.
- L is an algebraic extension of $K(B)$.

Example 15.2. $\mathbb{Q}(e)$ over $\mathbb{Q}$. $B = \{e\}$ transcendence basis.

$k(x_1, \cdots, x_n)/k$. Transcendence basis $\{x_1, \cdots, x_n\}$.

This notion of a transcendence basis will give us another sort of dimension theory. But in order for it to capture such a notion, intuitively our first sanity check is that two finite transcendence bases of an extenison L/K must have the same cardinality. Indeed:

Proposition 15.3. *Suppose extension L/K has a finite transcendence basis. Then*

- *If $A \subseteq L$ is a finite set of elements algebraically independent over K, and $S \subseteq L$ s.t. $L/K(S)$ is algebraic extension, then $|A| \leq |S|$.*
- *All transcendence bases of L/K have the same cardinality.*

Proof. Let $A = \{a_1, \cdots, a_n\}$. Consider the subset $\{a_2, \cdots, a_n\}$. Suppose S was algebraic over $K(a_2, \cdots, a_n)$. Then $L/K(S \cup \{a_2, \cdots, a_n\})$ is algebraic extension, and $K(S \cup \{a_2, \cdots, a_n\})/K(a_2, \cdots, a_n)$ is algebraic. Thus $L/K(a_2, \ldots, a_n)$ is algebraic. This implies a_1 is algebraic over $K(a_2, \cdots, a_n)$, contradiction since they're supposed to be algebraically independent. Then there exist some $s_1 \in S$ that is not algebraic over $K(a_2, \cdots, a_n)$. Thus, $\{s_1, a_2, \cdots, a_n\}$ are all algebraically independent over K. We can continue this process, replacing each a_i with a $s_i \in S$. This shows that $|A| \leq |S|$.

Suppose B, B' are two transcendence bases. By definition, and applying the above claim, we get $|B| \leq |B'|$ and $|B'| \leq |B| \implies |B| = |B'|$. □

We also have a nice additive property for trasncendence degree of extensions.

Proposition 15.4. *If we have extensions M/L and L/K, then $trdeg_K M = trdeg_L M + trdeg_K L$.*

A brief interlude back to Krull dimension theory:

Lemma 15.5. *Let $R \to S$ be an integral ring extension. Then* $\dim R = \dim S$.

Proof. Let $p_0 \subset \cdots \subset p_r$ be a strict chain of prime ideals in R. Then by lying over, there exist prime $q_0 \subset S$ lying over p_0. By the going up theorem, we have there exist $q_0 \subset \cdots \subset q_r$ s.t. q_i lies over p_i. Thus, $\dim R \leq \dim S$.

Let $q_0 \subset \cdots \subset q_r$ be a strict chain of prime ideals in S. Intersecting with R, we get $q_0 \cap R \subset \cdots \subset q_r \cap R$ is a strict chain of prime ideals by incomparability. □

Lemma 15.6. *Let K a field. Then* $\dim k[X_1, \cdots, X_r] = r$.

Proof. If $r = 0$, then $\dim k = 0$. Now we proceed by induction. Suppose our claim holds for up to $r - 1$. We show it also holds for r.

It's easy to see that $\dim k[X_1, \cdots, X_r] \geq r$. Let $0 \subset p_1 \subset \cdots \subset p_m$. We'd like to show $m \leq r$. Let $f \in p_1$ be a reducible polynomial. Note that $X_1, \cdots, X_{r-1}, X_r$ is a algebraically dependent set of elements of $k[X_1, \cdots, X_r]$. By the main lemma used to prove Noether normalization, there exists $X_1', \cdots, X_{r-1}', f$ such that $k[X_1, \cdots, X_r]$ is a finite integral extension of the k-algebra S generated by $X_1', \cdots, X_{r-1}', f$. Then $0 \subset S \cap p_1 \subset \cdots \subset S \cap p_m$ is a strict chain of primes in S of length m by incomparabaility. Then $\frac{S \cap p_1}{(f)} \subset \cdots \subset \frac{S \cap p_r}{(f)}$ is a strict chain of primes of length $m - 1$ in $S/(f) \cong k[X_1', \cdots, X_{r-1}']$. By the inductive hypothesis, this means $m - 1 \leq r - 1 \implies m \leq r$. □

As a corollary, any finite-type k-alegbra has finite dimension.

Proposition 15.7. *Let K be a field. Let $p \in k[X_1, \cdots, X_n]$, where* $\deg P > 0$. *Then* $\dim k[X_1, \cdots, X_n]/(P) = n - 1$.

Proof. Exercise to the reader: check that we can assume that P is irreducible. If P is not irreducible, write it as $P = \prod P_i^{n_i}$. Relate the dimension to $\dim k[X_1, \cdots, X_n]/(P_i)$. The dimension of finite union of closed sets is the maximal one.

Assume that P is irreducible and $P \notin k[X_1, \cdots, X_{n-1}]$. If you take the map $k[X_1, \cdots, X_{n-1}] \to A = k[X_1, \cdots, X_n]/(p)$. This an integral ring extension. This map is injective since $P \notin k[X_1, \cdots X_{n-1}]$. This means that $K(X_1, \cdots, X_{n-1}) \to Frac(A)$ is injective, and also algebraic. Thus, In fact, it is a finite extension because of the P. Thus, $trdeg_k K(A) = \dim A = trdeg_k K(X_1, \cdots, X_{n-1}) = n - 1$. This last step uses the next theorem. □

Here's a condition where transcendence degree and Krull dimension coincide:

Theorem 15.8. *Let K field, and A an integral domain, f.t. k-algebra. Then* $\dim A = trdeg_K K(A)$.

Proof. By Noether Normalization, there exist finite integral extension $k[X_1, \cdots, X_n] \to A$. Since the extension is integral, we have $\dim k[X_1, \cdots, X_n] = \dim A = n$. And since the extension is finite, $k(X_1, \cdots, X_n) \to K(A)$ is algebraic extension. Then $trdeg_K K(A) \leq n$. Note that we must have $tredeg_K K(A) \geq n$, because $X_1, \cdots, X_n$ is algebraically indepedent over K. So $trdeg_K K(X_1, \cdots, X_n) \geq n$, so $trdeg_k K(A) \geq n$. Thus $trdeg_k K(A) = n = \dim A$. □

Some chains are better than others. Here are some good ones:

Definition 15.9 (saturated chain)**.** R ring. A saturated chain of prime ideals is a chain that is not a part of a chain with larger length.

Do all the saturated chains have the same length? Is there a saturated chain with length the dimension of ring?

Theorem 15.10. *Let A be an integral domain, finite type k-algebra. Then every saturated chain of prime ideals has length* $\dim A$.

Proof. Proceed by induction on $\dim A$. If $\dim A = 0$, then the claim is trivially true. Now suppose our claim holds for up to $\dim A = n-1$. We show it holds for $\dim A = n$.

Let $0 \subset p_1 \subset \cdots p_m$ be a saturated chain of primes in A. By Noether Normalization, there exist algebraically independent $a_1, \cdots, a_k$ such that $k[a_1, \cdots, a_k] \to A$ is finite integral extension. Note since the extension is integral, we must have $\dim k[a_1, \cdots, a_k] = \dim A = n = k$.

Let $B = k[a_1, \cdots, a_n]$. Consider the chain $0 \subset p_1 \cap B \subset \cdots \subset p_m \cap B$. By incomporability, this remains a chain of length m. Let $f \in p_1 \cap B$ be an irreducible element. Then $(f) \subset B$ is a prime ideal. Then by lying over, we can lift this (f) to a prime ideal p_1' of A that lies over (f). But our chain is saturated, so we must have $p_1' = p_1$, so $(f) = p_1 \cap B$. Then consider the integral extension $B/(f) \to A/p_1$. Furthermore, $\dim B/(f) = \dim A/p_1 = n-1$. The chain $0 \subset p_2/p_1 \subset \cdots \subset p_m/p_1$ is saturated, so has length $n-1$. □

As a corollary:

Proposition 15.11. *if A is an integral domain, finite type k-algebra, and $p \subsetneq A$ prime. Then height + coheight* $= \dim A$.

16. Oct 25: saturated chains, composition series, length of module

Proposition 16.1. *Let A be an integral domain, finite type k-algebra. Let $p \subsetneq A$ be prime ideal. Then $ht(p) + coht(p)$* $= \dim A$.

Proof. Take

$$p_0 \subset \cdots p_n = p = q_0 \subsetneq q_1 \subset \cdots \subset q_r.$$

This gives a saturated chain, so it must have length $\dim A$. □

Another corollary.

Proposition 16.2. *A domain, finite type k-algebra. For every pair of prime ideals $q \subseteq p$, we have $sup\{r | q = p_0 \subset \cdots \subset p_r = p\}$* $= \dim(A/q) - \dim(A/p)$.

Proof. Apply the previous result to p/q in A/q. A/q is integral domain and still finite type K-algebra. □

You can relate all of this to geometry. Let $p \in Speck[X_1, \cdots, X_n]$. You have $\dim V(p) = \dim k[X_1, \cdots, X_n]/(p)$. And $codimV(p) = ht(p)$. We have $\dim + codim =$

As we can see, finite type k-algebras which are domains behave quite nicely.

We're going to start a new section now: composition series/length of modules. Section 24 of Eisenbud. "Artinian rings" in Atiyah-Macdonald.

We have a well-behaved dimension theory. This is a gift of nature; as opposed to dimension theory in topological spaces, it is very ill-behaved. Things like open sets with fractal boundaries are quite pathological.

So to study rings, we can start with studying rings of dimension 0. (This will correspond to points and curves). Then dimension 1 (surfaces, the work of the Italian geometers). Rings of dimension 3 (minimal model program, a big name in this field: Mori). Classifying rings of dimension 3 is a fields-medal worthy work.

Definition 16.3. Let R be a ring, M an R-module. Then M is said to be simple if $M \neq 0$ and M has no submodules other than 0 and M.

Simples modules M are very simple, in the following sense: let $x \in M \setminus \{0\}$. Look at Rx. If $Rx \neq 0$, then $Rx = M$. So in fact, M is just generated by one element.

Now think of the map $R \to M$ which sends an element $r \mapsto rx$. Then this factors through $R/Ann(x) \to M$. So $M \cong R/Ann(x)$. If $Ann(x) \subseteq I$, then $R/I \subseteq R/Ann(x) \cong M$. So either R/I is 0 or M. If $R/I = 0$, then $I = R$, so $Ann(x)$ is maximal. If $R/I = M$, then $I = Ann(x)$. This leads us to:

Proposition 16.4. *M is simple $\iff$ $M \cong R/m$ where m is maximal ideal of R.*

Definition 16.5. Let M be a R-module. A chain of submodules $0 = M_n \subset \cdots \subset M_1 \subset M_0 = M$ is called a **composition series** if M_i/M_{i+1} is simple for every i.

Similar to Jolden-Holder theorem in group theory (http://www.math.brown.edu/dabramov/MA/f1516/251/JordanHolder.pdf), in any other composition series, the integer n will be the same. The proof is exactly the same in Jordan-Holder.

We can use this to define a notion of "length" of a module.

Definition 16.6. The length of M $\ell(M) := \{$length of composition series if it exists$\}$

Example 16.7. $M = 0$, the length is 0. If $M = R/m$ for maximal ideal m, then length is 1.

Example 16.8. $R = k$ field. M a k-vector space. Then the length of M is $\dim M$ as a vector space.

Lemma 16.9. *Let $0 \to M \to N \to^{\pi} P \to 0$ be an exact sequence of R-modules.*

- *Then $\ell(N) < \infty$ if $\ell(M), \ell(P) < \infty$. If they're all finite, then $\ell(N) = \ell(M) + \ell(P)$.*
- *If $0 \to M_1 \to \cdots \to M_n \to 0$ is an exact sequence, $\ell(M_i) < \infty$ for all i, then $\sum_{i=1}^{n}(-1)^i \ell(M_i) \to 0$.*

Proof. Let's prove (1). Suppose we have a composition series $N_0 \subset \cdots \subset N_k = N$ for N. Both $N_0 \cap M \cdots N_k \cap M$ and $\pi(N_0) \subset \cdots \subset \pi(N_k)$ can be simplified into composition series for M, P respectively. This is because $N_i \cap M/N_{i+1} \cap M$ is a submodule of N_i/N_{i+1}. Since N_i/N_{i+1} is simple, either $N_i \cap M/N_{i+1} \cap M = 0$ or $N_i \cap M/N_{i+1} \cap M = N_i/N_{i+1}$. Also, if $\pi(N_i)/\pi(N_{i+1})$ is nonzero, then its preimage would be a submodule of N_i/N_{i+1}, which means it must be the entirety of N_i/N_{i+1}. Thus, for both filtrations, at each step either the quotient remains the same, or it becomes zero. The claim is that if we lose one step in one of the filtrations, then it is accounted for in the other filtration, so that indeed $\ell(M) + \ell(P) = \ell(N)$.

First, suppose $N_i \cap M = N_{i+1} \cap M$. Consider the diagram

$$\begin{tikzcd}
 & & 0 & 0 \\
 & & N_i/N_{i+1} \arrow[r] \arrow[u] & \pi(N_i)/\pi(N_{i+1}) \arrow[u] \\
0 \arrow[r] & N_i \cap M \arrow[r] & N_i \arrow[r] \arrow[u] & \pi(N_i) \arrow[u] \\
0 \arrow[r] & N_{i+1} \cap M \arrow[r] \arrow[u] & N_{i+1} \arrow[r] \arrow[u] & \pi(N_{i+1}) \arrow[u]
\end{tikzcd}$$

We'd like to show that $N_i/N_{i+1} \cong \pi(N_i)/\pi(N_{i+1})$. Surjectivity is clear. Now we show injectivity. Suppose $[x] \in N_i/N_{i+1}$ s.t. $[x]$ maps to $0 \in \pi(N_i)/\pi(N_{i+1})$. This means we have $x \in N_i$ such that x maps to $\pi(x) \in \pi(N_i)$, which is also in $\pi(N_{i+1})$. Note that $N_{i+1} \to \pi(N_{i+1})$ is surjective, so there exist $y \in N_{i+1}$ s.t. $y \mapsto \pi(x)$. Then consider $x - y \in N_i$. This maps to $[x] \in N_i/N_{i+1}$. Furthermore, $x-y \mapsto 0 \in \pi(N_i)$. Thus, by exactness, $x-y \in N_i \cap M$. Then $x-y \in N_{i+1} \cap M \implies x - y \in N_{i+1}$. This implies that $[x] = 0$.

Now we show $\pi(N_i)/\pi(N_{i+1}) = 0 \implies N_i \cap M/N_{i+1} \cap M$ simple. Consider the diagram

$$\begin{tikzcd}
 & 0 & 0 & & \\
 & N_i \cap M/N_{i+1} \cap M \arrow[r] \arrow[u] & N_i/N_{i+1} \arrow[u] & 0 & \\
0 \arrow[r] & N_i \cap M \arrow[r] \arrow[u] & N_i \arrow[r] \arrow[u] & \pi(N_i) \arrow[r] \arrow[u] & 0 \\
0 \arrow[r] & N_{i+1} \cap M \arrow[r] \arrow[u] & N_{i+1} \arrow[r] \arrow[u] & \pi(N_{i+1}) \arrow[r] \arrow[u, "="] & 0
\end{tikzcd}$$

We claim that $N_i \cap M/N_{i+1} \cap M \cong N_i/N_{i+1}$. Note we have an obvious map $N_i \cap M/N_{i+1} \cap M \to N_i/N_{i+1}$. This map is injective, since if there is $x \in N_i \cap M$ s.t. $[x] \mapsto 0 \in N_i/N_{i+1}$, then $x \in N_i$ is in N_{i+1}. Then since $\pi(x) = 0 \in \pi(N_i)$, this means $x \in N_{i+1} \cap M$. This map is also surjective. Suppose $x \in N_i$. We want an element of $N_i \cap M/N_{i+1} \cap M$ that maps to $[x] \in N_i/N_{i+1}$. Note $x \mapsto \pi(x) \in \pi(N_i)$, so there is $\pi(x) \in \pi(N_{i+1})$, so there exist $y \in N_{i+1}$ s.t. $y \mapsto \pi(x)$ by surjectivity. Then $x - y \mapsto 0 \in \pi(N_i)$, so $x - y \in N_i \cap M$. But this means $[x - y] \mapsto [x]$, as desired.

These facts show that $\ell(N) = \ell(M) + \ell(P)$.

For item (2), take inspiration from the rank nullity theorem of vector spaces. □

Definition 16.10. A ring R is **Artinian** if the ideals satisfying the descending chain condition (DCC): for $\cdots \subseteq I_n \subseteq I_{n_1} \subseteq \cdots \subseteq I_0$, there exist n_0 s.t. $I_n = I_{n_0}$ for all $n \geq n_0$. Same definition for R-module. M is artinian $\iff$ M has DCC.

Example 16.11. $\mathbb{Z}$ is Noetherian but not Artinian.

$k[X_1, \cdots, X_n]/(X_1, \cdots, X_n)^k$ is Artinian. Later on we'll develop ways of proving generally whether rings are Artinian.

Also, $\prod_{i=1}^r k_i$, k_i is a field is Artinian, because you have a finite set of ideals.

Lemma 16.12. *If R is an artinian domain, then R is a field.*

Proof. If $a \in R$, then consider $(a) \supseteq (a^2) \supseteq (a^3) \supseteq \cdots$. Since R is artinian, then $a^n = ma^{n+1}$ for some $m \in R$. So $a^n(1 - ma) = 0$. Integral domain implies $1 - ma = 0$. So a is a unit. □

17. Oct 27: Artinian rings

Lemma 17.1. *Let R be Artinian. Then R all prime ideals are maximal. Furthermore, R has only finitely many maximal ideals.*

Proof. Let $p \subseteq R$ be a prime. Then R/p is Artinian, but also a domain, so it is a field $\implies$ p maximal.

To show that R has finitely many maximal ideals, consider the chain

$$m_1 \supseteq m_1 m_2 \supseteq m_1 m_2 m_3 \supseteq \cdots$$

where m_i are maximal ideals of R. Since R is Artinian, the chain stabilizes at some index k. So $m_1 \cdots m_{k+1} = m_1 \cdots m_k$. Note $m_1 \cdots m_{k+1} \subseteq m_{k+1}$. So $m_1 \cdots m_k \subseteq m_{k+1}$. Then we claim that $m_i \subseteq m_{k+1}$ for some $1 \leq i \leq k$. Suppose not. Then there would exist $c_i \in m_i \setminus m_{k+1}$. Then $c_1 \cdots c_k \notin m_{k+1}$, but $m_1 \cdots m_k \subseteq m_{k+1}$ implies a contradiction. So $m_i \subseteq m_{k+1}$ for some i, and by maximality, this implies $m_i = m_{k+1}$. Then the set of maximal ideals of R is $\{m_1, \cdots, m_k\}$. □

Lemma 17.2. *Let M be an R-module. Then $\ell(M) < \infty \iff M$ is Noetherian and Artinian.*

Proof. Let's suppose that $\ell(M) < \infty$. So we have a composition series $0 = M_n \subset \cdots \subset M_1 \subset M_0 = M$, s.t. M_i/M_{i+1} is simple. Note that M_{n-1} is simple, so it is $\cong R/m$ where m is a maximal ideal. So M_{n-1} is a field, which implies it is Noetherian and Artinian. We can prove inductively that M_i is both Artinian and Noetherian, when knowing that M_{i+1} is Artinian and Noetherian. Consider the SES

$$0 \to M_{i+1} \to M_i \to M_i/M_{i+1} \to 0.$$

We have that M_{i+1} and $M_i/M_{i+1} \cong R/m_i$ are both Artinian and Noetherian. This implies that M_i is Noetherian and Artinian.

Now suppose that M is Noetherian and Artinian. We can build a sequence of quotients $0 = M_0 \subseteq M_1 \subseteq M_2 \subseteq \cdots$ s.t. $M_i/M_{i-1} \cong R/p_i$ for some prime p_i. Since M is Noetherian and Artinian, this implies M_i and thus M_i/M_{i-1} is Noetherian + Artinian. But this means that M_i/M_{i-1} is a field, so p_i is maximal. Thus, M_i/M_{i-1} is simple. Since M is Noetherian, this chain stabilizes, so we get a finite composition series. Thus, $\ell(M) < \infty$.

□

Proposition 17.3. *Let R be a Noetherian ring, M a f.g. R-module. TFAE:*

- *$\ell(M) < \infty$ ($\iff$ M artinian + noetherian)*
- *Every prime $p \in Ass(M)$ is maximal*
- *Every prime $p \in Supp(M)$ is maximal.*

Proof. We show (1) $\implies$ (2). There exists a composition series $0 = M_0 \subset M_1 \subset \cdots \subset M_n = M$. Every $M_i/M_{i-1} \cong R/m_i$, m_i is maximal. Then $Ass(M) \subseteq \{m_1, \cdots, m_n\}$. This follows from the fact that if you have an exact sequence

$$0 \to N \to M \to P \to 0$$

then $Ass(M) \subseteq Ass(N) \cup Ass(P)$. Thus, every element of $Ass(M)$ is maximal.

Now we show (2) $\implies$ (3). Let $p \in Supp(M)$. (As a reminder this means $M_p \neq 0$). We proved before that the set of minimal primes of $Supp(M)$ = set of minimal primes of $Ass(M)$. Then all the minimal primes of $Supp(M)$ are maximal. Which implies that, in fact, all the primes in $Supp(M)$ are maximal.

Now we show (3) $\implies$ (1). Look at the proof that R noetherian, M f.g. R-module $\implies$ finitely many associated primes. You'll see that we can construct a filtration by $0 = M_0 \subset M_1 \cdots \subseteq M_n = M$, where $M_i/M_{i-1} \cong R/p_i$ is prime ideal. This is because M is Noetherian module, so it has finitely many associated primes.

We claim for every p_i, $M_{p_i} \neq 0$, so $p_i \in Supp(M)$. To see this, note that $(M_i)_{p_i} \subseteq (M)_{p_i}$. Also, $(M_i)_{p_i}/(M_{i+1})_{p_i} = (M_i/M_{i+1})_{p_i} = (R/p_i)_{p_i}$ = nonzero field. Thus, $(M_i)_{p_i}/(M_{i+1})_{p_i}$ is nonzero, so M_{p_i} is nonzero. Thus, $p_i \in Supp(M) \implies p_i$ is maximal. Then the filtration we gave is in fact a composition series. So $\ell(M) < \infty$. □

An easy corollary is the following:

Proposition 17.4. *R noetherian, M f.g. R-module. If $\ell(M) < \infty$, then $Ass(M) = Supp(M)$.*

Proof. All the elements of $Ass(M)$ and $Supp(M)$ are maximal. The minimal elements coincide. So they're equal. □

Theorem 17.5. *Let R be a noetherian ring. Then TFAE:*

- *R is artinian.*
- *Every prime in R is maximal.*

Proof. So (1) $\implies$ (2) immediately. For (2) $\implies$ (1), we're assuming every prime in R is maximal. By the previous proposition, every prime $p \in Supp(R)$ is maximal. Thus, $\ell(R)$ as an R-module is finite. Thus, R is artinian. □

Lemma 17.6. *If R is Artinian, then $\sqrt{0}$ is nilpotent.*

Proof. There exist a k s.t. $\sqrt{(0)}^{k+1} = (\sqrt{(0)})^k$, since R is artinian.

If $(\sqrt{(0)})^{k+1} = 0$, we're done, for minimal $k+1$. Otherwise, let $F = \{I \subseteq R | I(\sqrt{(0)})^k \neq 0\}$. So F is nonempty. If R is artinian, then F has minimal element I. So $I(\sqrt{0})^k \neq 0$. So there exist $r \in I$ s.t. $r(\sqrt{0})^k \neq 0$. By minimality, $I = (r)$. But $r\sqrt{0}\sqrt{0}^k = r\sqrt{0}^{k+1} = r\sqrt{0}^k \neq 0$, so $r\sqrt{0} \in F$. But then $r\sqrt{0} \subseteq (r)$. Then $(r) = (r)\sqrt{0}^k$. So there is $s \in \sqrt{0}^k$, so $r = rs = rs^n$. But $s \in \sqrt{0}^k$ so $s^{n_0} = 0$ for some n_0. So $r = rs^{n_0} = 0 \implies r = 0$, contradiction. So F is empty, so $\sqrt{0}^k = 0$. □

Theorem 17.7. *Let R be a ring. R artinian $\implies \ell(R) < \infty$.*

Proof. For the reverse direction, if $\ell(R) < \infty$, then previous work tells us R is artinian and noetherian.

Now let R be Artinian. So all primes are maximal, and there are finitely many maximals, call them $m_1, \cdots m_n$. Note $m_1 \cdots m_n \subseteq m_1 \cap \cdots \cap m_n = \sqrt{(0)}$. By the lemma, there exist k such that $(\sqrt{(0)})^k = 0$. So $(m_1 \cdots m_n)^k = 0$.

So we filter by

$$0 = (m_1 \cdots m_n)^k \subset \cdots \subset m_1^k m_2^2 \subset m_1^k m_2 \subset m_1^k \subset \cdots \subset m_1^2 \subset m_1 \subset R$$

At each step, $M_\ell/M_{\ell-1}$ is a $R/m_{k\ell}$-module, and $m_{k\ell}$ is a maximal ideal of R. This is an Artinian $R/m_{k\ell}$-module. From the problem set, any Artinian k-vector space has finite dimension. We know $\ell_R(M_\ell/M_{\ell-1}) = \ell_{R/m_{k\ell}}(M/M_{\ell-1}) = \dim(M_\ell/M_{\ell-1}) < \infty$. Get SES GO BACK HERE □

Theorem 17.8. *A ring is Artinian* $\iff$ *noetherian and* $\dim(R) = 0$.

Theorem 17.9.

18. Nov 1: Krull's PID theorem, Hilbert function

At some point we proved something like:

Theorem 18.1. $P \in k[X_1, \cdots, X_n]$ *s.t.* $\deg P > 0$*, then* $\dim k[X_1, \cdots, X_n]/(p) = n - 1$.

Something about irreducible components. Codimension. the next theorem tells us something about irreducible components being at most codimension 1 in geometry.

We're going to talk about Krull's principal ideal theorem (Hampt ideal satz) today. This is section 8.2.1 in Eisenbud.

Some useful notation before we proceed: suppose I, J two ideals of R. Then $(I : J) = \{x \in R | xJ \subseteq I\}$.

Theorem 18.2 (Krull's PID theorem)**.** *Let R be a Noetherian ring. Let $a \in R$. For every minimal prime ideal p containing (a), we have $ht(p) \leq 1$.*

Proof. Let p be a minimal prime ideal containing a. Assume FSOC that we have a chain $p_0 \subset p_1 \subset p$. So we have a proper chain of height at least 2. If we replace R by R/p_0, we can assume that R is integral. This is harmless, so assume R is integral. Furthermore, if we localize at prime p, it's harmless again. Since the chain $p_0 \subset p_1 \subset p$ is all contained in p. So assume that R is local. So p is the unique maximal ideal of R.

The ring $R/(a)$ is Noetherian and all primes containing (a).. well p is minimal of containing a, but it is a maximal. So $R/(a)$ has only one prime, and its maximal, and the maximal ideal is p. So $R/(a)$ is Artinian.

Let $b \in p_1$, for $n \geq 1$. Let $M_n = R/(a^n)$. These are all $R/(a)$-modules of finite length. Now consider the map

$$m_b : M_n \to M_n$$

where $m_b : x \mapsto bx$. We have $\ker m_b = \{x \in R | bx \in (a^n)\}/(a^n)$. And $M_n/Im(m_b) = \frac{R/(a^n)}{(b)} = \frac{R}{(a^n b)}$. We have $\ell(\ker m_b) = \ell(R/(a^n)) - \ell(Im(m_b))$, which comes from the exact sequence

$$0 \to \ker(m_b) \to M_n \to Im(m_b) \to 0.$$

We also have $\ell(M_n) = \ell(Im(m_b)) + \ell(R/(a^n, b))$. So $\ell(\ker(m_b)) = \ell(R/(a^n, b))$. If $\overline{x} \in \ker(m_b)$, then there exist $y \in R$ s.t. $xb = ya^n = ba^n y_0$.

Then we define a map

$$\ker(m_b) \to \frac{((b):(a^n))}{(b)}$$

where $\overline{x} \mapsto \overline{y}$. Note $\ker(m_b) = \frac{((a^n):b)}{(a^n)}$. This map is an isomorphism. GO BACK HERE AND PROVE THAT.

The sequence of ideals $((b):(a^n)) \subseteq ((b):(a^{n+1}))$ is increasing. Because $a^n x \in (b) \implies a^{n+1}x \in (b)$. Since R is Noetherian, this chain stabilizes at some index n_0. So for every $n \geq n_0$, we have $((b):(a^n)) = ((b):(a^{n+1}))$.

In particular, $\frac{((a^n):b)}{(a^n)} \cong \frac{((a^{n+1}):b)}{(a^{n+1})}$, so they have the same length.

Then $R/(a^n, b)$ and $R/(a^{n+1}, b)$ have the same length. We have a SES

$$0 \to \frac{(a^n, b)}{(a^{n+1}, b)} \to \frac{R}{(a^{n+1}, b)} \to \frac{R}{(a^n, b)} \to 0$$

So $\ell(\frac{(a^n,b)}{(a^{n+1},b)}) = 0$, so $(a^n, b) = (a^{n+1}, b)$. So $a^n = xa^{n+1} + yb$ for some $x, y \in R$. Then $a^n(1 - xa) = yb$. Then $(a^n) \in (b) \subseteq p_1 \subset p$. Then $(a) \subseteq p_1 \subset p$. This contradicts the minimality of p. □

If you assume R is integral, then $ht(p) = 1$ or $ht(p) = 0$, in which case $p = 0$. If you don't assume R is integral, something about nilpotence.

We'll talk about graded rings and modules now. Section 1.5 of Eisenbud.

Definition 18.3. A $\mathbb{N}$-graded ring S is a ring together with a family of subgroups $S_d \subseteq S$, $d \geq 0$, s.t. $S = \oplus_{d\geq 0} S_d$ and $S_d S_e \subseteq S_{d+e}$.

Note S_0 is a subring of S, and S_d is a S_0-module $\forall d$. The irrelevant ideal is $S_+ = \oplus_{d>0} S_d$.

The most famous example is:

Example 18.4. $S = k[X_1, \cdots, X_n]$, where S_d is the subgroup of homogenous polynomials of degree d.

Example 18.5. $k[X_1, \cdots, X_n]/I$, where I is a homogenous ideal $I = \oplus_d I \cap S_d$ (i.e I is an ideal generated by homogenous elements). Then $k[X_1, \cdots, X_n]/I$ has a natural grading.

Example 18.6. Let $I \subseteq R$ be an ideal. Let $S = \oplus_{k\geq 0} I^k$, where $I^0 = R$. This is called the blow-up algebra. This is useful for resolution of singularities.

Definition 18.7 (Graded Modules)**.** Let S be a graded ring. A graded module is a S-module M s.t. $M = \oplus_{d\geq 0} M_d$, $M_d \subseteq M$ subgroup and $S_e M_d \subseteq M_{e+d}$.

In particular, M_d is a S_0-module. An element $m \in M_d$ is said homogenous of degree d.

Our goal is to define hilbert functions, which measures the dimension of M_d as S_0-vector spaces. Prove that the sequences of dimension has an almost polynomial behavior. Has a nice interpretation in algebraic geometry.

Definition 18.8. A polynomial-like function is a function $f : \mathbb{N} \to \mathbb{Q}$ s.t. there exist $g \in \mathbb{Q}[X]$ s.t. $f(n) = g(n)$ for n large enough. Define $\deg(f) = \deg(g)$.

Lemma 18.9. *Let $f : \mathbb{N} \to \mathbb{Q}$. Then f is polynomial-like of degree $r \iff \Delta f$ is polynomial like of degree $r - 1$. We define $\Delta f(n) = f(n+1) - f(n)$.*

Proof. We have the identity $\binom{n}{r} = \frac{n(n-1)\cdots(n-r+1)}{r!} = \frac{n^r}{r!} + \cdots$. Any $g \in \mathbb{Q}[x]$ can be written as $g(n) = a_0\binom{n}{r} + a_1\binom{n}{r-1} + \cdots + a_{r-1}\binom{n}{1} + a_r$ for some $a_i \in \mathbb{Q}$. Then $\Delta g(n) = a_0 \Delta\binom{n}{r} + \cdots + a_r$. Note $\Delta\binom{n}{r} = \binom{n}{r-1}$. So if f is polynomial-like of degree r, then Δf is polynomial like of degree $r-1$.

Now we show the converse. Assume Δf is polynomial like of degree $r-1$. Then $\Delta f(n) = g(n)$ for some polynomial g of degree $r-1$, for n sufficiently large.

We can write $g(x) = a_0\binom{x}{r-1} + \cdots + a_{r-1}$. Then we can define $h(x) = a_0\binom{x}{r} + \cdots + a_{r-1}\binom{x}{1}$.

Then we have $\Delta h(n) = g(n) = \Delta f(n)$ for $n >> 0$. Then $\Delta(h-f)(n) = 0$ for $n >> 0$. So $h(n+1) - f(n+1) = h(n) - f(n)$ for $n > n_0$. So $h(n) - f(n) = h(n_0) - f(n_0)$. Then $f(n) = h(n) - h(n_0) + f(n_0)$. Then f is polynomial-like of degree r. □

We're going to apply this to study the behavior of a specific type of object(s):

Theorem 18.10 (Hilbert Polynomials)**.** *Let $S = \oplus_{d\geq 0} S_d$ be a graded ring with $S_0 = k$ a field, s.t. S is a f.g. k-algebra, generated by n elements in S_1.*

Let M be a f.g. graded S-module, and define $h_M(n) = \dim_k M_n$, $n \in \mathbb{N}$. Then h_M is polynomial like of degree $\leq r-1$.

Definition 18.11 (Hilbert function)**.** The function h_M is called the Hilbert function of M, where $h_M(n) = P(n)$ for $n >> 0$. Then P is called the Hilbert polynomial of M.

Example 18.12. Let $S = k[X_1, \cdots, X_n]$, $M = S$. Then $h_S(n) = \dim k[X_1, \cdots, X_n]_d = \binom{n+d-1}{d}$.

19. Nov 3: hilbert functions, artin-rees

Recall from last time how we defined hilbert functions/polynomials.

Let $S = \oplus_{n\geq 0} S_n$ graded ring that is a k-algebra, where S_0 is a field, generated in degree 1 by r elements.

Let M be a f.g. S-module. Then $h_M(n) = \dim_k M_n$. Then h_M is polynomial-like of degree $\leq r-1$.

Proof. Induct on r. If $r = 0$. Then $S = S_0$. M is a f.g. module over k. So there exist $m_1, \cdots, m_\ell \in M$ generators, $m_i \in M_{n_i}$. If $n = \max(n_i)$, then $SM_n \subseteq M_n$, since $S = S_0$. Then $M_{n+1} = 0$. Note this is because M is a graded module, and we only have linear combination of elements. Then since the dimensions all goto zero, we see that $h_M(n)$ is like the zero polynomial. This completes the base step.

Now assume $r \geq 1$. Let S be generated in degree 1 by $a_1, \cdots, a_r$. Let $\phi_r : M \to M$ be defined by $x \mapsto a_r x$. Let $C = M/a_r M = M/Im(\phi_r)$. And $K = \ker(\phi_r)$. Notice $\phi_r(M_n) \subseteq M_{n+1}$. Then we get graded S-modules

$$K = \oplus_{n\geq 0} K_n, C = \oplus_{n\geq 0} C_n.$$

If you look at the exact sequence

$$0 \to K_n \to M_n \to M_{n+1} \to C_n \to 0.$$

as vector spaces, then

$$\dim_k(K_n) - \dim_k(M_n) + \dim_k M_{n+1} - \dim_k C_n = 0.$$

Which is true $\iff$ $\delta h_M(n) = h_C(n) - h_k(n)$.

But $a_r K = 0$, and $a_r C = 0$. Hence, K and C are $S/\langle a_r\rangle$-modules. Let $S/\langle a_r = \widetilde{S}$. This is naturally graded as $\widetilde{S} \oplus_{d\geq 0} \widetilde{S}_d$, where $\widetilde{S_0} = k$, which is generated in degree 1 by $r-1$ elements.

By induction, $h_C(n)$ and $h_K(n)$ are polynomial like of degree $\leq r-2$. Then $\delta h_M(n)$ is polynomial like of degree r_2, so $h_M(n)$ is polynomial like of degree $r-1$. □

As a corollary, we have

Proposition 19.1. *Let $S = \oplus_{n\geq 0} S_n$ be a graded ring, and S_0 artinian. Furthermore, S f.g. over S_0 by elements in degree 1. Let M be a f.g. graded S-module. And $h_M(n) = \ell_{S_0}(M_n)$. Then h_M is polynomial-like.*

Proof. The proof is analagous to the above, except you replace dimension with length. □

Now we'll talk about Filtrations and Artin-Reese lemma. Section 5 of Eisenbud.

Definition 19.2. Let R be a ring. A descending multiplicative filtration of R is a sequence of ideals $R = I_0 \supseteq I_1 \supseteq \cdots$, s.t. $I_n I_m \subseteq I_{n+m}$.

Example 19.3 (I-adic filtration)**.** Let $I \subseteq R$ be an ideal. Let the filtration be defined by $I_k = (I)^k$, and let $I^0 := R$.

Definition 19.4. Let R be a ring with a filtration. Let M be an R-module. We say a filtration

$$M = M_0 \supseteq M_1 \supseteq \cdots$$

on M is compatible with a filtration

$$R = I_0 \supseteq I_1 \supseteq I_2 \supseteq \cdots$$

on R if $I_k M_\ell \subseteq M_{k+\ell}$.

If the filtration on R is given by an ideal I (so it is an I-adic filtration), then the filtration on M is called an **I-filtration**. In other words, $IM_n \subseteq M_{n+1}$ $\forall n$.

An I-filtration of M is called **I-stable** if in addition $IM_n = M_{n+1}$ for $n >> 0$.

Example 19.5. If the filtration on M is given by $M_n = I^n M$, then this is I-stable.

We want to prove the following theorem:

Theorem 19.6 (Artin-Rees)**.** *Let R be a noetherian ring, and M f.g. R-module. Let $M' \subseteq M$ be a submodule (which must be finitely generated). Let $M = M_0 \supseteq M_1 \supseteq \cdots$ be an I-stable filtration. Then the induced filtration on M' is also I-stable. In other words, there exist n_0, s.t. for all $k > 0$, $M' \cap M_{k+n} = I^k(M' \cap M_{n_0})$.*

Before we prove this, we need to set up some machinery.

Let $I \subseteq R$ be an ideal. An associated graded ring is

$$gr_I(R) = R/I \oplus I/I^2 \oplus I^2/I^3 \oplus \cdots = \bigoplus_{k\geq 0} I^k/I^{k+1}.$$

And if $F = (I_n)$ is any filtration of R, then we can form the associated graded

$$gr_F(R) = \oplus_{n\geq 0} I_n/I_{n+1}.$$

We see that $gr_I(R)$ is a graded ring, where $I^n/I^{n+1} \times I^m/I^{m+1} \to I^{n+m}/I^{n+m+1}$.

Let M be an R-module with an I-filtration $F = \{M_n\}$. Then

$$gr_F(M) = \oplus M_i/M_{i+1}$$

is a graded $gr_I R$-module.

If $I = (a_1, \cdots, a_r)$, then $gr_I R$ is generated in degree 1 by $\overline{a_1}, \cdots, \overline{a_r}$ over $(gr_I R)_0 = R/I$.

Proposition 19.7. *Let $I \subseteq R$ be an ideal. M f.g. R-module. Let $F = \{M_n\}$ be a filtration on M. Assume that F is a stable I-filtration by f.g. submodules (i.e. every M_i is f.g. over R). Then $gr_F M$ is a f.g. module over $gr_I R$.*

Proof. We know that $IM_i = M_{i+1}$ for $\forall i \geq n_0$ for some n_0, since the filtration is I-stable. Then $(I/I^2)M_i/M_{i+1} = M_{i+1}/M_{i+2}$ for $i \geq n_0$. Or more generally, $(I^k/I^{k+1})(M_{n_0}/M_{n_0+1}) = M_{n_0+k}/M_{n_0+k+1}$.

Note we can write

$$gr_F M = \oplus_{i \leq n_0} M_i/M_{i+1} \oplus_{i > n_0} M_i/M_{i+1}.$$

Since M_i is f.g. over R, let $a_1^i, \cdots, a_{n_i}^i$ be a set of generators. Then $\{\overline{a}_j^i\}$ is a set of generators of $\oplus_{i \leq n_0} M_i/M_{i+1}$ over R/I.

Hence they generate $gr_F M$ as $gr_I R$. □

Definition 19.8. Let R be a ring, $I \subseteq R$ an ideal. The blow-up algebra $Bl_I(R) = R \oplus I \oplus I^2 \oplus \cdots$. If you take $Bl_I(R)/\langle I \rangle = gr_I R$, since $\langle I \rangle = I \oplus I^2 \oplus \cdots$.

If M is an R-module with an I-filtration, $F = \{M_n\}$, then the blow-up $B_F M = \oplus M_i$. This is naturally a graded $Bl_I R$-module.

Proposition 19.9. *Let $I \subseteq R$ be an ideal, M f.g. R-module with an I-filtration $F = (M_n)$ where each M_i is f.g R-module. Then F is I-stable $\iff$ $Bl_F M$ is a f.g. module over $Bl_I R$.*

Proof. Let's assume that F is I-stable. Then $IM_n = M_{n+1}$ for $n \geq n_0$. Then take generators of $M_0, \cdots, M_{n_0}$. They generate $Bl_F(M)$ over $Bl_I(R)$.

Now assume that $Bl_F(M)$ is a f.g. $BL_I(R)$-module. Take generators $m_1, \cdots, m_k$ in $M_0, \cdots, M_{n_0}$. Let $n \geq n_0$. Then for $x \in M_{n+1}$, we can write $x = \sum_k \mu_k m_{ik}$. Note $\deg m_{ik} = d_k \leq n_0$. And we must have $\mu_k \in I^{n+1-d_k}$. And we can write $\mu_k = \sum_j v_j w_j$, where $v_j \in I, w_j \in I^{n-d_k}$.

So $x = \sum_{j,k} v_j w_j m_{ik}$, but we know $w_j m_{ik} \in M_n$. So $v_j w_j m_{ik} \in IM_n$. So $IM_n = M_{n+1}$, so F is I-stable. □

Now we will prove the Artin-Rees lemma.

Theorem 19.10 (Artin-Rees)**.** *Let R be a noetherian ring, and M f.g. R-module. Let $M' \subseteq M$ be a submodule (which must be finitely generated). Let $M = M_0 \supseteq M_1 \supseteq \cdots$ be an I-stable filtration. Then the induced filtration on M' is also I-stable. In other words, there exist n_0, s.t. for all $k > 0$, $M' \cap M_{k+n} = I^k(M' \cap M_{n_0})$.*

Proof. Let F' filtration on M', where $M' = M'_0 \supseteq M'_1 \supseteq \cdots$ where $M'_n = M' \cap M_n$.

Then $Bl_{F'}(M')$ is a sub $Bl_I R$-module of $Bl_F M$. Since F is I-stable, $BL_F M$ is a f.g. $BL_I R$-module.

Since R is Noetherian, $BL_I R$ is finite type R-algebra. So $Bl_I R$ is Noetherian. This implies that $Bl_{F'}(M')$ is finitely generated $Bl_I(R)$-module. This implies that F' is I-stable filtration on M'. □

Let (R, m) be a Noetherian local ring.

Definition 19.11. An ideal I of R is a definition ideal if

$$m^n \subseteq I \subseteq m$$

for some $n \geq 1$.

20. Nov 8: hilbert-samuel, chevalley dimension, Dimension theorem

Definition 20.1. Let (R, m) be a local Noetherian ring. An ideal of definition $I \subseteq R$ is an ideal s.t. $m^k \subseteq I \subseteq m$ for some k.

Proposition 20.2. *Let $I \subseteq R$ be an ideal of definition for local Noetherian (R, m). Then R/I is artinian.*

Proof. Note R/I is Noetherian. The prime ideals of R/I correspond to those prime ideals of R containing I, which contain m^k. This implies they contain m, which is maximal. Thus, there is only one prime ideal of R/I, and it is maximal. Since R/I is Noetherian and all of its prime ideals are maximal, R/I is Artinian. □

Before we define the hilbert-samuel function, we need to note a few facts:

Proposition 20.3. *Let $I \subseteq R$ be an ideal of definition of local Noetherian (R, m). Then M/I^kM and $I^{k-1}M/I^kM$ are f.g. R/I^k-modules. Thus, they are Artinian and Noetherian.*

Proof. Note M/I^kM and $I^{k-1}M/I^kM$ both inherit R/I^k-module structures. M/I^kM is clearly finitely generated. $I^{k-1}M$ is finitely generated since M is Noetherian, so I^{k-1}/I^kM is finitely generated. Note I^k is an ideal of definition,so R/I^k is Artinian. Thus, both M/I^kM and $I^{k-1}M/I^kM$ are Artinian (and Noetherian). □

Note this implies that $\ell(M/I^kM)$ and $\ell(I^{k-1}M/I^kM)$ are finite. We now define the Hilbert-Samuel function.

Definition 20.4. Let I be an ideal of definition of local Noetherian (R, m). Let M be f.g. R-module. Then $S^I_M(n) = \ell(M/I^nM)$.

Note $S^I_M(n) < \infty$ since M/I^nM is both Noetherian and Artinian. Using our knowledge of hilbert functions, we can say something about the behavior of hilbert-samuel functions:

Proposition 20.5. *Let I be an ideal of definition, (R, m) local Noetherian, M f.g. R-module. Let r be the number of generators of I. Then S^I_M is polynomial like of degree $\leq r$.*

Proof. Note we have a SES

$$0 \to I^nM/I^{n+1}M \to M/I^{n+1}M \to M/I^nM \to 0.$$

Since the lengths are all finite, we have $\ell(M/I^{n+1}M) - \ell(M/I^nM) = \ell(I^nM/I^{n+1}M)$. So $\Delta S^I_M(n) = \ell(I^nM/I^{n+1}M)$. If we denote F to be the filtration of M via $M_n := I^nM$, then $gr_FM = \oplus I^nM/I^{n+1}M$ is a graded gr_IR-module. Note gr_IR is finitely generated in degree 1. Furthermore, $(gr_IR)_0 = R/I$ is Artinian. Thus, the hilbert functionon of gr_FM, which is $h_{gr_FM}(n) = \ell(I^nM/I^{n+1}M)$ is polynomial like of degree $\leq r - 1$. Thus, $S^I_M(n)$ is polynomial like of degree $\leq r$. □

Proposition 20.6. *The degree of S^I_M depends only on M, and not on I. Denote the degree of M as $d(M) := \deg S^I_M$.*

Proof. There exist k s.t. $m^k \subseteq I \subseteq m$. Then $m^{kn} \subseteq I^n \subseteq m^n$. Then $S^m_M(kn) \geq S^I_M(n) \geq S^m_M(n)$. As $n \to \infty$, the degrees of these tend to $k^{\deg S^m_M} n^{\deg S^m_M} \leq n^{\deg S^I_M} \leq n^{\deg S^m_M}$. This shows that $\deg S^I_m = \deg S^m_M$. □

Theorem 20.7. *Let I be an ideal of definition of local Noetherian (R, m). Let*

$$0 \to M_1 \to M \to M_2 \to 0$$

be a SES of f.g R-modules. Then $S^I_{M_1}(n)+S^I_{M_2}(n) = S^I_M(n)+R(n)$ for some residue function $R(n)$. The claim is that $R(n)$ is polynomial like of degree $< \deg S^I_M$, where the polynomial has positive leading coefficient.

Proof. Note we have SES

$$0 \to M_1 \cap I^n M/I^n M_1 \to M_1/I^n M_1 \to M/I^n M \to M_2/I^n M_2 \to 0.$$

Then we find that $S^I_{M_1}(n) + S^I_{M_2}(n) = S^I_M(n) + \ell(M_1 \cap I^n M/I^n M_1)$. Let $R(n) = \ell(M_1 \cap I^n M/I^n M_1)$.

Note we can give M a filtration via $M_n := I^n M$. This is an I-stable filtration of f.g submodules, since M is noetherian. Furthermore, $M_1 \subset M$ is a f.g. submodule. Then by Artin-Rees lemma, the induced filtration on M_1, namely $M_1 \cap I^n M$, is I-stable. Then there exist $m \geq 0$ s.t. for all $n \geq m$, we have $M_1 \cap I^n M = I^{n-m}(M_1 \cap I^m M)$. This implies that we have an injection

$$M_1 \cap I^n M/I^n M_1 \hookrightarrow I^{n-m} M_1/I^n M_1.$$

Then $R(n) = \ell(M_1 \cap I^n M/I^n M_1) \leq \ell(I^{n-m} M_1/I^n M_1)$. Note we have SES

$$0 \to I^{n-m} M_1/I^n M_1 \to M_1/I^n M_1 \to M_1/I^{n-m} M_1 \to 0.$$

Then $R(n) \leq \ell(I^{n-m} M_1/I^n M_1) = S^I_{M_1}(n) - S^I_{M_1}(n-m)$. Then the degree of $R(n)$ as $n \to \infty$ is $\leq \deg S^I_{M_1} < \deg S^I_M$. This also shows that the polynomial $R(n)$ tends toward has positive leading coefficient.

□

We now introduce another notion of dimension of an R-module M.

Definition 20.8. Let M be an R-module. The dimension of M is $\dim M = \dim R/Ann(M)$ if $M \neq 0$, and -1 if $M = 0$.

And we introduce yet another notion of dimension:

Definition 20.9. Let (R, m) local ring, and M a f.g. R-module. The Chevalley dimension of M is $\delta(M) = \min\{r | \exists a_1, \cdots, a_r \in m, \ell(M/(a_1, \cdots, a_r)M) < \infty\}$ and $\delta(M) = -1$ if $M = 0$.

If R is Noetherian, then $\delta(M) < \infty$ because m is finitely generated, and M/mM is R/m-module, and m is an ideal of definition os R/m is Artinian. Thus, M/mM is both Noetherian and Artinian. So $\ell(M/mM) < \infty$, so $\delta(M) < \infty$.

We've introduced all of these notions of dimension. It turns out that we have the following wonderfult result:

Theorem 20.10 (Dimension Theorem)**.** *Let M be a f.g. R-module. And (R, m) local Noetherian. Then $\dim M = \delta(M) = d(M)$, where $d(M)$ is the Hilbert-Samuel degree, $\delta(M)$ is the Chevalley degree, and $\dim M = \dim R/Ann(M)$.*

We won't prove this now, but here are some corollaries:

Proposition 20.11. *Let (R, m) local Noetherian, M f.g. R-module.*

- $\dim(M) < \infty$.
- $\dim R$ *is the minimal number of generators among all ideals of definition.*

Proof. We have $\dim(M) = \delta(M)$, and m is finitely generated since R noetherian. Note M/mM is finitely generated R/m-module, and R/m is Noetherian and Artinian. So M/mM is artinian Noetherian $\implies \ell(M/mM) < \infty$. So $\dim(M) < \infty$.

Note $\dim R = \delta R$. By definition, we have $\delta(R) \leq$ the minimal number of generators among all ideals of definition. Now we want to show $\geq$ inequality. Suppose $\delta(R) = n$. Then there exist $a_1, \cdots, a_n \in m$ s.t. $\ell(R/(a_1, \cdots, a_n)) < \infty$. So $R/(a_1, \cdots, a_n)$ is Artinian. Then the only prime, which is the image of m in the quotient, equals $\sqrt{0}$. But in Artinian ring, the nilradical is nilpotent. So there exist k s.t. $m^k \subseteq (a_1, \cdots, a_n) \subseteq m$. Then $(a_1, \cdots, a_n)$ is an ideal of definition. This completes the proof. □

A second corollary:

Proposition 20.12. $\dim k[[X_1, \cdots, X_n]] = n$.

Proof. We have the dimension is $\geq n$, you can just take a sequence of prime ideals $(x_1, \cdots, x_i)$. But $(x_1, \cdots, x_n)$ is an ideal of definition. So the dimension, which is equal to Chevalley of dimension, is $\leq n$. □

21. Nov 10: corollary of dimension theorem, general Krull PID

Recall from last time we had a nice dimension theorem:

Theorem 21.1 (Dimension Theorem)**.** *Let M be a f.g. R-module, (R, m) local Noetherian. Then $\dim M = d(M) = \delta(M)$. Note $\dim M = \dim R/Ann(M)$, $d(M)$ is the degree of the Hilbert samuel polynomial. And $\delta(M)$ is the Chevalley dimension.*

Here's another corollary of this theorem.

Proposition 21.2. *Let R be Noetherian. Then every prime has finite height.*

Proof. We have $ht(p) = \dim R_p$, which is Noetherian and local. We have $\dim R_p = \delta R_p$, and $\ell(R_p/pR_p) < \infty$, while pR_p has finitely many generators since R is Noetherian. So $\dim R_p < \infty$. □

Nagata constructed a Noetherian ring R with infinite dimension. But the corollary implies that this ring has infinitely many maximal ideals with heights going to infinity.

Proposition 21.3. *If you have a local Noetherian ring (R, m), and $k = R/m$, then $\dim R \leq \dim_k m/m^2$. Note m/m^2 is finite dimensional vector space.*

Proof. Let $a_1, \cdots, a_r \in m$ s.t. their reductions $\overline{a_1}, \cdots, \overline{a}_r$ is a basis of m/m^2 over k. By Nakayama, $a_1, \cdots, a_r$ is a set of generators of m. Also $\dim R \leq$ the minimum set of generators of an ideal of definition. m is an ideal of definition, so $\dim R \leq r =_k m/m^2$. □

We also obtain an easier proof of Krull's PID theorem:

Theorem 21.4 (Krull's PID Theorem)**.** *Let R be a Noetherian ring, and $p \subseteq R$ prime. Then $ht(p) \leq n \iff$ there exists I generated by n elements s.t. p is minimal among primes containing I.*

Proof. Suppose $ht(p) \leq n$. Then $ht(p) = \dim R_p \leq n$. Then there exists an ideal of definition $(pR_p)^k \subseteq J \subseteq pR_p$ s.t. J is generated by n elements. So let $J = (a_1/s, \cdots, a_n/s)$ for $a_i \in p$, $s \notin p$. Then let $I = (a_1, \cdots, a_n) \subseteq p$. We claim that p is minimal among primes containing I. Suppose we had $I \subseteq p' \subseteq p$ for some prime p'. Localizing, we find $p'R_p \supseteq (pR_p)^k \implies p'R_p \supseteq pR_p$. This implies $p'R_p = pR_p \implies p' = p$.

Now assume we have $I = (a_1, \cdots, a_n) \subseteq p$, where p is minimal among those containing I. We have $IR_p \subseteq pR_p$. Note R_p is Noetherian, so we can consider the primary decomposition $IR_p = I_1 \cap \cdots \cap I_k$. Then $\sqrt{IR_p} = \sqrt{I_1} \cap \cdots \cap \sqrt{I_k} = p_1 \cap \cdots \cap p_k$, where p_i is an associated prime of IR_p. Restricting to those p_i which are minimal, we find $p_i \subseteq pR_p$. But p is minimal among those containing I. So we must have $p_i = pR_p$. So $\sqrt{IR_p} = pR_p$. Since R_p is noetherian, pR_p is finitely generated, so there exist k s.t. $(pR_p)^k \subseteq IR_p \subseteq pR_p$. So IR_p is an ideal of definition, so $ht(p) = \dim R_p \leq n$. □

Another corollary:

Proposition 21.5. *Let R be Noetherian, $0 \neq x \in R$ which is not invertible, and not a zero divisor. Then every p minimal over x has height 1.*

Proof. We know already that $ht(p) \leq 1$. If $ht(p) = 0$, then $\dim R_p = 0$. If R_p itself is zero, then there exists $t \notin p$ s.t. $tx = 0$, which can't happen. Then $R_p \neq 0$, and $p \in Supp(R)$. The $ht(p) = 0 \implies p$ is minimal element in $Supp(R)$. Then $p \in Ass(R)$. So $x \in p \subseteq \bigcup_{p \in Ass(R)} p = Z(R)$. But this means x is a zero divisor, contradiction.

We see that we cannot have $ht(p) = 0$ so $ht(p) = 1$. □

We've seen some nice applications. Let's now prove the dimension theorem.

Theorem 21.6 (Dimension Theorem)**.** *Let (R, m) be local Noetherian. Let M be f.g. R-module. Then $\dim M = d(M) = \delta(M)$.*

Proof. We're going to prove that

$$\dim(M) \leq^1 d(M) \leq^2 \delta(M) \leq^3 \dim(M).$$

From there, the claim will follow.

Let's prove $\dim(M) \leq d(M)$.

- Let $S_M = S_M^m$ be the Hilbert-Samuel polynomial. If $d(M) = -1$, then $S_M(n) = 0$ for $n >> 0$. Then $M/m^nM = 0$ for $n >> 0$. Then by Nakayama's, if $M/IM = 0$ for $I \subseteq J(R) = m$, then $M = 0$. So $M = 0$. So $\dim(M) = -1$.
- If $d(M) \geq 0$. Look at $p \in Supp(M) \iff p \supseteq Ann(M)$. Note $\dim M = \dim R/Ann(M)$. Taking the primary decomposition of $Ann(M)$, and taking the radical, we have $\sqrt{Ann(M)} = \bigcap p_i$, where the p_i are prime ideals associated to M. We have $V(Ann(M)) = V(\sqrt{Ann(M)}) = V(\bigcap p_i) = \bigcup V(p_i)$. But $\dim(V(Ann(M)) = \max \dim V(p_i) = \max coht(p_i)$. But since this is a finite set, there is a $p \in Ass(M)$ s.t. $\dim M = \dim R/p$. Since $p \in Ass(M)$, there exist nonzero $x \in M$ s.t. $p = Ann(x)$. We can

put $R/p \hookrightarrow M$ by $v \mapsto vx$. So $d(R/p) \leq d(M)$. Since $\dim M = \dim R/p$. So we just need to show $\dim R/p \leq d(R/p)$. We claim that every chain $p = p_0 \subset \cdots \subset p_t$, then $t \leq d(R/p)$. This is true for any prime p. If $t = 0$, then $R/p \neq 0 \implies d(R/p) \geq 0$. Now assume our results holds up to $t-1$. We show it holds for t. Let's consider $p = p_0 \subset \cdots \subset p_t$. Let $x \in p_1 \setminus p_0$. Note the ideal $Rx + p_0 \subseteq p_1$. Let $q \in Ass(R/p + Rx)$ s.t. $q \subseteq p_1$ and is minimal over $Rx + p_0$. We can do this because taking primary decomposition of $Rx + p_0$ and taking the radical, we get $\sqrt{Rx + p_0} = \bigcap p_i \subseteq p_1$. We have $d(R/q) \leq d(R/p + Rx)$ because $Rx + p_0 \subseteq q$, becuase $R/Rx + p_0 \to R/q$ surjects, so that's why $d(R/q) \leq d(R/p + Rx)$. Then $q \subset p_2 \subset \cdots \subset P - t$ is a chain of length $t - 1$. Then by induction, $t - 1 \leq d(R/q)$. We have a SES

$$0 \to R/p \to R/p \to R/Rx + p \to 0$$

where $R/p \to R/p$ is the map $v \mapsto [x]v$. This is because $[x] \neq 0 \in R/p$, and R/p is integral. Then $S_{R/p}(n) + S_{R/Rx+p}(n) = S_{R/p}(n) + R(n)$, where R is polynomial like of degree $< d(R/p)$. This shows $d(R/Rx + p) < d(R/p)$. So what we get is that $t - 1 < d(R/p)$. So $t \leq d(R/p)$.

□

22. Nov 15: proving dimension theorem

We're going to continue with the dimension theorem proof.

Theorem 22.1 (Dimension Theorem)**.** *Let (R, m) be local Noetherian. Let M be f.g. R-module. Then $\dim M = d(M) = \delta(M)$.*

Proof. We're going to prove that

$$\dim(M) \leq^1 d(M) \leq^2 \delta(M) \leq^3 \dim(M).$$

From there, the claim will follow.

First we prove $\dim(M) \leq d(M)$.

- If $d(M) = -1$, then this means the hilbert samuel polynomial $S_M(n)$ is 0 for $n >> 0$¿ Then $M/m^n M = 0$ for $n >> 0$. Then by Nakayama's, this means $M = 0$. Then $\dim M = -1$.
- Now assume $d(M) \geq 0$. Note by lemma 5.3, $Supp(M) = V(Ann(M))$. Taking the primary decomposition of $Ann(M)$ then taking the radical, we find $\sqrt{Ann(M)} = \bigcap p_i$. Taking minimal p_i containing $Ann(M)$, this p_i must be in $Ass(M)$. Furthermore, note $V(Ann(M)) = V(\sqrt{Ann(M)}) = V(\bigcap p_i) = \bigcup V(p_i)$. So $\dim M = \dim V(Ann(M)) = \dim \bigcup V(p_i) = \max \dim V(p_i) = \max \dim R/p_i$. Since there are finitely many associated primes, and thus finitely many minimal primes containing $Ann(M)$, we have $\dim M = \dim R/p$ for some $p = Ann(x)$. Then note $R/p \hookrightarrow M$ via $v \mapsto vx$. So $d(R/p) \leq d(M)$. Then it suffices to show that $\dim R/p \leq d(R/p)$.

  Let $p = p_0 \subset \cdots \subset p_t$ be a chain of R/p. We claim $t \leq d(R/p)$. We proceed by induction. The base case we have $R/p \neq 0$, so $d(R/p) \geq 0$. Now assume our claim holds for up to $t-1$. We show it holds for t. Let our chain be $p = p_0 \subset \cdots \subset p_t$. Let $x \in p_1 \setminus p_0$. Note $Rx + p \subseteq p_1$. Then consider $R/(p + Rx)$. The annihilator of this is $p + Rx$, and taking its primary decomposition then its square root yields $\sqrt{p + Rx} = \bigcap q \subseteq p_1$. Choose $p + Rx \subseteq q$ minimal, and note $q \subseteq p_1$. Then this is in $Ass(R/(p + Rx))$.

Then note $R/(p+Rx)$ surjects onto R/q, so $d(R/q) \leq d(R/(p+Rx))$. In R/q, we have chain $q \subset p_2 \subset \cdots \subset p_t$. By induction, $t-1 \leq d(R/q)$, so $t-1 \leq d(R/(p+Rx))$. Furthermore, we have SES

$$0 \to R/p \to R/p \to R/(p+Rx) \to 0$$

where the map $R/p \to R/p$ is given by $v \mapsto [x]v$. This gives us a SES $S_{R/p}(n) + S_{R/(p+Rx)}(n) = S_{R/p}(n) + R(n)$, telling us that $d(R/(p+Rx)) < d(R/p)$. Thus, $t-1 < d(R/p) \implies t \leq d(R/p)$, as desired.

We will now prove that $d(M) \leq \delta(M)$. Let $\delta(M) = r$. Then there $\exists I = (a_1, \cdots, a_r)$ such that $\ell(M/IM) < \infty$. Let $p = Ann(M)$, and $q = I + p$. We're going to show that q is m-primary. Note $Ass(R/q) \subseteq Supp(R/q)$. We will show that $Supp(R/q) = \{m\}$, and since $Ass(R/q)$ must be non-empty, we must have $Ass(R/q) = \{m\}$.

Note $Supp(R/q) = V(q) = V(I+p) = V(I) \cap V(p) = Supp(R/I) \cap Supp(M)$. We claim that $Supp(R/I) \cap Supp(M) = Supp(M/IM)$. Suppose $p_1 \in Supp(R/I) \cap Supp(M)$. Then $M_{p_1} \neq 0$, and $p_1 \in V(I)$. But if $(M/IM)_{p_1} = 0$, then $M_{p_1} = I_{p_1} M_{p_1}$. Note $I_{p_1} \subseteq p_1 R_{p_1}$, so by Nakayama's, this implies $M_{p_1} = 0$, contradiction. So $p_1 \in Supp(M/IM)$. Now suppose $p_1 \in Supp(M/IM)$. Then $M_{p_1} \neq 0$, so $p_1 \in Supp(M)$. Assume FSOC $p_1 \notin Supp(R/I)$. Then $p_1 \notin V(I)$. Then $R \setminus p_1$ contains an element of I. This contradicts the fact $(M/IM)_{p_1} \neq 0$. So $p_1 \in Supp(R/I) \cap Supp(M)$, and so $Supp(R/I) \cap Supp(M) = Supp(M/IM)$. Note $\ell(M/IM) < \infty \implies$ all the primes in $Supp(M/IM)$ are maximal, namely m. Thus, $Supp(R/q) = Supp(M/IM) = \{m\}$

Now that we know that q is m-primary, note $\sqrt{q} = m$. Since R noetherian, m finitely generated, so there exists n s.t. $m^n \subseteq q \subseteq m$. So q is an ideal of definition. Note since $p = Ann(M)$, M is a finitely generated R/p-module. Also, $q/p = ([a_1], \cdots, [a_r])$ is still an ideal of definition. The hilbert samuel polynomial $S_M^{q/p}$ then has deg $\leq r$. But note

$$\ell_{R/p}(M/(q/p)^n M) = \ell_R(M/q^n M).$$

To see this, note $q^n M = (q/p)^n M$. Then $d(M) \leq r$, so we're done.

Finally, we prove that $\delta(M) \leq \dim(M)$. Suppose $\dim(M) = -1$. Then $M = 0 \implies \delta(M) = -1$. Now suppose $\dim(M) = 0$. Then every prime of $R/Ann(M)$ is Artinian, and since M is f.g. $R/Ann(M)$-module, M is Artinian. Since it's also Noetherian, this implies $\ell(M) < \infty \implies \delta(M) = 0$.

Now suppose $\dim(M) > 0$. Let $\{p_1, \cdots, p_t\} \subseteq Ass(M)$ s.t. $coht(p_i) = \dim(M)$. Note $m \not\subseteq p_i$ for every i, since $(p_i) = \dim(M) > 0$. So by prime avoidance, $m \not\subseteq \bigcup p_i$. So there exist $x \in m$ s.t. $x \notin p_i, \forall i$. Let $N = M/xM$. Note $Supp(N) \subseteq Supp(M)$. In fact, $Supp(N) \subseteq Supp(M) \setminus \{p_1, \cdots, p_t\}$, because N_{p_i} is an R_{p_i}-module, and x is a unit, which would imply $N_{p_i} = 0$. Then $V(Ann(N)) \subseteq V(Ann(M)) \setminus \{p_1, \cdots, p_t\}$, from which it follows that $\dim(N) < \dim(M)$. By induction, we can assume that $\delta(N) \leq \dim(N)$. Let $\delta(N) = r$. Then $\ell(N/(a_1, \cdots, a_r)N) < \infty$ for some $a_1, \cdots, a_r$. Then $\ell(M/(x, a_1, \cdots, a_r)M) < \infty$, so $\delta(M) \leq 1 + r$. Then $\delta(M) \leq 1 + r \leq 1 + \dim(N) \leq \dim(M)$. So $\delta(M) \leq \dim(M)$ as desired. □

As a corollary:

Proposition 22.2. *Let* (R, m) *be local Noetherian. Let* $x \in R$ *be neither a unit nor zero divisor. Then* $\dim R/(x) = \dim(R) - 1$.

Proof. Assume FSOC that $\dim(R) = 0$. Then R is Artinian, and its only prime is m. So $Ass(R) = \{m\}$. But $m = Z(R)$. But if x is not a unit, $x \in m$, but this means its a zero divisor, contradiction.

So assume $\dim(R) > 0$. Let $\{p_1, \cdots, p_t\} \subseteq Ass(R)$ s.t. $coht(p_i) = \dim R$. Note the union of all associated primes is the zero divisors, so $x \notin p_i, \forall i$. Then $Supp(R/(x)) \subseteq Supp(R)$, but furthermore $Supp(R/(x)) \subseteq Supp(R) \setminus \{p_1, \cdots, p_t\}$, because $(R/(x))_{p_i}$ is R_{p_i}-module, and x would be invertible in this case, making $(R/(x))_{p_i} = 0$. Then $V(Ann(R/(x)) \subseteq V(Ann(R)) \setminus \{p_1, \cdots, p_t\}$. This shows that $\dim R/(x) < \dim(R)$. So $\dim R/(x) \leq \dim(R) - 1$.

Now we show $\dim(R) - 1 \leq \dim R/(x)$. Let $\dim R/(x) = r$. Then there exist $a_1, \cdots, a_r \in m$ s.t. $([a_1], \cdots, [a_r])$ ideal of definition of $R/(x)$. Then $(x, a_1, \cdots, a_r)$ is ideal of definition of R. Then $\dim R \leq r + 1$, as desired.

□

We're going to talk more about "system of parameters." This is maybe an algebraic version of the notion of a system of coordinates in a variety geometrically.

Definition 22.3. Let (R, m) be Noetherian local, M f.g. R-module, and $n = \dim(M)$. A system of parameters for M is a tuple of elements $\{a_1, \cdots, a_n\} \subseteq m$ s.t. $\ell_R(M/(a_1, \cdots, a_n)M) < \infty$.

Example 22.4. (R, m) Noetherian local. $\dim R = n$, $I = (a_1, \cdots, a_n)$ ideal of definition, then $(a_1, \cdots, a_n)$ is a SOP.

$(x_1, \cdots, x_n)$ in $k[[X_1, \cdots, X_n]]$

Proposition 22.5. *(R, m) local Noetherian, M f.g. R-module, $a_1, \cdots, a_t \in m$. Then $\dim M/(a_1, \cdots, a_t)M \geq \dim M - t$ and equality $\iff$ $\{a_1, \cdots, a_t\}$ is part of system of parameters of M.*

Proof. Let $a \in M$, $N = M/aM$. let $r = \dim N$, there exists $b_1, \cdots, b_r \in m$ such that $\ell(N/(b_1, \cdots, b_r N) < \infty$ which equals $\ell(M/(a, b_1, \cdots, b_r)M) < \infty$. So $\dim(M) \leq r+1$, so $\dim(M)-1 \leq \dim(N)$. By induction, $\dim(M/(a_1, \cdots a_{t+1})M) \geq \dim(M/(a_1, \cdots, a_t)M) - 1 \leq \dim(M) - t - 1$ (induction step). □

Now we will talk briefly about regular sequences.

Definition 22.6. Let M be an R-module. A sequence $(a_1, \cdots, a_t) \in R \setminus \{0\}$ is an M-regular sequence if $(a_1, \cdots, a_t)M \neq M$ and $a_i \notin Z(M/(a_1, \cdots, a_{i-1}M)$.

Example 22.7. For any $a \notin Z(M)$, $aM \neq M$, then $\{a\}$ is a regular sequence.

$R = k[[X_1, \cdots, X_n]]$, then $(X_1, \cdots, X_n)$ is a regular sequence.

Permuting elements of a regular sequence may not be a regular sequence anymore. Order matters.

Example 22.8. In $R = k[X, Y, Z]$, where k a field. Claim $\{X, Y(1-X), Z(1-X)\}$ is a regular sequence. Modding out by X, we obtain $k[Y, Z]$. Y, Z regular sequence here.

What if we switched the order? $Y(1-X), Z(1-X), X$. Then $k[X, Y, Z]/Y(1-X)$, then $Z(1-X)$ is a zero divisor, since $\overline{YZ(1-X)} \cong 0$.

Proposition 22.9. *Let M be a f.g. R-module. Then (R, m) local Noetherian. Then $(a_1, \cdots, a_t)$ is a M-regular sequence. Then it can be extended to a system of parameters of M.*

Proof. Induct on t. For $t = 1$, $a_1 \notin Z(M)$, and a_1 not invertible since otherwise $a_1 M = M$. We saw that $\dim M/a_1 M = \dim M - 1$. Then let $(b_1, \cdots, b_k)$ be SOP for $M/(a_1)M$. Then $a_1, b_1, \cdots, b_k$ is SOP for M. So there are $k+1$ elements, equal to $\dim M$. And $\ell(M/(a_1, b_1, \cdots, b_k)M) = \ell(\widetilde{M}/(b_1, \cdots, b_k))$, where $\widetilde{M} = M/(a_1)$.

Now let $t > 1$. By induction, $\{a_1, \cdots, a_{t-1}\}$ is a part of a SOP. By a previous proposition, $\dim M/(a_1, \cdots, a_{t-1})M = \dim M - t + 1$. So $a_t \notin Z(M/(a_1, \cdots, a_{t-1}M)$. So by the same argument, $\dim M/(a_1, \cdots, a_t)M = \dim M - t$. Take $b_1, \cdots, b_k$ SOP for $M/(a_1, \cdots, a_t)M$. Then $a_1, \cdots, a_t, b_1 \cdots, b_k$ SOP for M. □

Definition 22.10 (Depth)**.** Let (R, m) local Noetherian, M f.g. R-module (nonzero). The depth of M is

$$\mathit{depth}(M) = \max\{t | a_1, \cdots, a_t \text{ is a regular sequence }\}$$

We see $\mathit{depth}(M) \leq \dim M$, since any regular sequence can be completed to a system of parameters.

Definition 22.11 (Cohen-Macaulay)**.** (R, m) local Noetherian. M f.g. R-module.

- M is **Cohen-Macaulay** if $\mathit{depth}(M) = \dim M$.
- (R, m) is Cohen-Macaulay if $\dim R = \mathit{depth}(R)$.
- (R, m) regular if m can be generated by n elements, $n = \dim R$. $\dim R = \dim m/m^2$. If $m = (a_1, \cdots, a_r)$, then $a_1, \cdots, a_r$ is said to be a regular system of parameters.

Dora is taking over texing today! yay

Proposition 22.12. *Dora is cool*

23. Nov 17th: Valuation Rings

References are Pg 65, Atiyah Macdonald or Pg 268 in Eisenbud.

Definition 23.1 (valuation-ring)**.** Let K be a field, $R \subset K$ a ring. We say that R is a valuation ring for K if for every $\alpha \in K$, $\alpha \neq 0$, either $\alpha \in R$ or $\alpha^{-1} \in R$. (Obviously you can also have that both happen).

Example 23.2. Let $K = \mathbb{Q}$. Consider $R = \mathbb{Z}_{(p)}$ (localization at p). R consists of all fractions a/b s.t. b is not divisible by p. Any fraction a/b in $\mathbb{Q}$ can be simplified so either a or b is not divisible by p. Then either $a/b \in R$ or $b/a \in R$.

Example 23.3. Let $K = k(x)$ (the fraction field of polynomials). Fix $P \in k[x]$ an irreducible polynomial and let R be the localization of $k[x]$ at (P). Same reasoning as previous example: R is a valuation ring for K.

Example 23.4. Let $K = k(x)$ as before. Let $R = \{\frac{f}{g} | \deg f \leq \deg g\}$. Then R is a valuation ring for K.

Example 23.5. $K = \{\sum_{i \geq r} a_i x^i | a_i \in k, r \in \mathbb{Z}\}$ = field of Laurent polynomials. Take $R = k[[x]] \subset K$; this is a valuation ring.

Here a few properties of valuation rings:

Proposition 23.6. *Let $R \subseteq K$ be a valuation ring. Then*

(1) $K = \operatorname{Frac} R$
(2) If $R \subset S$, then S valuation ring for K.
(3) R is local.

(4) R is integrally closed.

Proof. (1) : Let $\alpha \in K$. If $\alpha \in R$, we're done. Otherwise, $\alpha^{-1} \in R$. $\alpha = \frac{1}{\alpha^{-1}} \in \operatorname{Frac} R$.

(2) : Immediate.

(3): Note for any ring R, $M = R \setminus R^\times$ is the union of all maximal ideals of R. It suffices to show that M is an ideal. Then M must be maximal, and thus R is local. Suppose $a \in M$, $b \in R$. If $ab \in R^\times$, then there exist c s.t. $abc = 1$. Then $a \in R^\times$, contradiction. So $ab \in M$. Now suppose $a, b \in M$. We want to show $a + b \in M$. Note $a/b \in \operatorname{Frac} R = K$. So either $a/b \in R$ or $b/a \in R$. WLOG suppose $a/b \in R$. Then $a + b = b(1 + \frac{a}{b})$. Note $b \in M$, and $1 + \frac{a}{b} \in R$. then $a + b \in M$.

(4). Let $\alpha \in K$ integral over R. So $\alpha^n + c_{n-1}\alpha^{n-1} + \cdots + c_1\alpha + c_0 = 0$. If $\alpha \in R$ already, we're done. Otherwise, $\frac{1}{\alpha} \in R$. Otherwise, multiply by α^{-n+1}. We obtain $\alpha + c_{n-1} + \cdots + c_1 \frac{1}{\alpha^{n-2}} + \frac{c_0}{\alpha^{n-1}}$. This shows that $\alpha \in R$. □

The ideals of valuation rings have very nice structure with respect to each other. Namely:

Proposition 23.7. *Let $R \subset K$ be a valuation ring. Then the ideals of R form a totally ordered set. In other words, if I, J are ideals of R, then either $I \subset J$ or $J \subset I$.*
Suppose we have some integral domain $R \subset \operatorname{Frac} R = K$ with ideals forming totally ordered set. Then R is valuation ring for K.

Proof. We prove the first part. Suppose $I \not\subseteq J$. Then there exists $a \in I, a \notin J$. Let $b \in J$. Either $a/b \in R$ or $b/a \in R$. If $a/b \in R$, then $b(a/b) = a \implies a \in J$, contradiction. If $b/a \in R$, then $b = (b/a)a \implies b \in I$. So $J \subset I$.

Now we prove the second part. Let $\alpha = \frac{a}{b} \in K$, where $a, b \in R$. Consider the ideals $(a), (b)$. Suppose $(a) \subseteq (b)$. Then $bx = a$ for some $x \in R$. Then $a/b \in R$. If $(b) \subseteq (a)$, then there is some $x \in R$ s.t. $ax = b$. Then $b/a \in R$. So either $\alpha \in R$ or $\alpha^{-1} \in R$, showing R is a valuation ring for K. □

The structure of Noetherian valuation rings is even nicer.

Proposition 23.8. *Let $R \subset K$ be a Noetherian evaluation ring. Then R is PID and there is a prime element π s.t. every ideal I is of the form (π^n) for some $n > 0$. Furthermore, $\bigcap_{n>0}(\pi^n) = 0$.*

Proof. Let $I \subseteq R$ be an ideal. Since R is Noetherian, $I = (g_1, \cdots, g_n)$ for some g_i. But since R is a valuation ring, the (g_i) are totally ordered. So $I = (g_i)$ for some g_i.

Since R is valuation ring, it is local. So $(g) \subseteq (\pi)$ maximal. Then $g = \pi g_1$ for some g_1. If g_1 is a unit, then $(g) = (\pi)$. Otherwise, $(g_1) \subseteq (\pi)$, so $g_1 = \pi g_2$ for some g_2. We can continue this process to get a chain $(g) \subseteq (g_1) \subseteq (g_2) \subseteq \cdots$. Since R is Noetherian, this stabilizes, so that $g_n = \pi g_{n+1}$ for some unit g_{n+1}. Then $(g) = (\pi^n)$.

If $a \in \bigcap_{n>0}(\pi^n)$, we have $\pi^n | a$ for every n. But R PID implies R is UFD. So only a finite power of π can divide a. □

A nice fact is the following:

Theorem 23.9. *Let $R \subset K$ a subring. Then, $\tilde{R}$ (the integral closure of R in K) is equal to*

$$\bigcap_{R \subset S, S \text{ valuation}} S$$

We need some preparation to prove this:

Proposition 23.10. *Let $R \subset K$, $h : R \to L$ a homomorphism where L is an algebraically closed field. If $0 \neq \alpha \in K$, then h can be extended to either $\tilde{h} : R[\alpha] \to L$ or $\tilde{h} : R[\alpha^{-1}] \to L$.*

Proof. Exercise: we can assume that $h(R)$ is a subfield, R is local (hint: localize at $\ker(h)$). From now on, we assume this.

Step 1: we can extend h to $R[x]$. If $f = \sum a_n x^n$, set $h(f) = \sum h(a_n)x^n \in F[x]$ (where $F = h(R)$ as a subfield). Let $I = \{f \in R[x] | f(\alpha) = 0\} \subset R[x]$. We have $h(I) = J \subset F[x]$, which is a PID, so $h(I) = (g)$ for $g \in F[x]$. Note g is either non-constant or zero.
Case 1: Suppose g is non constant. Since $L = \bar{L}$, g has a root $\beta \in L$. Then $\widetilde{h} : R[\alpha] \to L$ where $\alpha \mapsto \beta$ and $\sum c_i \alpha^i \mapsto \sum h(c_i)\beta^i$ is a well-defined ring homomorphism which restricts to h over R.

Case 2: if $g = 0$, extend by sending α to any β. If g is a nonzero constant.

□

Proposition 23.11. *Let $R \subset K$, and $h : R \to L$ homomorphism where L algebraically closed field. Then h has a maximal extension $\widetilde{h} : S \to L$ (so $R \subseteq S \subseteq K$ and doesn't extend to larger subring). For any such extension, S is valuation ring of K.*

Proof. Let $\mathcal{A}$ be a family of such extensions. The extensions $h_i : R_i \to L$ are partially ordered by $(h_i, R_i) \leq (h_j, R_j)$ if $R_i \subseteq R_j$ and $h_j|_{R_i} = h_i$. Any chain has an upper bound. Then by Zorn's lemma, there is a maximal element.

If $\alpha \in K$, either $\alpha \in S$ or $\alpha^{-1} \in S$. If neither of these were true, by the previous lemma we could construct an extension, contradicting the maximality of S. □

24. Nov 22:

Recall we were trying to prove that

Theorem 24.1. *Let $R \subseteq K$ be subring. Then the integral closure*

$$\widetilde{R} = \bigcap_{R \subset S} S$$

is the intersection of all valuation rings containing it.

Proof. Note if $\alpha \in \widetilde{R}$, then α is in the integral closure of each $S \supset R$. But since each S is a valuation ring, they're integrally closed, so $\alpha \in \bigcap_{R \subset S} S$. So $\widetilde{R} \subseteq \bigcap_{R \subset S} S$.

Now we want to show that $\bigcap_{R \subset S} S \subseteq \widetilde{R}$. We prove by contraposition. Suppose $\alpha \notin \widetilde{R}$. Note $\alpha \notin R[\alpha^{-1}]$. Otherwise, we could multiply by a power of α to obtain an expression that indicates $\alpha \in \widetilde{R}$, which is impossible. Then $\alpha^{-1} \notin R[\alpha^{-1}]^\times$. Then there is a maximal ideal $m \subseteq R[\alpha^{-1}]$ containing α^{-1}. So we have a homomorphism $R[\alpha^{-1}] \to R[\alpha^{-1}]/m \hookrightarrow L$, where L is the algebraic closure of $R[\alpha^{-1}]/m$.

This gives us a homomorphism $h : R[\alpha^{-1}] \to L$. Then there is a maximal extension $\widetilde{h} : S \to L$, where S is valuation ring and restricts to h over $R[\alpha^{-1}]$. We claim that $\alpha \notin S$. Assume FSOC that it were. Then $\widetilde{h}(\alpha)\widetilde{h}(\alpha^{-1}) = \widetilde{h}(1) = 1$. But we also have that $\widetilde{h}(\alpha^{-1}) = h(\alpha^{-1}) = 0$. So we get an immediate contradiction. Then $\alpha \notin S$. □

Let's talk about **valuations** now.

Definition 24.2. An ordered abelian group is an abelian group H together with a total order relation compatible with addition. Namely, if $x \geq y, a \geq b$, then $x + a \geq y + b$.

From this, immediately deduce that if $x \geq y$, then $-y \geq -x$. And if $x > 0, y \geq 0$, then $x + y > 0$.

We will consider an element ∞ in $H \cup \{\infty\}$, s.t. for all $x \in H$:

1. $x \leq \infty$
2. $x + \infty = \infty$
3. $\infty + \infty = \infty$

Definition 24.3 (valuation)**.** If K is a field, a valuation on k is a map $v : k \to H \cup \{\infty\}$ where H is an ordered abelian group such that $\forall x, y \in K$

1. $v(xy) = v(x) + v(y)$
2. $v(x + y) \geq \min(v(x), v(y))$
3. $v(x) = \infty \iff x = 0$

It follows that $v(1) = 0$, since $v(1) = v(1) + v(1)$.

The valuation v induces a group morphism $K^\times \to H$. The image $v(K^\times)$ is a subgroup and is called the value group of v.

Example 24.4. On $\mathbb{Q}$, there are different types of valuations:

- Non-archimidean valuation for every prime p. $v : \mathbb{Q} \to \mathbb{Z} \cup \infty$ where $\frac{a}{b} \mapsto v_p(a) - v_p(b)$.

Example 24.5. k field, $k(x)$. Valuation $v : k(x) \to \mathbb{Z} \cup \infty$, map $\frac{P}{Q} \mapsto v(P) - v(Q)$, where $v(P)$ is the first power of x to appear in P.

Definition 24.6. Let $v : k \to H \cup \infty$ be a valuation. Define

$$R_v = \{x \in K | v(x) \geq 0\}$$

$$m_v = \{x \in K | v(x) > 0\}.$$

Lemma 24.7. *R_v is a valuation ring, m_v is the unique maximal ideal.*

Proof. If $\alpha \in K$, then $v(\alpha) \geq 0$, or $v(\alpha^{-1}) = -v(\alpha) \geq 0$, so either $\alpha \in R_v$ or $\alpha^{-1} \in R_v$. Also $\alpha \in R_v^\times \iff v(\alpha) = 0$. So $m_v = R_v \setminus R_v^\times = \{\alpha \in K, v(\alpha) > 0\}$. □

What we did is from a valuation, we got a valuation ring. We can go in the other direction.

Proposition 24.8. *Let $R \subseteq K$ be a valuation ring. Define $G = \{Rx | x \in K^\times\}$. This is a totally ordered abelian group, with group operation $(Rx)(Ry) = Rxy$ and order given by $Rx \geq Ry \iff Rx \supseteq Ry$. We obtain a valuation $v : K \to G \cup \infty$ via $x \mapsto Rx$ and $0 \mapsto \infty$.*

Furthermore, for any valuation $v' : K \to H \cup \infty$ s.t. $R_{v'} = R$ and the value group of v' is H, there exist isomorphism $\phi : G \to H$ s.t.

$$\begin{tikzcd}
K \arrow[rr, "v"] \arrow[dr, "v'"'] & & H \\
& G \arrow[ur, "\phi"'] &
\end{tikzcd}$$

commutes.

Proof. First we show that the order is indeed a total order. Suppose we have Rx, Ry, where $x, y \in K^\times$. We want to show that either $Rx \supseteq Ry$ or $Rx \subseteq Ry$. Suppose $Rx \not\supseteq Ry$. Then there exists $a \in Rx, a \notin Ry$. Let $b \in Ry$. Consider a/b. Since R is valuation ring, either $a/b \in R$ or $b/a \in R$. If $a/b \in R$, then $b(a/b) = a \in Ry$, contradiction. Then $b/a \in R$, so $a(b/a) = b \in Rx$. So $Rx \supseteq Ry$.

We claim that with the group operation, the total order gives G the structure of a totally ordered abelian group. Suppose $Rx \geq Ry, Ra \geq Rb$. Then $Rx \supseteq Ry, Ra \supseteq Rb$. Then $Rax \supseteq Ryb$, so we're done.

Now we check that $v : K \to G \cup \infty$ given by $x \mapsto Rx$ and $0 \mapsto \infty$ is indeed a valuation. Note $v(xy) = Rxy = (Rx)(Ry) = v(x)v(y)$. Furthermore, $v(x + y) = R(x + y)$. We want to show that $R(x + y) \geq \min\{Rx, Ry\}$. WLOG suppose $Rx \subseteq Ry$. So we want to show that $Rx \subseteq R(x+y)$. If not, then $R(x+y) \subseteq Rx$, so $\frac{x+y}{x} \in R$, so $x + y = rx \implies y = (r - 1)x$. Then $Ry \subseteq Rx$. Then $Rx = Ry$. Then $rx = y$ for some $r \in R$ where $r^{-1} \in R$ as well. FILL IN DETAIL HERE □

Lemma 24.9. *Let $R \subseteq K$ be a valuation ring. Define $G = \{Rx | x \in K^\times\}$. Then G is totally ordered given by $Rx \leq Ry \iff Rx \subseteq Ry$ (same idea as in proof of totally ordered structure of ideals of R). Also G is a group: $(Rx)(Ry) = Rxy$. Check G is ordered abelian group.*

We can define $v : K \to G \cup \infty$ given by $x \mapsto Rx$, $0 \mapsto \infty$.

One must check that v is a valuation, $Rv = R$, and for all valuations $v : k \to H \cup \infty$ s.t. $R_{v'} = R$, H value group of v', there exists $\phi : G \to H$ isomorphism s.t.

$$\begin{tikzcd}
K \arrow[rr, "v"] \arrow[dr, "v'"'] & & H \\
& G \arrow[ur, "\phi"'] &
\end{tikzcd}$$

commutes.

Consequently, there is a one-to-one correspondence between valuations and valuation rings. Yay!

Definition 24.10. A discrete valuation is a valuation with value group $\mathbb{Z}$. In other words, $v : K^\times \to \mathbb{Z}$ surjective.

Proposition 24.11. *Let $v : K \to \mathbb{Z} \cup \infty$ be a discrete valuation. Let $0 < c < 1$. Then $k \to \mathbb{R}$ given by $x \mapsto |x| = c^{v(x)}$ is a non-archimidean absollute value*

- $|x| \geq 0$ *and* $|x| = 0 \iff x = 0$
- $|xy| = |x||y|$
- $|x + y| \leq \max(|x|, |y|)$.

Definition 24.12 (DVR)**.** If v is a discrete valuation, then $R = R_v$ is called a discrete valuation ring.

Example 24.13. If $K = \mathbb{Q}$, $v = v_p$, then the localization at p $\mathbb{Z}_{(p)}$ is a DVR.
$K(X)$, v is vanishing order at 0, the valuation ring $k[X]_{(X)}$ is a DVR.

For any totally ordered abelian group H, there exists a field K and a valuation on K whose value group is H. This is in Atiyah-Macdonald, Exercise 3.3.

Let's explore DVRs more.

Definition 24.14. Let R be a DVR. If $t \in R$ s.t. $v(t) = 1$, then t is called a uniformiser.

Lemma 24.15. *Let (R, m) be a DVR, $t \in R$. then t is a uniformiser $\iff$ $m = (t)$.*

Proof. If $v(t) = 1$, then $(t) \leq m$. But $x \in m$, $v(x) \geq 1$ and $v(x/t) \geq 0 \implies x \in (t)$. So $(t) = m$. If $m = (t)$, then $v(t) \geq 1$. There exists t' s.t. $v(t') = 1$. Then $m = (t') = (t)$, so $t = \alpha t'$ and $\alpha \in R^\times$. So $v(t) = v(t') = 1$. □

Lemma 24.16. *Let R be a DVR, t a uniformiser. Then for each $x \in K$, there exists a unique $\mu \in R^\times$ and $n \in \mathbb{Z}$ s.t. $x = \mu t^n$. And in particular, $k = R[1/t]$.*

Proof. Let $n = v(x) \in \mathbb{Z}$. Then $v(x/t^n) = 0 \implies x/t^n \in R^\times$. □

Lemma 24.17. *If (R, m) DVR. Then $VI \subseteq R$, $I \neq 0$, there exists unique n s.t. $I = m^n$.*

Proof. Take $n = \min\{v(x) | x \in I\}$. □

We state but won't have time to prove the following theorem (in Atiyah Macdonald)

Theorem 24.18. *Let (R, m) be a noetherian local domain. Then TFAE:*

- *R is a DVR*
- *R is a PID*
- *m is principal*
- *$R = \widetilde{R}$ and every nonzero prime is maximal.*
- *$\forall I \subseteq R$, there exists n s.t. $I = m^n$.*
- $\dim_{R/m} m/m^2 = 1$

We will briefly mention Dedekind rings.

Definition 24.19. A Dedekind ring is an integrally closed Noetherian domain of dimension 1. So every nonzero prime is maximal.

25. Nov 29: Completions

Suppose you had $k[x]$, and $m = (x)$. Localizing, you get $k[x]_m$, which you can think of as inverting functions which do not vanish at zero. Taking the completion of $k[x]_m$ is $k[[x]]$. If you continue along the system

$$\cdots \to k[x]/x^3 \to k[x]/x^2 \to k[x]/x$$

you get $k[[x]]$. Note at each step, $k[x]/x^k$, the idea of an Artinian ring captures this k-th order differentials around the origin.

We'll begin by talking about inverse limits. There's a categorical formulation, but for the purposes of this class we'll state a simple version. See Appendix 6 of Eisenbud for more.

Definition 25.1. An inverse system is a collection of abelian groups (M_i), s.t. for $i \geq j$, we have maps $\phi_{ij} : M_i \to M_j$ which are compatible in the sense that when $i \geq j \geq k$, we have a commutative diagram:

$$\begin{tikzcd}
M_i \arrow[rr, "\phi_{ij}"] \arrow[dr, "\phi_{ik}"'] & & M_j \arrow[dl, "\phi_{jjk}"] \\
& M_k &
\end{tikzcd}$$

Definition 25.2. Let R be an abelian group, and a filtration $R = m_0 \supseteq m_1 \supseteq m_2 \supseteq \cdots$ by abelian subgroups. We obtain an inverse system

$$\cdots \to R/m_{i+1} \to R/m_i \to R/m_{i-1} \to \cdots$$

The inverse limit of the system $\{R/m_i\}$ is

$$\widehat{R} = \varprojlim R/m_i = \{(g_1, g_2, \cdots)\imath \prod R/m_i | \phi_{ji}(g_j) \cong g_i \in R/m_i, j \geq i\}$$

, which comes equipped with projection maps $\phi_i : \widehat{R} \to R/m_i$ which satisfies

$$\begin{tikzcd}
\widehat{R} \arrow[r, "\phi_j"] \arrow[dr, "\phi_i"'] & R/m_j \arrow[d, "\phi_{ji}"] \\
& R/m_i
\end{tikzcd}$$

If R is a ring, and m_i are ideals, then R/m_i is a ring, and $\widehat{R}$ is a ring. To show that $\widehat{R}$ is a ring, you'll have to show that the component-wise multiplication of elements of $\widehat{R}$ is well-defined.

Because of the projection maps, $\widehat{R}$ has a natural filtration by the ideals $\widehat{m}_i = \ker(\widehat{R} \to R/m_i)$.

Definition 25.3 (I-adic completion)**.** Let $I \subseteq R$. The I-adic filtration is the one given by $\{I^k\}$. The completion of R with respect to the the I-adic filtration is called the I-adic completion.

Lemma 25.4. *If m is maximal, then the m-adic completion $\widehat{R}$ is a local ring with maximal ideal $\widehat{m} = \ker(\widehat{R} \to R/m)$.*

Proof. Note this implies that $\widehat{R}/\widehat{m} \cong R/m$ which is a field, so indeed $\widehat{m}$ is maximal.

Let $g = (g_1, g_2, \cdots) \in \widehat{R}$ which is not in $\widehat{m}$. So $g_1 \in R/m$ is non-zero. So g_1 is invertible. And for any i, $g_i \notin m(R/m^i)$, so g_i is invertibe. This is because g_i maps to g_1 in R/m, so it cannot be in $m(R/m^i)$. And in R/m^i, the unique maximal ideal is m. So if you look at $(g_1^{-1}, g_2^{-1}, \cdots)$, and $g_j^{-1} \cong g_i^{-1} \mod R/m^i$ if $j \geq i$, so $g^{-1} \in \widehat{R}$, and $gg^{-1} = 1$. So any element not in the maximal ideal $\widehat{m}$ is invertible. So $\widehat{R}$ is local. $\square$

Example 25.5. If $R = k[x]$, $I = (X)$, then $\widehat{R} = k[[x]] = \varprojlim k[x]/(x^i)$.

Example 25.6. $R = \mathbb{Z}$, $I = (p)$ prime. Then $\widehat{R} = \mathbb{Z}_p$, ring of p-adic integers.

Example 25.7. More generally, if you have $k[X_1, \cdots, X_n]$ and $I = (X_1, \cdots, X_n)$, then $\widehat{R} = k[[X_1, \cdots, X_n]] = \varprojlim k[X_1, \cdots, X_n]/I^k$.

A remark: if $I \subseteq R$ is an ideal, then I defines a topology on R which makes it a topological ring, where $+, \times$ are continuous operations. Basis of neighborhoods of zero is given by $(I^k)_{k\geq 0}(x_n \to 0 \iff \forall k, \exists n_0, \forall n \geq n_0, x_n \in I^k)$.

If $I = R$, you get the coarse topology. If $I = 0$ discrete topology.

This topology is Hausdorff if $\bigcap_{n\geq 0} I^n = \{0\}$.

In this case, $\widehat{R}$ is the usual completion of R defined by Cauchy sequences. So $\widehat{R}$ is complete w.r.t this topology and $R \hookrightarrow \widehat{R}$ is injection with dense image.

In $\widehat{R}$, a series $\sum_{n\geq 0} a_n$ converges $\iff$ $a_n \to 0$ as $n \to \infty$. The reason is because when you fix k, there exist n_0 s.t. for all $n \geq n_0$, then $\sum_{\ell=n}^{n+m} a_\ell \in I^k$. So cauchy criterion tells you that this converges. Conversely if the series converges, $a_n \to 0$ as $n \to \infty$.

Completion is a very useful way of detecting local properties of a subvariety along a variety.

Valuable intuition for future: suppose you were asking for a solution in $\mathbb{Z}$. You could ask if it has a solution in Z/pZ. If it does, ask if it has solution Z/p^2Z. Continue in this manner, so maybe you get a solution in p-adics Z_p. If it has a solution in every Z_p, you could maybe get solution in $\mathbb{Z}$. There are still some obstructions you have to deal with of a cohomological nature. (see Hasse principle).

Theorem 25.8. *Let R be a Noetherian ring and $m \subseteq R$ be an ideal. Then*

- *$\widehat{R}$ is a Noetherian ring*
- *$\widehat{R}/\widehat{m}^j\widehat{R} \cong R/m^j$ for every j. So $\widehat{R}$ is complete w.r.t $\widehat{m}$ and $gr_{\widehat{m}}\widehat{R} = gr_m R$.*
- *If M is f.g. R-module, then the natural map $\widehat{R} \otimes M \to \varprojlim M/m^jM$ is an isomorphism. So $\widehat{R} \otimes_R M$ is the inverse limit of the inverse system M/m^jM.*

Proof. Proof of (a). Assume you've proved (b), so $gr_{\widehat{m}}\widehat{R} =_m R$. Since R is Noetherian, and R/m is noetherian, and $gr_m R$ is generated over R/m by finitely many elements of degree 1 in m/m^2, then $gr_m R$ is noetherian. Then $gr_{\widehat{m}}\widehat{R}$ is Noetherian. Now we can assume $R = \widehat{R}$, $gr_m R$ is noetherian, and $\bigcap m^n = 0$. because if you have $R \to \widehat{R}$, then $\bigcap m^n \mapsto 0$. Then the initial form is a well-defined operation on $\widehat{R}$. Let iR an ideal. The claim is that $a_1, \cdots, a_s \in I$ s.t. $in(a_1), \cdots, in(a_s)$ generates $in(I)$ as an ideal in $gr_M R$, then $a - 1, \cdots, a_s$ generate I.

Let $I' = (a_1, , a_s)$ where $a_i \neq 0$ and $in(a_i)$ generate $in(I)$ in $gr_m R$. Let $d \geq 1$, large enough such that $a_i \in m^d, \notin m^{d+1}$. Let $f \in I$ with $in(f) = \overline{f} \in m^e/m^{e+1}$. So $in(f) = \sum_j G_j in(a_j)$, where G_j homogenous of degree $e - \deg in(a_j)$. We can find $\widetilde{G_j} \in R$ with $in(\widetilde{G}_j) = G_j$. Then $f - \sum_j \widetilde{G}_j a_j = 0 \in m^e/m^{e+1}$ means $f - \sum \widetilde{G}_j a_j \in m^{e+1}$. We can repeat the process until $f - f' \in m^{d+1}$, $f' \in I'$. We can assume $f \in m^{d+1}$. So G_j has degree $e - d > 0$. We can find $\widehat{G_j} \in m^{e-d}$ s.t. $f - \sum_j \widehat{G}_j a_j \in m^{d+2}$. So we can construct sequences $g_j^{(i)} \in m_{e-d+i}$ s.t. $f - \sum_j g_j^{(0)} a_j - \sum_j g_j^{(1)} a_j - \cdots \sum g_j^{(i)} a_j \in m^{e+i+1}$. So $f - \sum_j(\sum_i g_j^{(i)}) a_j \in m^{e+i+1}$. This series converges when $i \to \infty$ to α_j. So $f - \sum \alpha_j a_j = 0$. So $f = \sum \alpha_j a_j \in I' \implies I = I'$. □

Definition 25.9. Let $M = M_0 \supseteq M_1 \supseteq M_2 \supseteq \cdots$ be a filtration by R-modules. Let $f \in M$, m greatest number s.t. $f \in M_m$, then the initial fom of f is $in(f) = \overline{f} M_m/M_{m+1}$. Otherwise, $in(f) = 0$ if $f \in \bigcap_{n=1}^{\infty} M_n$.

26. Dec 1: a light introduction to homological algebra

Let R be a ring.

Definition 26.1. A chain complex C_* is a sequence of R-modules

$$\cdots \to C_{n+1} \to^{d_{n+1}} C_n \to^{d_n} C_{n-1} \to^{d_{n-1}} \cdots$$

such that $d_n \circ d_{n+1} = 0$ for every n.

A cochain complex is a sequence of R-modules

$$\cdots \to C_{n-1} \to C_n \to^{d_n} C_{n+1} \to^{d_{n+1}} \cdots$$

s.t. $d_{n+1} \circ d_n = 0$.

Given a chain complex C_*, we can obtain a cochain complex $Hom(C_*, R)$ which looks like

$$\cdots \to Hom(C_{n-1}, R) \to Hom(C_n, R) \to Hom(C_{n+1}, R) \to \cdots$$

Given a chain complex C_*, we define the group of n-cycles to be $Z_n(C_*) = \ker d_n$, and the group of n-boundaries $B_n(C_*) = Im(d_{n+1})$. Check for yourself that $B_n(C_*) \subseteq Z_n(C_*) \subseteq C_n$.

We define the **nth-homology** of C_* to be $H_n(C_*) = \frac{Z_n}{B_n}$.

Definition 26.2. A chain map $f_* : C_* \to D_*$ between complexes is a collection of R-module maps $f_n : C_n \to D_n$ s.t.

$$\begin{tikzcd}
\cdots \arrow[r] & C_{n+1} \arrow[r] \arrow[d, "f_{n+1}"] & C_n \arrow[r] \arrow[d, dashed, "f_n"] & C_{n-1} \arrow[r] \arrow[d, dashed, "f_{n-1}"] & \cdots \\
\cdots \arrow[r] & D_{n+1} \arrow[r] & D_n \arrow[r] & D_{n-1} \arrow[r] & \cdots
\end{tikzcd}$$

commutes.

Proposition 26.3. *A chain map $f_* : C_* \to D_*$ induces a map on homology $H_n(f) : H_n(C_*) \to H_n(D_*)$.*

Proof. Check for yourself that the commutativity of

$$\begin{tikzcd}
\cdots \arrow[r] & C_{n+1} \arrow[r] \arrow[d, "f_{n+1}"] & C_n \arrow[r] \arrow[d, dashed, "f_n"] & C_{n-1} \arrow[r] \arrow[d, dashed, "f_{n-1}"] & \cdots \\
\cdots \arrow[r] & D_{n+1} \arrow[r] & D_n \arrow[r] & D_{n-1} \arrow[r] & \cdots
\end{tikzcd}$$

sends cycles to cycles, and boundaries to boundaries. So there is a well-defined map $H_n(C_*) \to H_n(D_*)$. □

Definition 26.4. Let $f_*, g_* : C_* \to D_*$ be two morphism of chain complexes. Then f_* and g_* are chain homotopic if there $\exists h_* : C_* \to D_*$

$$\begin{tikzcd}
\cdots \arrow[r] & C_{n+1} \arrow[r] \arrow[d] & C_n \arrow[r] \arrow[d] \arrow[dl, "h_n"] & C_{n-1} \arrow[r] \arrow[d] \arrow[dl, "h_{n-1}"] & \cdots \\
\cdots \arrow[r] & D_{n+1} \arrow[r] & D_n \arrow[r] & D_{n-1} \arrow[r] & \cdots
\end{tikzcd}$$

s.t. $f - g = hd + dh$.

Proposition 26.5. *If $f_*, g_* : C_* \to D_*$ are chain homotopic, then the induced maps on homology are equal, i.e. $H_n(f) = H_n(g) : H_n(C_*) \to H_n(D_*)$.*

Proof. Check for yourself that from the commutativity of the diagram, the map on homology induced by $f_* - g_*$ is zero. □

Theorem 26.6. *A short exact sequence of chain complexes is a collection of SES*

$$0 \to A_n \to B_n \to C_n \to 0$$

s.t.

$$\begin{tikzcd}
 & \vdots \arrow[d] & \vdots \arrow[d] & \vdots \arrow[d] & \\
0 \arrow[r] & A_{n+1} \arrow[r] \arrow[d] & B_{n+1} \arrow[r] \arrow[d] & C_{n+1} \arrow[r] \arrow[d] & 0 \\
0 \arrow[r] & A_n \arrow[r] \arrow[d] & B_n \arrow[r] \arrow[d] & C_n \arrow[r] \arrow[d] & 0 \\
0 \arrow[r] & A_{n-1} \arrow[r] \arrow[d] & B_{n-1} \arrow[r] \arrow[d] & C_{n-1} \arrow[r] \arrow[d] & 0 \\
 & \vdots & \vdots & \vdots &
\end{tikzcd}$$

commutes. A SES of chain complexes induces a long exact sequence of homology:

$$\begin{tikzcd}
 & & \cdots \arrow[dll] \\
H_{n+1}(A) \arrow[r] & H_{n+1}(B) \arrow[r] & H_{n+1}(C) \arrow[dll] \\
H_n(A) \arrow[r] & H_n(B) \arrow[r] & H_n(C) \arrow[dll] \\
H_{n-1}(A) \arrow[r] & H_{n-1}(B) \arrow[r] & H_{n-1}(C) \arrow[dll] \\
\cdots & &
\end{tikzcd}$$

Proof. See proof in section 9, page 23 of https://math.mit.edu/~hrm/papers/lectures-905-906.pdf. It will also tell you how to construct the boundary operator ∂. □

We will now talk about resolutions and derived functors, namely Tor and Ext.

The idea of resolutions is that free modules are the simplest objects in the category of R-modules. How far is a given object from a free R-module?

Definition 26.7. Let R be a ring. A free R-module is a direct sum $\bigoplus_I R = R^{(I)}$, where every element of $R^{(I)}$ is a finite linear combination.

An R-module P is projective if P is a direct summand of free R-modules. So there exists I and Q s.t. $P \oplus Q = R^{(I)}$.

WARNING: it's not true that a submodule of a free R-module is necessarily free as well.

Projective modules are

Proposition 26.8. *An R-module P is projective $\iff$ for every surjective morphism $g : M \to N$, and morphism $f : P \to N$, there exists $h : P \to M$ s.t.*

$$\begin{tikzcd}
M \arrow[r] & N \arrow[r] & 0 \\
& P \arrow[u, "f"'] \arrow[ul, dotted, "\exists"] &
\end{tikzcd}$$

commutes.

Proof. Let's prove the forward direction first. So assume that P is projective. Then there exists Q s.t. $P \oplus Q = R^{(I)}$. Let $(a_i)_{i \in I}$ be a basis of $R^{(I)}$. Note that we obtain a map $\widetilde{f} : R^{(I)} \to N$ by projecting $R^{(I)} \to P$, and then compose with the map $P \to N$.

$$\begin{tikzcd}
M \arrow[r] & N \arrow[r] & 0 \\
& R^{(I)} \arrow[u, "\widetilde{f}"] \arrow[r] & P \arrow[ul, "f"]
\end{tikzcd}$$

Note that since $M \to N$ is surjective, there exist b_i mapping to $f(a_i)$ for every i. To specify a map from a free R-module to another R-module, it suffices to specify where the generators go. So define a map $\widetilde{h} : R^{(I)} \to M$ via $a_i \mapsto b_i$. This gives us a map $h : P \to R^{(I)} \to M$.

For the reverse direction, note that you can always find a free module surjection $R^{(I)} \to P \to 0$. Then apply the assumption to the diagram

$$\begin{tikzcd}
R^{(I)} \arrow[r] & P \arrow[r] & 0 \\
& P \arrow[u, "Id"] \arrow[ul, "\exists"'] &
\end{tikzcd}$$

. $\square$

Proposition 26.9. *Let P be an R-module. TFAE:*

- *P is projective*
- *The functor $Hom_R(P, -)$ is exact*
- *Every SES $0 \to M \to N \to P \to 0$ is split. $N \cong M \oplus P$.*
- *P is a direct summand of a free R-module*

Example 26.10.

- Vector space over field k is projective.
- Note any finite abelian group is not projective over $\mathbb{Z}$.
- R PID, M f.g. R-module, then M projective $\iff$ M has no torsion $\iff$ M is free.

There is a dual notion: injective R-modules.

Definition 26.11. Let E be an R-module. E is injective if for every diagram

$$\begin{tikzcd}
0 \arrow[r] & N \arrow[r, "f"] \arrow[d, "g"] & M \arrow[dl, dashed, "\exists h"] \\
& E &
\end{tikzcd}$$

there exists $h : M \to E$ making the diagram commute.

We also have a list of equivalences for an R-module to be injective:

Proposition 26.12. *Let E be an R-module. TFAE:*

- *E is injective.*
- *$Hom_R(-, E)$ is exact.*
- *Every SES $0 \to E \to M \to N \to 0$ splits.*

Definition 26.13 (Resolutions)**.** Let M be an R-module. A **left resolution** of M is an exact sequence

$$\cdots \to P_2 \to P_1 \to P_0 \to M \to 0$$

constructed by first finding a projective R-module P_0 surjecting onto M, and if $\ker(P_0 \to M)$ is not zero, then find projective module P_1 surjecting onto $\ker(P_0 \to M)$. Continue this process.

If all P_i are free R-modules, then this is called a **free resolution**.

Example 26.14. Let R PID, M f.g. R-module. A left resolution of M is

$$\cdots \to 0 \to R^k = (a_1 R \oplus \cdots \oplus a_k R) \to R^n \oplus R^k \to M = R^n \oplus R/a_1 \oplus \cdots \oplus R/a_k$$

Definition 26.15. A right resolution is an exact sequence $0 \to M \to E_0 \to E_1 \to \cdots$, where E_k is injective module.

Theorem 26.16. *Every R-module has a free left resolution and an injective right resolution.*

Proof. Start with an R-module M. Consider surjection $\oplus_{m \in M} R \to M \to 0$. Then look at the kernel of this map, and repeat this process. This gives you a free resolution. Easy money.

Claim: there exists injection $M \hookrightarrow E_0$ where E_0 is injective. Then repeat this process on the cokernel of $M \hookrightarrow E_0$ to obtain $E_0 \to E_1$. □

All of this machinery with resolutions is useful for 'deriving' derived functors.

Fix R-module M. Consider right exact functor $F : Mod_R \to Ab$ from R-modules to abelian groups via $F(N) = M \otimes_R N$.

If you have a SES $0 \to M \to N \to P \to 0$, by definition of being a right exact functor, $F(M) \to F(N) \to F(P) \to 0$ is exact. But what do you get on the left hand side?

Let A be an R-module. Take projective resolution $P^* \to A \to 0$. Applying the functor F yields a chain complex (not necessarily exact)

$$\cdots \to F(P^1) \to F(P^0) \to F(A)$$

Then let the *nth* left derived functor of F be defined as $(L_n F)(A) := H_n(F(P^*))$. Check that $L_0 F = F$.

This is independent from projective resolutions. Proof of this is in Allufi Chapter 9 section 6-8.

Furthermore, if you have SES $0 \to A \to B \to C \to 0$ then you can get

$$\begin{tikzcd}
0 \arrow[r] & A \arrow[r] & B \arrow[r] & C \arrow[r] & 0 \\
0 \arrow[r] & P^* \arrow[r] \arrow[u] & M^* \arrow[r] \arrow[u] & N^* \arrow[r] \arrow[u] & 0
\end{tikzcd}$$

there exists SES of chain complexes, from which you get a LES of derived functors

$$\cdots \to (L_nF)(A) \to (L_nF)(B) \to (L_nF)(C) \to (L_{n-1}F)(A) \to \cdots$$