250B: Commutative Algebra

For the Morbidly Curious

Nir Elber

Spring 2022

Contents

THEME 1

INTRODUCTION

Hold tight to your geometric motivation as you learn the formal structures which have proved to be so effective in studying fundamental questions.

—Ravi Vakil

1.1 January 18

So it begins.

1.1.1 Logistics

Here are some logistic things.

- We are using Eisenbud's *Commutative Algebra: With a View Toward Algebraic Geometry*. We will follow it pretty closely.
- All exams will be open-book and at-home. The only restrictions are time constrains (1.5 hours, 1.5 hours, and 3 hours).
- The first homework will be posted on Monday, and it will be uploaded to bCourses.
- Supposedly there will be a reader for the course, but nothing is known about the reader.

1.1.2 Rings

Commutative algebra is about commutative rings.

Convention 1.1. All of our rings will have a 1_R element and be commutative, as God intended. We do permit the zero ring.

We are interested in particular kinds of rings. Here are some nice rings.

Definition 1.2 (Integral domain)**.** An *integral domain* is a (nonzero) ring R such that, for $a, b \in R$, $ab = 0$ implies $a = 0$ or $b = 0$.

Definition 1.3 (Units). Given a ring R, we define the group of *units* $R^\times$ to be the set of elements of R which have multiplicative inverses.

Definition 1.4 (Field). A *field* is a nonzero ring R for which $R = \{0\} \cup R^\times$.

Definition 1.5 (Reduced). A ring R is *reduced* if and only if it has no nonzero nilpotent elements.

Definition 1.6 (Local). A ring R is *local* if and only if it has a unique (proper) maximal ideal.

It might seem strange to have lots a unique maximal ideal; here are some examples.

Example 1.7. Any field is a local ring with maximal ideal $\{0\}$.

Example 1.8. The ring of p-adic integers $\mathbb{Z}_p$ is a maximal ring with maximal ideal (p).

Example 1.9. The ring $\mathbb{Z}/p^2\mathbb{Z}$ is a local ring with maximal ideal $p\mathbb{Z}/p^2\mathbb{Z}$.

1.1.3 Ideals

The following is our definition.

Definition 1.10 (Ideal). Given a ring R, a subset $I \subseteq R$ is an *ideal* if it contains 0 and is closed under R-linear combination.

Given a ring R, we will write

$$(S) \subseteq R$$

to be the ideal generated by the set $S \subseteq R$.

Definition 1.11 (Finitely generated). An ideal $I \subseteq R$ is said to be *finitely generated* if and only if there are finitely many elements $r_1, \ldots, r_n \in R$ such that $I = (r_1, \ldots, r_n)$.

Definition 1.12 (Principal). An ideal $I \subseteq R$ is *principal* if and only if there exists $r \in R$ such that $I = (r)$.

We mentioned maximal ideals above; here is that definition.

Definition 1.13 (Maximal). An ideal $I \subseteq R$ is *maximal* if and only if $I \neq R$ and, for any ideal $J \subseteq R$, $I \subseteq J$ implies $I = J$ or $I = R$.

Alternatively, an ideal $I \subseteq R$ is maximal if and only if the quotient ring R/I is a field. We will not show this here.

Definition 1.14 (Prime). An ideal $I \subseteq R$ is *prime* if and only if $I \neq R$ and, for $a, b \in R$, $ab \in I$ implies $a \in I$ or $b \in I$.

Again, we can view prime ideals by quotient: I is prime if and only if R/I is a (nonzero) integral domain.

With the above definitions in mind, we can define the following very nice class of rings.

Definition 1.15 (Principal ideal)**.** An integral domain R is a *principal ideal domain* if and only if all ideals of R are principal.

Example 1.16. The ring $\mathbb{Z}$ is a principal ideal domain. The way this is showed is by showing $\mathbb{Z}$ is Euclidean. Explicitly, fix $I \subseteq \mathbb{Z}$ an ideal. Then if $I \neq (0)$, find an element of $m \in I$ of minimal absolute value and use the division algorithm to write, for any $a \in I$,

$$a = mq + r$$

for $0 \leq r < m$. But then $r \in I$, so minimality of m forces $r = 0$, so $a \in (m)$, finishing.

Example 1.17. For a field k, the ring $k[x]$ is a principal ideal domain. Again, this is because $k[x]$ is a Euclidean domain, where we measure size by degree.

1.1.4 Unique Factorization

We have the following definition.

Definition 1.18 (Irreducible, prime)**.** Fix R a ring and $r \in R$ an element.

- We say that $r \in R$ is *irreducible* if and only if r is not a unit, not zero, and $r = ab$ for $a, b \in R$ implies that one of a or b is a unit.
- We say that $r \in R$ is *prime* if and only if r is not a unit, not zero, and (r) is a prime ideal: $ab \in (r)$ implies $a \in (r)$ or $b \in (r)$.

This gives rise to the following important definition.

Definition 1.19 (Unique factorization domain)**.** Fix R an integral domain. Then R is a *unique factorization domain* if and only if all nonzero elements of R have a factorization into irreducible elements, unique up to permutation and multiplication by units.

Remark 1.20. Units have the "empty" factorization, consisting of no irreducibles.

Example 1.21. The ring $\mathbb{Z}$ is a unique factorization domain. We will prove this later.

Note there are two things to check: that the factorization exists and that it is unique. Importantly, existence does not imply uniqueness.

Exercise 1.22. There exists an integral domain R such that every element has a factorization into irreducibles but that this factorization is not unique.

Proof. Consider the subring $R := k\left[x^2, xy, y^2\right] \subseteq k[x, y]$. Here x^2, xy, y^2 are all irreducibles because the only way to factor a quadratic nontrivially would be into linear polynomials, but R has no linear polynomials.

However, these elements are not prime:

$$x^2 \mid xy \cdot xy$$

while x^2 does not divide xy. More concretely, $(xy)(xy) = x^2 \cdot y^2$ provides non-unique factorization into irreducibles. ■

The following condition will provide an easier check for the existence of factorizations.

Definition 1.23 (Ascending chain condition)**.** Given a collection of sets $\mathcal{S}$, we say that $\mathcal{S}$ *has the ascending chain condition* (ACC) if and only every chain of sets in $\mathcal{S}$ must eventually stabilize.

Definition 1.24 (ACC for principal ideals)**.** A ring R has the ascending chain condition for principal ideals if and only if every ascending chain of principal ideals

$$(a_1) \subseteq (a_2) \subseteq (a_3) \subseteq \cdots$$

has some N such that $(a_N) = (a_n)$ for $n \geq N$.

Now, the fact that $\mathbb{Z}$ is a unique factorization domain roughly comes from the fact that $\mathbb{Z}$ is a principal ideal domain.

Theorem 1.25. Fix R a ring. Then R is a principal ideal domain implies that R is a unique factorization domain.

Proof. We start by showing that R has the ascending chain for principal ideals. Indeed, suppose that we have some ascending chain of principal ideals

$$(a_1) \subseteq (a_2) \subseteq (a_3) \subseteq \cdots .$$

Then the key idea is to look at the union of all these ideals, which will be an ideal by following the chain condition. However, R is a principal ideal domain, so there exists $b \in R$ such that

$$\bigcup_{k=1}^{\infty} (a_k) = (b).$$

However, it follows $b \in (a_N)$ for some N, in which case $(a_n) = (a_N)$ for each $n \geq N$.

We can now show that every nonzero element in R has a factorization into irreducibles.

Lemma 1.26. Suppose that a ring R has the ascending chain condition for principal ideals. Then every nonzero element of R has a factorization into irreducibles.

Proof. Fix some $r \in R$. If $(r) = R$, then r is a unit and hence has the empty factorization.

Otherwise, note that every ideal can be placed inside a maximal and hence prime ideal, so say that $(r) \subseteq \mathfrak{m}$ where $\mathfrak{m}_1$ is prime; because R is a principal ring, we can say that $\mathfrak{m} = (\pi_1)$ for some $\pi_1 \in R$, so $\pi_1 \mid r$. This π_1 should go into our factorization, and we have left to factor r/π_1.

The above argument can then be repeated for r/π_1, and if r/π_1 is not a unit, then we get an irreducible π_2 and consider $r/(\pi_1\pi_2)$. This process must terminate because it is giving us an ascending chain of principal ideals

$$(r) \subseteq \left(\frac{r}{\pi_1}\right) \subseteq \left(\frac{r}{\pi_1\pi_2}\right) \subseteq \cdots ,$$

which must stabilize eventually and hence must be finite. Thus, there exists N so that

$$\left(\frac{r}{\pi_1\pi_2\cdots\pi_N}\right) = R,$$

so $r = u\pi_1\pi_2\cdots\pi_N$ for some unit $u \in R^\times$. ■

It remains to show uniqueness of the factorizations. The main idea is to show that all prime elements of R are the same as irreducible ones. One direction of the implication does not need the fact that R is a principal ring.

Lemma 1.27. Fix R an integral domain. Then any prime $r \in R$ is also irreducible.

Proof. Note that r is not a unit and not zero because it is prime. Now, suppose that $r = ab$ for $a, b \in R$; this implies that $r \mid ab$, so because r is prime, without loss of generality we force $r \mid a$. Then, dividing by r (which is legal because R is an integral domain), we see that

$$1 = (a/r)b,$$

so b is a unit. This finishes showing that r is irreducible. ■

Warning 1.28. The reverse implication of the above lemma is not true for arbitrary integral domains: in the ring $\mathbb{Z}[\sqrt{-5}]$, there is the factorization

$$\left(1+\sqrt{-5}\right)\left(1-\sqrt{-5}\right) = 2 \cdot 3.$$

One can show that all elements above are irreducible, but none of them are prime.

The other side of this is harder. Pick up some $\pi \in R$ which is irreducible, and we show that π is prime. In fact, we will show stronger: we will show that (π) is a maximal ideal. Note $(\pi) \neq R$ because π is not a unit.

Indeed, suppose that $(\pi) \subseteq (r)$ for some ideal $(r) \subseteq R$. Then

$$\pi = rs$$

for some $s \in R$. Now, one of r or s must be a unit (π is irreducible). If s is a unit, then $(\pi) = (r)$; if r is a unit then $(r) = R$. This finishes showing that (π) is maximal.

From here we show the uniqueness of our factorizations.

Lemma 1.29. Fix R a domain in which irreducible element is prime. Then R factorizations into irreducibles in R are unique up to units and permutation.

Proof. Note that the lemma does not assert that factorization into irreducibles in R actually exist.

We proceed inductively, noting that two empty factorizations are of course the same up to permutation and units. Now suppose we have two factorizations of irreducibles

$$\prod_{k=1}^{m} p_k = \prod_{\ell=1}^{n} q_\ell,$$

where $m + n \geq 1$. Note that we cannot have exactly one side with no primes because this would make a product of irreducibles into 1, and irreducibles are not units.

Now, consider p_m. It is irreducible and hence prime and hence divides one of the right-hand factors; without loss of generality $p_m \mid q_n$, so $(q_n) \subseteq (p_m)$. But (p_m) and (q_n) are both maximal ideals, so $(q_n) \subseteq (p_m)$ forces equality, so p_m/q_n is a unit. So we may cross off p_m and q_n and continue downwards by induction. ■

The above lemma finishes the proof because we showed principal ideal domains satisfy that all irreducible elements are prime. ■

Remark 1.30 (Nir)**.** In fact, if a domain R satisfies the ascending chain condition on principal ideals and has that all irreducibles elements are prime, then R will be a unique factorization domain. Indeed, factorization into irreducibles exists by Lemma 1.26 and is unique by Lemma 1.29.

Remark 1.31 (Nir)**.** We can even provide a converse for Lemma 1.29: if R is a unique factorization domain, we claim all irreducible elements are prime. Namely, if π is an irreducible element such that $\pi \mid ab$, then we can write out factorizations for $a \cdot b$ and $\pi \cdot (ab)/\pi$. By uniqueness, they must be the same up to units and permutation, so $u\pi$ (for some $u \in R^\times$) will appear in either the factorization of a or of b, giving $\pi \mid a$ or $\pi \mid b$.

Example 1.32. Fix k a field. Because $k[x]$ is a principal ideal domain, it is also a unique factorization domain.

1.1.5 Digression on Gaussian Integers

As an aside, the study of unique factorization came from Gauss's study of the Gaussian integers.

Definition 1.33 (Gaussian integers)**.** The *Gaussian integers* are the ring

$$\mathbb{Z}[i] := \{a + bi : a, b \in \mathbb{Z}\}.$$

One can in fact check that $\mathbb{Z}[i]$ is a principal ideal domain, which implies that $\mathbb{Z}[i]$ is a unique factorization domain. The correct way to check that $\mathbb{Z}[i]$ is a principal ideal domain is to show that it is Euclidean.

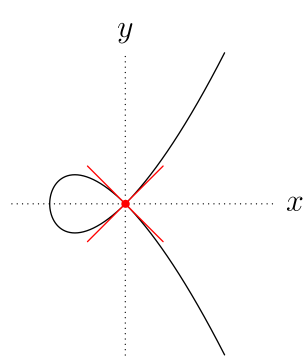
Lemma 1.34. The ring $\mathbb{Z}[i]$ is Euclidean, where our norm is $\mathrm{N}(a + bi) := a^2 + b^2$. In other words, given $\alpha, \beta \in \mathbb{Z}[i]$, we need to show that there exists $q \in \mathbb{Z}[i]$ such that

$$a = bq + r$$

where $r = 0$ or $\mathrm{N}(r) < \mathrm{N}(\beta)$.

Proof. The main idea is to view $\mathbb{Z}[i] \subseteq \mathbb{C}$ geometrically as in $\mathbb{R}^2$. We may assume that $|\beta| \le |\alpha|$, and then it suffices to show that in this case we may find q so that $a - bq$ has smaller norm than a and induct.

Well, for this it suffices to look at $a + b, a - b, a + ib, a - ib$; the proof that one of these works essentially boils down to the following image.



Note that at least one of the endpoints here has norm smaller than a. ∎

What about the primes? Well, there is the following theorem which will classify.

Theorem 1.35 (Primes in $\mathbb{Z}[i]$)**.** An element $\pi := a + bi \in \mathbb{Z}[i]$ is *prime* if and only if $\mathrm{N}(\pi)$ is a $1 \pmod 4$ prime, $(pi) = (1 + i)$, or $(\pi) = (p)$ for some prime $p \in \mathbb{Z}$ such that $p \equiv 3 \pmod 4$.

We will not fully prove this; it turns out to be quite hard, but we can say small things: for example, $3 \pmod 4$ primes p remain prime in $\mathbb{Z}[i]$ because it is then impossible to solve

$$p = a^2 + b^2$$

by checking $\pmod 4$.

Remark 1.36. This sort of analysis of "sums of squares" can be related to the much harder analysis of Fermat's last theorem, which asserts that the Diophantine equation

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

for $xyz \neq 0$ integers such that $n > 2$.

1.1.6 Noetherian Rings

We have the following definition.

Definition 1.37 (Noetherian ring)**.** A ring R is said to be *Noetherian* if its ideals have the ascending chain condition.

There are some equivalent conditions to this.

Proposition 1.38. Fix R a ring. The following conditions are equivalent.

- R is Noetherian.
- Every ideal of R is finitely generated.

Proof. We show the directions one at a time.

- Suppose that R has an ideal which is not finitely generated, say $J \subseteq R$. Then we may pick up any $a_1 \in J$ and observe that $J \neq (a_1)$.

  Then we can pick up $a_2 \in J \setminus (a_1)$ and observe that $J \neq (a_1, a_2)$. So then we pick up $a_3 \in J \setminus (a_1, a_2)$ and continue. This gives us a strictly ascending chain

  $$(a_1) \subsetneq (a_1, a_2) \subsetneq (a_1, a_2, a_3) \subsetneq \cdots,$$

  contradicting the ascending chain condition.

- Suppose that every ideal is finitely generated. Then, given any ascending chain of ideals

  $$I_1 \subseteq I_2 \subseteq I_3 \subseteq \cdots,$$

  we need this chain to stabilize. Well, the union

  $$I \coloneqq \bigcup_{k=1}^{\infty} I_k$$

  is also an ideal, and it must be finitely generated, so suppose $I = (a_1, a_2, \ldots, a_m)$. However, each a_k must appear in some $I_\bullet$ (and then each $I_\bullet$ after that one as well); choose N large enough to that $a_k \in I_N$ for each k. This implies that, for any $n \geq N$,

  $$I_n \subseteq I = (a_1, a_2, \ldots, a_m) \subseteq I_N \subseteq I_n$$

  verifying that the chain has stabilized. ■

Remark 1.39 (Nir)**.** In fact, R being Noetherian is also equivalent to every set of nonempty ideals having a maximal element. In fact, for any partially ordered set $\mathcal{P}$, the condition that every ascending chain stabilizes is equivalent to every subset having a maximal element.

- If every subset has a maximal element, then each ascending chain (which is a subset) has a maximal element, which must be the stabilizing element.
- Conversely, if there is a subset with no maximal element, we can inductively choose larger and larger elements from the subset to make a non-stabilizing ascending chain.

A large class of rings turn out to be Noetherian, and in fact oftentimes Noetherian rings can build more Noetherian rings.

Proposition 1.40. Fix R a Noetherian ring and $I \subseteq R$ an ideal. Then R/I is also Noetherian.

Proof. Any chain of ideals in R/I can be lifted to a chain in R by taking pre-images along $\varphi : R \twoheadrightarrow R/I$. Then the chain must stabilize in R, so they will stabilize back down in R/I as well. ■

The above works because taking quotients is an algebraic operation. In contrast, merely being a subring is less algebraic, so it is not so surprising that $R_1 \subseteq R_2$ with R_2 Noetherian does not imply that R_1 is Noetherian.

Example 1.41. The ring $k[x_1, x_2, \ldots]$ is not Noetherian because we have the infinite ascending chain

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

However, $k[x_1, x_2, \ldots] \subseteq k(x_1, x_2, \ldots)$, and the latter ring is Noetherian because it is a field. (Fields are Noetherian because they have finitely many ideals and therefore satisfy the ascending chain condition automatically.)

Here is another way to generate Noetherian rings.

Theorem 1.42 (Hilbert basis)**.** If R is a Noetherian ring, then $R[x]$ is also a Noetherian ring.

Corollary 1.43. By induction, if R is Noetherian, then $R[x_1, x_2, \ldots, x_n]$ is Noetherian for any finite n.

Warning 1.44. Again, it is not true that $R[x_1, x_2, \ldots]$ is Noetherian, even though "inducting" with the Hilbert basis theorem might suggest that it is.

Proof of Theorem 1.42. The idea is to use the degree of polynomials to measure size. Fix $I \subseteq R[x]$ an ideal, and we apply the following inductive process.

- Pick up $f_1 \in I$ of minimal degree in I.
- If $I = (f_1)$ then stop. Otherwise, find $f_2 \in I \setminus (f_1)$ of minimal degree.
- In general, if $I \neq (f_1, \ldots, f_n)$, then pick up $f_{n+1} \in I \setminus (f_1, \ldots, f_n)$ of minimal degree.

Importantly, we do not know that there are only finitely many $f_\bullet$ yet.

Now, look at the leading coefficients of the $f_\bullet$, which we name $a_\bullet$. However, the ideal

$$(a_1, a_2, \ldots) \subseteq R$$

must be finitely generated, so there is some finite N such that

$$(a_1, a_2, \ldots) = (a_1, a_2, \ldots, a_N).$$

To finish, we claim that

$$I \stackrel{?}{=} (f_1, f_2, \ldots, f_N).$$

Well, suppose for the sake of contradiction that we had some $f_{N+1} \in I \setminus (f_1, f_2, \ldots, f_N)$ of least degree. We must have $\deg f_{N+1} \geq \deg f_\bullet$ for each $f_\bullet$, or else we contradict the construction of $f_\bullet$ as being the least degree.

To finish, we note $a_{N+1} \in (a_1, a_2, \ldots, a_N)$, so we are promised constants $c_1, c_2, \ldots, c_N$ such that

$$a_{N+1} = \sum_{k=1}^{N} c_k a_k.$$

In particular, the polynomial

$$g(x) := f_{N+1}(x) - \sum_{k=1}^{N} c_k a_k x^{(\deg g)-(\deg f_k)} f_k(x),$$

will be guaranteed to kill the leading term of $f_{N+1}(x)$. But $g \equiv f_{N+1} \pmod{I}$, so g is suddenly a polynomial also not in I while of smaller degree than f_{N+1}, which is our needed contradiction. ■

1.1.7 Modules

To review, we pick up the following definition.

Definition 1.45 (Module)**.** Fix R a ring. Then M is an abelian group with an R-action. Explicitly, we have the following properties; fix any $a, b \in R$ and $m, n \in M$.

- $1_R m = m$.
- $a(bm) = (ab)m$.
- $(a+b)m = am + bm$.
- $a(m+n) = am + an$.

Example 1.46. Any ideal $I \subseteq R$ is an R-module. In fact, ideals exactly correspond to the R-submodules of R.

Example 1.47. Given any two R-module M with a submodule $N \subseteq M$, we can form the quotient M/N.

Modules also have a notion of being Noetherian.

Definition 1.48 (Noetherian module)**.** We say that an R-module M is *Noetherian* if and only if all R-submodules of M are finitely generated.

Remark 1.49. Equivalently, M is Noetherian if and only if the submodules of M have the ascending chain condition. The proof of the equivalence is essentially the same as Proposition 1.38.

Because modules are slightly better algebraic objects than rings, we have more ways to stitch modules together and hence more ways to make Noetherian modules. Here is one important way.

Proposition 1.50. Fix a short exact sequence

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

of R-modules. Then B is Noetherian if and only if A and C are both Noetherian.

Proof. We will not show this here; it is on the homework. Nevertheless, let's sketch the forwards direction, which is easier. Take B Noetherian.

- To show that A is Noetherian, it suffices to note that any submodules $M \subseteq A$ will also be a submodule of B and hence be finitely generated because B is Noetherian.
- To show that C is Noetherian, we note that C is essentially a quotient of B, so we can proceed as we did in Proposition 1.40.[1] ■

Because we like Noetherian rings, the following will be a useful way to make Noetherian modules from them.

Proposition 1.51. Every finitely generated R-module over a Noetherian ring R is Noetherian.

Proof. If M is finitely generated, then there exists some $n \in \mathbb{N}$ and surjective morphism

$$\varphi : R^n \twoheadrightarrow M.$$

Now, because R is Noetherian, R^n will be Noetherian by an induction: there is nothing to say when $n = 1$. Then the inductive step looks at the short exact sequence

$$0 \to R \to R^n \to R^{n-1} \to 0.$$

Here, the fact that R and R^{n-1} are Noetherian implies that R^n is Noetherian by Proposition 1.50. Anyways, the point is that M is the quotient of a Noetherian ring and hence Noetherian by Proposition 1.50 (again). ■

Here is the analogous result for algebras.

Definition 1.52 (Algebra)**.** An R-*algebra* S is a ring equipped with a homomorphism $\iota : R \to S$. Equivalently, we may think of an R-algebra as a ring with an R action.

Proposition 1.53. Fix R a Noetherian ring. Then any finitely generated R-algebra is Noetherian.

Proof. Saying that S is a finitely generated R-algebra (with associated map $\iota : R \to S$) is the same as saying that there is a surjective morphism

$$\varphi : R[x_1, \ldots, x_n] \twoheadrightarrow S$$

for some $n \in \mathbb{N}$. (Explicitly, $\varphi|_R = \iota$, and each x_k maps to one of the finitely many generating elements of S.) But then S is the quotient of an $R[x_1, \ldots, x_n]$, which is Noetherian by Corollary 1.43, so S is Noetherian as well by Proposition 1.40. ■

[1] In fact, Proposition 1.40 is exactly this in the case where $B = R$.

1.1.8 Invariant Theory

In the following discussion, fix k a field of characteristic 0, and let G be a finite group or $\mathrm{GL}_n(\mathbb{C})$ (say). Now, suppose that we have a map

$$G \to \mathrm{GL}_n(k).$$

Then this gives $k[x_1, \ldots, x_n]$ a G-action by writing $gf(\vec{x}) := f(g^{-1}\vec{x})$. The central question of invariant theory is then as follows.

Question 1.54 (Invariant theory)**.** Fix everything as above. Then can we describe $k[x_1, \ldots, x_n]^G$?

By checking the group action, it is not difficult to verify that $k[x_1, \ldots, x_n]^G$ is a subring of $k[x_1, \ldots, x_n]$. For brevity, we will write $R := k[x_1, \ldots, x_n]$.

Here is a result of Hilbert which sheds some light on our question.

Theorem 1.55 (Hilbert's finiteness)**.** Fix everything as above with G finite. Then $R^G = k[x_1, \ldots, x_n]^G$ is a finitely generated k-algebra and hence Noetherian.

Proof. We follow Eisenbud's proof of this result. We pick up the following quick aside.

Lemma 1.56. Fix everything as above. If we write some $f \in R^G$ as

$$f = \sum_{d=0}^{\deg f} f_d$$

where f_d is homogeneous of degree d (i.e., f_d contains all terms of f of degree d), then $f_d \in R^G$ as well.

Proof. Indeed, multiplication by $\sigma \in G$ will not change the degree of any monomial (note G is acting as $\mathrm{GL}_n(k)$ on the variables themselves), so when we write

$$\sum_{d=0}^{\deg f} \sigma f_d = \sigma f = f = \sum_{d=0}^{\deg f} f_d,$$

we are forced to have $\sigma f_d = f_d$ by degree comparison arguments. ■

Remark 1.57. In other words, the above lemma asserts that R^G may be graded by degree.

The point of the above lemma is that decomposition of an element $f \in R^G$ into its homogeneous components still keeps the homogeneous components in R^G, which is a fact we will use repeatedly.

We now proceed with the proof. The main ingredients are the Hilbert basis theorem and the Reynolds operator. Here is the Reynolds operator.

Definition 1.58 (Reynolds operator)**.** Fix everything as above. Then we define the *Reynolds operator* $\varphi : R \to R$ as

$$\varphi(f) := \frac{1}{\#G} \sum_{\sigma \in G} \sigma f$$

for given $f \in R$. Note that division by $\#G$ is legal because k has characteristic zero.

It is not too hard to check that $\varphi : R \to R^G$ and $\varphi|_{R^G} = \mathrm{id}_{R^G}$. Additionally, we see $\deg \varphi(f) \le \deg f$.

Let $\mathfrak{m} \subseteq R^G$ be generated by the homogeneous elements of R^G of positive degree. The input by the Hilbert basis theorem is to say that $\mathfrak{m}R \subseteq R$ is an R-ideal, and R is Noetherian (by the Hilbert basis theorem!), so $\mathfrak{m}R$ is finitely generated. So set

$$\mathfrak{m}R = (f_1, \ldots, f_n) = f_1R + \cdots + f_nR.$$

Now, because each $f_\bullet$ lives in $\mathfrak{m}R$, we may decompose each $f_\bullet$ into an R-linear combination of G-invariant pieces in $\mathfrak{m}$, so we may assume that the $f_\bullet$ are G-invariant. Further, by decomposing the $f_\bullet$ into their (finitely many) homogeneous components, we may assume that the $f_\bullet$ are homogeneous.

Now we claim that the $f_\bullet$ generate R^G (as a k-algebra). Note that there is actually nontrivial difficulty turning the above finite generation of $\mathfrak{m}R$ as an R-module into finite of R^G as a k-algebra and that these notions are nontrivially different. I.e., we are claiming

$$R^G \stackrel{?}{=} k[f_1, \ldots, f_n].$$

Certainly we have $\supseteq$ here. For $\subseteq$, we show that any $f \in R^G$ lives in $k[f_1, \ldots, f_n]$ by induction. By decomposing f into homogeneous parts, we may assume that f is homogeneous.

We now induct on $\deg f$. If $\deg f = 0$, then $f \in k \subseteq k[f_1, \ldots, f_n]$. Otherwise, f is homogeneous of positive degree and hence lives in $\mathfrak{m}$. In fact, $f \in \mathfrak{m}R$, so we may write

$$f = \sum_{i=1}^n g_i f_i.$$

Note that, because f and f_i are all homogeneous, we may assume that the g_i is also homogeneous because all terms in g_i of degree not equal to

$$\deg f - \deg f_i$$

will have to cancel out in the summation and hence may as well be removed entirely. In particular, each g_i has $g_i = 0$ or is homogeneous of degree $\deg f - \deg f_i$, so $\deg g_i < \deg f$ always.

We would like to finish the proof by induction, noting that $g_i \in R^G$ and $\deg g_i < \deg f$ forces $g_i \in k[f_1, \ldots, f_n]$, and hence $f \in k[f_1, \ldots, f_n]$ by summation. However, we cannot do that because we don't actually know if $g_i \in R^G$! To fix this problem, we apply the Reynolds operator, noting

$$f = \varphi(f) = \sum_{i=1}^n \varphi(g_i) f_i.$$

So now we may say that $\varphi(g_i) \in R^G$ and $\deg \varphi(g_i) < \deg f$, so $\varphi(g_i) \in k[f_1, \ldots, f_n]$, and hence $f \in k[f_1, \ldots, f_n]$ by summation. This finishes. ■

The main example here is as follows.

> **Exercise 1.59.** Let S_n act on $R := k[x_1, \ldots, x_n]$ as follows: $\sigma \in S_n$ acts by $\sigma x_m := x_{\sigma m}$. Then we want to describe R^G, the *homogeneous polynomials in n letters.*

Proof. We won't work this out in detail here, but the main point is that the fundamental theorem of symmetric polynomials tells us that

$$R^G = k[e_1, e_2, \ldots, e_n],$$

where the $e_\bullet$ are *elementary symmetric functions.* Namely,

$$e_m := \sum_{\substack{S \subseteq \{1, \ldots, n\} \\ \#S = m}} \prod_{s \in S} x_s.$$

It is quite remarkable that R^G turned out to be a freely generated k-algebra, just like R. ■

Here is more esoteric example.

Exercise 1.60. Let $G =: \{1, g\} \cong \mathbb{Z}/2\mathbb{Z}$ act on $R := k[x, y]$ by $g \cdot x = -x$ and $g \cdot y = -y$. Then we want to describe R^G.

Proof. Here, R^G consists of all polynomials $f(x, y)$ such that $f(x, y) = f(-x, -y)$. By checking coefficients of the various $x^m y^n$ terms, we see that $f(x, y) = f(-x, -y)$ is equivalent to forcing all terms of odd degree to have coefficient zero.

In other words, the terms of even degree are the only ones which can have nonzero coefficient. Each such term $x^a y^b$ (taking $a \geq b$ without loss of generality) can be written as

$$x^a y^b = x^{a-b}(xy)^b = \left(x^2\right)^{(a-b)/2} (xy)^b,$$

where $a - b \equiv a + b \equiv 0 \pmod 2$ justifies the last equality. So in fact we can realize R^G as

$$R^G = k\left[x^2, xy, y^2\right].$$

To see that this ring is Noetherian, we note that there is a surjection

$$\varphi : k[u, v, w] \to k\left[x^2, xy, y^2\right]$$

taking $u \mapsto x^2$ and $v \mapsto xy$ and $w \mapsto y^2$. Thus, R is the quotient of a Noetherian ring and hence Noetherian itself. In fact, we can check that[2] $\ker \varphi = \left(uw - v^2\right)$ so that

$$R^G \cong \frac{k[u, v, w]}{(uw - v^2)}.$$

Even though R^G is Noetherian, it is not a freely generated k-algebra (i.e., a polynomial ring over k) because it is not a unique factorization domain! ■

Next class we will start talking about the Nullstellensatz, which has connections to algebraic geometry.

1.2 January 20

We continue following the Eisenbud machine.

1.2.1 Affine Space

To begin our discussion, we start with some geometry.

Definition 1.61 (Affine space)**.** Given a field k and positive integer n, we define n-dimensional *affine space* over k to be $\mathbb{A}^d(k) := k^n$.

Now, given affine space $\mathbb{A}^n(k)$, we are interested in studying subsets which are solutions to some set of polynomial equations

$$f_1, \ldots, f_n \in k[x_1, \ldots, x_d].$$

This gives rise to the following definition.

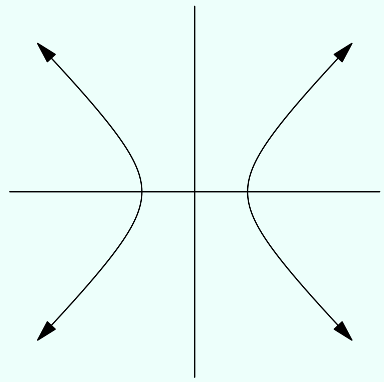
Definition 1.62 (Algebraic)**.** A subset $X \subseteq \mathbb{A}^n(k)$ is (affine) *algebraic* if and only if it is the set of solutions to some system of polynomials equations $f_1, \ldots, f_n \in k[x_1, \ldots, x_d]$.

[2] Certainly $uw - v^2 \in \ker \varphi$. In the other direction, any term $u^a v^b w^c$ can be written $\pmod{uw - v^2}$ as a term not having both u and w. However, each $x^d y^e$ has a unique representation in exactly one of the ways $u^a v^b \mapsto x^{2a+b} y^b$ $(a > 0)$ or $v^b w^c \mapsto x^b y^{b+2c}$ $(c > 0)$ or $v^b \mapsto x^b y^b$, so after applying the $\pmod{uw - v^w}$ movement, we see that the kernel is trivial.

Example 1.63. The hyperbola

$$\{(x,y) \in \mathbb{R}^2 : x^2 - y^2 - 1 = 0\}$$

is an algebraic set. Geometrically, it looks like the following.



Example 1.64. The set $\varnothing \subseteq \mathbb{A}^1(\mathbb{R})$ is algebraic because it is the set of solutions to the equation $x^2+1=0$ in $\mathbb{R}$.

The above example is a little disheartening because it feels like x^2+1 really ought to have a solution, namely $i \in \mathbb{C}$. More explicitly, there are no obvious algebraic obstructions that make x^2+1 not have a solution. So with this in mind, we make the following convention.

Convention 1.65. In the following discussion on the Nullstellensatz, k will always be an algebraically closed field.

1.2.2 Nullstellensatz

The Nullstellensatz is very important.

Remark 1.66. Because the Nullstellensatz is important, its name is in German (which was the language of Hilbert).

Now, the story so far is that we can take a set of polynomials and make algebraic sets as their solution set. We can in fact go in the opposite direction.

Definition 1.67 ($I(X)$)**.** If $X \subseteq \mathbb{A}^n(k)$ is an (affine) algebraic set, we define

$$I(X) := \{f \in k[x_1, \ldots, x_n] : f(X) = 0\}.$$

It is not hard to check that $I(X) \subseteq k[x_1, \ldots, x_n]$ is in fact an ideal. Namely, if $f, g \in I(X)$ and $r, s \in k[x_1, \ldots, x_n]$, then we need to know $rf + sg \in I(X)$ as well. Well, for any $x \in X$, we see

$$(rf+sg)(x) = rf(x) + sg(x) = 0,$$

so $rf + sg \in I(X)$ indeed.

One might hope that all ideals would be able to take the form $I(X)$, but this is not the case. For example, if $f^m(X) = 0$, then $f(X) = 0$ because k is a field. Thus, I will satisfy the property that $f^m \in I$ implies $f \in I$. To keep track of this obstruction, we have the following definition.

Definition 1.68 (Radical)**.** Fix R a ring. Given an R-ideal I, we define the *radical of I* to be

$$\operatorname{rad} I := \{x \in R : x^n \in I \text{ for some } n \geq 1\} \supseteq I.$$

If $I = \operatorname{rad} I$, then we call I a *radical ideal.*

To make sense, this definition requires a few sanity checks.

- We check $\operatorname{rad} I$ is in fact an ideal. Well, given $f, g \in \operatorname{rad} I$, there exists positive integers m and n such that $f^m, g^n \in I$. Then, for any $r, s \in R$, we see

$$(rf + sg)^{m+n} = \sum_{k=0}^{m+n} \left[\binom{m+n}{k} r^k s^{m+n-k} \cdot f^k g^{m+n-k} \right].$$

  However, for any k, we see that either $k \geq m$ or $m + n - k \geq n$, so all terms of this sum contain an f^m or g^n factor, so the sum is in I. So indeed, $rf + sg \in \operatorname{rad} I$.

- We check that $\operatorname{rad} I$ is a radical ideal. Well, if $f^n \in \operatorname{rad} I$ for some positive integer n, then $f^{mn} = (f^n)^m \in I$ for some positive integer m, from which $f \in \operatorname{rad} I$ follows.

- Certainly any $x \in I$ has $x^1 \in I$ and so $x \in \operatorname{rad} I$. Thus, $I \subseteq \operatorname{rad} I$.

It is not too hard to generate examples where the radical is strictly larger than the original ideal.

Example 1.69. Fix $R := \mathbb{Z}[\sqrt{2}]$ and $I = (2) = 2\mathbb{Z}[\sqrt{2}] = \{2a + 2b\sqrt{2} : a, b \in \mathbb{Z}\}$. Then $\left(\sqrt{2}\right)^2 = 2 \in I$ while $\sqrt{2} \notin I$, so $I \subsetneq \operatorname{rad} I$.

Example 1.70. Fix $R = \mathbb{Z}$ and $I = (4)$. Then $2^2 \in I$ but $2 \notin I$, so $I \subsetneq \operatorname{rad} I$.

Remark 1.71. Prime ideals will always be radical, essentially by definition: if $\mathfrak{p}$ is prime, then $x^n \in \mathfrak{p}$ implies that one of the factors of x^n will be in $\mathfrak{p}$, forcing $x \in \mathfrak{p}$.

Here is an alternative characterization of being radical.

Lemma 1.72. Fix R a ring. Then an ideal $I \subseteq R$ is radical if and only if R/I is reduced.

Proof. This proof is akin to the one showing $I \subseteq R$ is prime if and only if R/I is an integral domain.

Anyways, I is radical if and only if $x^n \in I$ for $x \in R$ and $n \geq 1$ implies $x \in I$. Translating this condition into R/I, we are saying that $[x]_I^n \in [0]_I$ for $[x]_I \in R/I$ and $n \geq 1$ implies that $[x]_I = [0]_I$. This is exactly the condition for R/I to be radical. ■

With all the machinery we have in place, we can now state the idea of Hilbert's Nullstellensatz.

Theorem 1.73 (Nullstellensatz, I)**.** Fix k an algebraically closed field. Then there is a bijection between radical ideals of $k[x_1, \ldots, x_n]$ and (affine) algebraic sets $\mathbb{A}^n(k)$.

So far we have defined a map from algebraic sets to radical ideals by $X \mapsto I(X)$. The reverse map is as follows.

Definition 1.74 ($Z(I)$)**.** Given a subset $S \subseteq k[x_1, \ldots, x_n]$, we define the *zero set* of S by

$$Z(S) := \{x \in \mathbb{A}^n(k) : f(x) = 0 \text{ for all } f \in I\}.$$

Note that replacing S with the ideal it generates (S) makes no difference to $Z(S)$ (i.e., linear combinations of the constraints do not make the problem harder), so we may focus on the case where S is an ideal.

With these maps in hand, we can restate the Nullstellensatz.

Theorem 1.75 (Nullstellensatz, II)**.** Fix k an algebraically closed field. Then for ideals $I \subseteq k[x_1, \ldots, x_n]$, we have

$$I(Z(I)) = \operatorname{rad} I.$$

In particular, if I is radical, then $I(Z(I)) = I$.

Remark 1.76. Yes, it is important that k is algebraically closed here. Essentially this comes from Example 1.64: the ideal $\left(x^2+1\right)$ is not of the form $Z(X)$ for any subset $X \subseteq \mathbb{A}^1(\mathbb{R})$ because x^2+1 has no roots and would need $X = \varnothing$, but $Z(\varnothing) = \mathbb{R}[x]$.

Example 1.77. We have that $I(Z(R)) = R$ because $Z(R) = \varnothing$ (no points satisfy $1 = 0$) and $I(\varnothing) = R$ (all functions vanish on $\varnothing$).

Remark 1.78 (Nir)**.** One might object that $I(Z(I)) = \operatorname{rad} I$ only contains one direction of the bijection, but in fact it is not too hard to show directly that $Z(I(X)) = X$ for algebraic sets X. We argue as follows.

- Each $x \in X$ will cause all polynomials in $I(X)$ to vanish by construction of $I(X)$, so $X \subseteq Z(I(X))$.
- Now set $X = Z(S)$. Each $f \in S$ has $f(x) = 0$ for each $x \in S$, so $f \in I(X)$ as well. So $S \subseteq I(X)$, so $Z(I(X)) \subseteq Z(S) = X$.

1.2.3 More on Affine Space

Let's talk about $\mathbb{A}^n(k)$ a bit more. We mentioned that this should be a geometric object, so let's give it a topology.

Definition 1.79 (Zariski topology, I)**.** Given affine space $\mathbb{A}^n(k)$, we define the *Zariski topology* as having closed sets which are the algebraic sets.

Remark 1.80 (Nir)**.** Here is one reason why we might do this: without immediate access to better functions (the field k might have no easy geometry, like $k = \mathbb{F}_p(t)$) it makes sense to at least require polynomial functions to be continuous and k to be Hausdorff. In particular, given a polynomial f, we see that

$$Z(f) = f^{-1}(\{0\})$$

should be closed. Further, for any subset $S \subseteq k[x_1, \ldots, x_n]$ of polynomials

$$Z(S) = \bigcap_{f \in S} Z(f)$$

will also have to be closed. In particular, all algebraic sets are closed. One can then check that polynomials do remain continuous in this topology also, as promised.

We have the following checks to make sure that the algebraic sets do actually form a topology (of closed sets).

- The empty set is closed: $\varnothing$ is the set of solutions to the equation $1 = 0$.

- The full space is closed: $\mathbb{A}^n(k)$ is the set of solutions to the equation $0 = 0$.
- Arbitrary intersection of closed sets is closed: given algebraic sets $Z(S)$ for given subsets $S \in \mathcal{S}$ of $k[x_1, \ldots, x_n]$, we note

$$\bigcap_{S \in \mathcal{S}} Z(S) = Z\left(\bigcup_{S \in \mathcal{S}} S\right),$$

  so the union is in fact an algebraic set.
- Finite unions of closed sets are closed: given algebraic sets $Z(S_1), \ldots, Z(S_n)$, we note

$$\bigcup_{i=1}^{n} Z(S_i) = Z\left(\prod_{i=1}^{n} (S_i)\right),$$

  where (S_i) is the ideal generated by S_i. In particular, $\prod_i (S_i)$ is generated by elements $s_1 \cdot \ldots \cdot s_n$ such that $s_i \in S_i$ for each i, so any point in any of the $Z(S_i)$ will show up in the given algebraic set.

Now that we've checked we actually have a topology, we remark that it is a pretty strange topology.

Proposition 1.81. Let k be an algebraically closed field. Given affine space $\mathbb{A}^n(k)$ the Zariski topology.

- The space $\mathbb{A}^n(k)$ is not Hausdorff.
- The space $\mathbb{A}^n(k)$ is compact.

Proof. We take the claims individually.

- Because $\mathbb{A}^n(k)$ has more than one point, it suffices to show that there are no disjoint nonempty Zariski open subsets of $\mathbb{A}^n(k)$. In other words, given two Zariski open sets $\mathbb{A}^n(k) \setminus Z(I)$ and $\mathbb{A}^n(k) \setminus Z(J)$, we claim that

$$(\mathbb{A}^n(k) \setminus Z(I)) \cap (\mathbb{A}^n(k) \setminus Z(J)) = \varnothing$$

  implies $\mathbb{A}^n(k) \setminus Z(I) = \varnothing$ or $\mathbb{A}^n(k) \setminus Z(J) = \varnothing$. Taking complements, we know that

$$Z(IJ) = Z(I) \cup Z(J) = \mathbb{A}^n(k) = Z((0)).$$

  But now, by the Nullstellensatz (!), we see that $\operatorname{rad}(IJ) = \operatorname{rad}((0))$. But $k[x_1, \ldots, x_n]$ is an integral domain, so $\operatorname{rad}((0)) = (0)$.

  Now, this means $f^n \in IJ$ for some $n \in \mathbb{N}$ requires $f = 0$, which means that $IJ = (0)$, so because $k[x_1, \ldots, x_n]$ is an integral domain, $I = (0)$ or $J = (0)$. (Explicitly, I and J cannot both have nonzero terms.) Without loss of generality, take $I = (0)$.

  So to finish, we see $Z(I) = Z((0)) = \mathbb{A}^n(k)$, so $\mathbb{A}^n(k) \setminus Z(I) = \varnothing$.
- Suppose we are given an open cover $\{\mathbb{A}^n(k) \setminus Z(I)\}_{I \in \mathcal{S}}$ indexed by some collection $\mathcal{S}$ of ideals of $k[x_1, \ldots, x_n]$. The fact that these sets form an open cover is equivalent to saying

$$Z\left(\sum_{I \in \mathcal{S}} I\right) = \bigcap_{I \in \mathcal{S}} Z(I) = \varnothing.$$

  Now, by the Nullstellensatz (we will use this trick again later on!), it follows

$$1 \in R = I(\varnothing) = I\left(Z\left(\sum_{I \in \mathcal{S}} I\right)\right) = \operatorname{rad} \sum_{I \in \mathcal{S}} I,$$

  so it follows $1 \in \sum_{I \in \mathcal{S}} I$.

The key trick, now is that we can reduce this to a finite condition: $1 \in \sum_{I \in \mathcal{S}} I$ merely means there are elements $\{f_i\}_{i=1}^N$ such that $f_i \in I_i$ for some $I_i \in \mathcal{S}$ such that $\sum_i f_i = 1$. This means that in fact $1 \in I_1 + \cdots + I_N$, so

$$\varnothing = Z(I_1 + \cdots + I_N) = \bigcap_{i=1}^{N} Z(I_i).$$

Thus, the finite number of sets $\mathbb{A}^n(k) \setminus Z(I_i)$ for each $1 \leq i \leq N$ provides us with a finite subcover of $\mathbb{A}^n(k)$. ■

In another direction, we note can also understand algebraic sets $X \subseteq \mathbb{A}^n(k)$ by their ring of functions. Again, the only functions we have easy access to are polynomials, so we take the following definition.

Definition 1.82 (Coordinate ring)**.** Given an algebraic set $X \subseteq \mathbb{A}^n(k)$, we define the *coordinate ring* on X as

$$A(X) := k[x_1, \ldots, x_n]/I(X).$$

In other words, we are looking at polynomials on $\mathbb{A}^n(k)$ and identifying them whenever they are equal on X.

Note that, because $I(X)$ is a radical ideal, the ring $A(X)$ will be reduced.

1.2.4 Corollaries of the Nullstellensatz

Let's return to talking about the Nullstellensatz. To convince us that the Nullstellensatz is important, here are some nice corollaries.

Criteria for Polynomial System Solutions

The following is the feature of this discussion.

Corollary 1.83. A system of polynomial equations

$$\begin{cases} f_1(x_1, \ldots, x_n) = 0, \\ \qquad \vdots \\ f_r(x_1, \ldots, x_n) = 0, \end{cases}$$

has no solutions if and only if there exists $p_1, \ldots, p_r \in k[x_1, \ldots, x_n]$ such that

$$\sum_{i=1}^{r} p_i f_i = 1.$$

Proof. In the reverse direction, we proceed by contraposition: if there is a solution $x \in \mathbb{A}^n(k)$ such that $f_i(x) = 0$ for each f_i, then any set of polynomials $p_1, \ldots, p_n \in k[x_1, \ldots, x_n]$ will give

$$\sum_{i=1}^{r} p_i(x) f_i(x) = 0 \neq 1,$$

so it follows $\sum_{o=1}^{n} p_i f_i \neq 1$. Observe that we did not use the Nullstellensatz here.

The forwards direction is harder. The main point is that we are given $Z((f_1, \ldots, f_r)) = \varnothing$, so

$$\operatorname{rad}(f_1, \ldots, f_r) = I(Z((f_1, \ldots, f_n))) = I(\varnothing) = R,$$

so the Nullstellensatz gives $1 \in \operatorname{rad}(f_1, \ldots, f_r)$. Then it follows $1 = 1^n \in (f_1, \ldots, f_r)$ for some positive integer n, so there exists $p_1, \ldots, p_r \in k[x_1, \ldots, x_n]$ such that

$$\sum_{i=1}^{r} p_i f_i = 1.$$

This is what we wanted. ■

Maximal Ideals Are Points

To set up the next corollary, we claim that any point $a = (a_1, \ldots, a_n) \in \mathbb{A}^n(k)$ makes a closed set corresponding to the ideal

$$I(\{a\}) \stackrel{?}{=} (x_1 - a_1, \ldots, x_n - a_n) \subseteq k[x_1, \ldots, x_n] = A(\mathbb{A}^n(k)).$$

Indeed, $I(\{a\})$ certainly contains $x_i - a_i$ for each i; conversely, if $f \in I(\{a\})$, then

$$f(x_1, \ldots, x_n) \equiv f(a_1, \ldots, a_n) = 0 \pmod{x_1 - a_1, \ldots, x_n - a_n},$$

so $f \in (x_1 - a_1, \ldots, x_n - a_n)$.

Example 1.84. In fact, in the case of $\mathbb{C}[x]$, it is not too hard to see that such ideals are maximal: given $z \in \mathbb{C}$, suppose that $I \subseteq \mathbb{C}[x]$ had $(x - z) \subseteq I$. If each $f \in I$ has $f(z) = 0$, then we are done; otherwise if there is $f \in I$ with $f(z) \neq 0$, then $f(x)$ and $(x - z)$ are coprime in a principal ideal domain, so

$$1 \in (f) + (x - z) \subseteq I,$$

meaning $I = \mathbb{C}[x]$.

The above example gives us the hope that maximal ideals might turn out to all be of the above form. Indeed, this is true, with the help of the Nullstellensatz.

Corollary 1.85. Fix $X \subseteq \mathbb{A}^n(k)$ an (affine) algebraic set. Then points $a = (a_1, \ldots, a_n) \in X$ are in bijection with maximal ideals $\mathfrak{m}_a \subseteq A(X)$ by

$$a \mapsto \mathfrak{m}_a := I(\{a\})/I(X) = (x_1 - a_1, \ldots, x_n - a_n)/I(X).$$

Proof. The input from the Nullstellensatz will come from the following lemma.

Lemma 1.86. Suppose that $I \subseteq A\left(\mathbb{A}^n(k)\right)$ has $Z(I) = \varnothing$. Then $I = A\left(\mathbb{A}^n(k)\right)$.

Proof. By the Nullstellensatz,

$$1 \in A\left(\mathbb{A}^n(k)\right) = I(\varnothing) = I(Z(I)) = \operatorname{rad} I,$$

so $1 \in I$ follows. ■

Now, we have already shown that $I(\{a\}) = (x_1 - a_1, \ldots, x_n - a_n)$. Additionally, for $x \in X$, we have $I(X) \subseteq I(\{a\})$, so $I(\{a\})/I(X)$ is an ideal which makes sense. Thus, we may write $I(\{a\})/I(X) = (x_1 - a_1, \ldots, x_n - a_n)/I(X)$.

Before continuing, we also check that $Z(I(\{a\})) = \{a\}$ as well. (This shows that $\{a\}$ is an algebraic set.) Well, set $a = (a_1, \ldots, a_n)$, and we note that $x_i - a_i \in I(\{a\})$ for each i, so any $b = (b_1, \ldots, b_n) \in Z(I(\{a\}))$ must vanish on each $x_i - a_i$, so

$$b_i - a_i = 0$$

for each i. Thus, $b = a$.

We now check that $a \mapsto \mathfrak{m}_a$ is a bijection.

- Well-defined: we show that $\mathfrak{m}_a$ is a maximal ideal. It is proper because $1 \notin \mathfrak{m}_a$. Now suppose we have $I \subseteq A(X)$ such that $\mathfrak{m}_a \subseteq I$. So note that $I + I(X) \subseteq A(\mathbb{A}^n(k))$ is an ideal (namely, the pre-image) containing $I(\{a\})$.

  Now, observe that $I(\{a\}) \subseteq I + I(X)$, so

  $$Z(I + I(X)) \subseteq Z(I(\{a\})) = \{a\}.$$

  We now have two cases.

  - If $Z(I + I(X)) = \varnothing$, then Lemma 1.86 gives $I + I(X) = A(\mathbb{A}^n(k))$, so $I/I(X) = A(X)$.
  - Otherwise, if $Z(I + I(X)) = \{a\}$, then $I + I(X) \subseteq I(\{a\})$. Thus, $I \subseteq \mathfrak{m}_a$, finishing.

- Injective: suppose $a, b \in X$ have $\mathfrak{m}_a = \mathfrak{m}_b$. But then

  $$I(\{a\}) = \mathfrak{m}_a + I(X) = \mathfrak{m}_b + I(X) = I(\{b\}),$$

  so $\{a\} = Z(I(\{a\})) = Z(I(\{b\})) = \{b\}$, so $a = b$ follows.

- Surjective: suppose that $\mathfrak{m} \subseteq A(X)$ is a maximal ideal. Then we look at the pre-image ideal $I := \mathfrak{m} + I(X) \subseteq A(\mathbb{A}^n(k))$. We claim that $Z(I)$ is a singleton.

  - We show that $Z(I) \neq \varnothing$. Indeed, $Z(I) = \varnothing$ implies by Lemma 1.86 that $1 \in I$, so $[1]_{I(X)} \in \mathfrak{m}$, which violates the fact that $\mathfrak{m} \subseteq A(X)$ is proper.
  - We show all elements of $Z(I)$ are equal. Suppose $a, b \in Z(I)$; because $I(X) \subseteq I$, we see $a, b \in X$ is forced by Remark 1.78. Then $\{a\}, \{b\} \subseteq Z(I)$, so

    $$I \subseteq I(\{a\}) \cap I(\{b\}),$$

    so $\mathfrak{m} = I/I(X)$ is contained in $\mathfrak{m}_a = I(\{a\})/I(X)$ and $\mathfrak{m}_b = I(\{b\})/I(X)$. But, if $a \neq b$, then $\mathfrak{m}_a$ and $\mathfrak{m}_b$ are distinct maximal ideals, so we see $\mathfrak{m} \subseteq \mathfrak{m}_a \cap \mathfrak{m}_b \subsetneq \mathfrak{m}_a \subsetneq A(X)$, violating the fact that $\mathfrak{m}$ is maximal. So we must have $a = b$ instead.

  Thus, set $Z(I) = \{a\}$; note $a \in X$ because $I(X) \subseteq I$ (by Remark 1.78 again). Now, $I \subseteq I(\{a\})$, so we see $\mathfrak{m} = I/I(X) \subseteq I(\{a\})/I(X) = \mathfrak{m}_a$, so the maximality of $\mathfrak{m}$ forces $\mathfrak{m} = \mathfrak{m}_a$. ■

The reason the above is nice is because, instead of having to look at the geometry of X, it is now legal to study the algebra of $A(X)$.

1.2.5 The Spectrum of a Ring

We continue trying to move the geometry of affine sets $X \subseteq \mathbb{A}^n(k)$ into the coordinate ring $A(X)$.

Later in life we will want to consider maps $\varphi : X \to Y$ between affine sets. In affine space, we again remark that really the only functions we have access to are polynomials, so our only morphisms will be functions which are polynomials in each coordinate.

Now let's move φ to geometry. Note that $A(X)$ and $A(Y)$ are intended to describe functions $X \to k$ and $Y \to k$ respectively, so a morphism $\varphi : X \to Y$ induces a ring homomorphism

$$\varphi : A(Y) \to A(X)$$

by $f \mapsto f \circ \varphi$. (This is a ring homomorphism because φ is made of polynomials.) So under the paradigm that points should become maximal ideals, we would like to recover φ as some kind of map of maximal ideals $A(X) \to A(Y)$. The natural way is to simply pull back along φ, writing

$$\mathfrak{m} \subseteq A(X) \mapsto \varphi^{-1}(\mathfrak{m}) \subseteq A(Y).$$

However, this is a problem: $\varphi^{-1}(\mathfrak{m})$ need not be maximal!

Example 1.87. If $\mathfrak{p} \subseteq R$ is a prime but not maximal ideal (e.g., $(x) \subseteq k[x, y]$), we can define the composite

$$R \twoheadrightarrow R/\mathfrak{p} \hookrightarrow \operatorname{Frac}(R/\mathfrak{p}).$$

Now, (0) is maximal in $\operatorname{Frac}(R/\mathfrak{p})$, but its pre-image in R is $\mathfrak{p}$, which is not maximal by construction.

However, if we weaken requiring our points to be prime ideals $\mathfrak{p}$ instead of maximal ideals, we do have that $\varphi^{-1}(\mathfrak{p})$ is a prime ideal: $ab \in \varphi^{-1}(\mathfrak{p})$ implies $\varphi(a)\varphi(b) = \varphi(ab) \in \mathfrak{p}$ implies $a \in \varphi^{-1}(\mathfrak{p})$ or $b \in \varphi^{-1}(\mathfrak{p})$.

So instead of making our geometry on $A(X)$ defined by maximal ideals, we use prime ideals. This gives the following definition.

Definition 1.88 (Spectrum of a ring)**.** Given a ring R, we define *spectrum of R* by

$$\operatorname{Spec} R := \{\mathfrak{p} \subseteq R : \mathfrak{p} \text{ is a prime ideal}\}.$$

In fact, $\operatorname{Spec} R$ also has a Zariski topology as follows.

Definition 1.89 (Zariski topology, II)**.** Given a ring R, we define the *Zariski topology* to have closed sets

$$X(I) := \{\mathfrak{p} \in \operatorname{Spec} R : I \subseteq \mathfrak{p}\}$$

for R-ideals I.

Remark 1.90 (Nir)**.** As for motivation for why we might define our topology like this, recall the case of affine varieties: we have $a \in X(I)$ if and only if $I \subseteq I(\{a\})$. So when we translate $X(I)$ into the algebraic side, we call the maximal ideal $\mathfrak{m}_a = I(\{a\})$ our "point" and see that

$$X(I) = \{\mathfrak{m}_a : I \subseteq \mathfrak{m}_a\}.$$

It is a different story why we use prime ideals instead of maximal ones, which we discussed above.

The checks that the $X(I)$ do actually define closed sets for a topology are essentially the same as for the first version of the Zariski topology. The main points are that

$$\bigcap_{I \in \mathcal{S}} X(I) = X\left(\sum_{I \in \mathcal{S}} I\right) \qquad \text{and} \qquad \bigcup_{k=1}^{N} X(I_k) = X\left(\prod_{k=1}^{N} I_k\right)$$

give that arbitrary intersection of closed sets is closed and finite union of closed sets is closed.[3]

Again, the Zariski topology is very weird, like with affine space.

Proposition 1.91. Fix R a ring. Given $\operatorname{Spec} R$ the Zariski topology.

- If R is an integral domain which is not a field, then $\operatorname{Spec} R$ is not Hausdorff.
- The space $\operatorname{Spec} R$ is compact.

Proof. We take the claims one at a time.

- The fact that R is a not field means that $\operatorname{Spec} R$ has more than one point. So again, it suffices to show that there are no disjoint open subsets of $\operatorname{Spec} R$. Indeed, suppose

$$(\operatorname{Spec} R \setminus X(I)) \cap (\operatorname{Spec} R \setminus X(J)) = \varnothing,$$

[3] The second equality requires some care. The main point is to show, for $\mathfrak{p}$ prime, $IJ \subseteq \mathfrak{p}$ is equivalent to $I \subseteq \mathfrak{p}$ or $J \subseteq \mathfrak{p}$. The reverse is easy. For the forwards, suppose $IJ \subseteq \mathfrak{p}$ and $J \not\subseteq \mathfrak{p}$ so that we have $j \in J \setminus \mathfrak{p}$. Then $jI \subseteq IJ \subseteq \mathfrak{p}$ forces $I \subseteq \mathfrak{p}$.

and we claim $\operatorname{Spec} R \setminus X(I) = \varnothing$ or $\operatorname{Spec} R \setminus X(J) = \varnothing$.

Again, we know that $X(IJ) = X(I) \cup X(J) = \operatorname{Spec} R$, so by definition, we see $IJ \subseteq \mathfrak{p}$ for each prime $\mathfrak{p}$, or

$$IJ \subseteq \bigcap_{\mathfrak{p}} \mathfrak{p}.$$

Now, because R is an integral domain, we see that (0) is a prime ideal, so $IJ = (0)$ follows. Thus, because R is an integral domain again, $I = (0)$ or $J = (0)$, so without loss of generality, we take $I = (0)$. But then

$$\operatorname{Spec} R \setminus X(I) = \operatorname{Spec} R \setminus \operatorname{Spec} R = \varnothing,$$

as desired.

- Suppose that the Zariski open sets $\{\operatorname{Spec} R \setminus X(I)\}_{I \in \mathcal{S}}$ cover $\operatorname{Spec} R$, for some collection $\mathcal{S}$ of ideals. Now, the sets $\{\operatorname{Spec} R \setminus X(I)\}_{I \in \mathcal{S}}$ covering $\mathbb{A}^n(k)$ is equivalent to

$$X\left(\sum_{I \in \mathcal{S}} I\right) = \bigcap_{I \in \mathcal{S}} X(I) = \varnothing.$$

However, $X\left(\sum I\right) = \varnothing$ implies that there is no prime ideal $\mathfrak{p}$ such that $\sum I \subseteq \mathfrak{p}$, but any proper ideal is contained in some maximal and hence prime ideal. Thus, we must have that

$$\sum_{I \in \mathcal{S}} I = R.$$

In particular, 1 is in this ideal, so we can express 1 as the sum of some elements $x_i \in I_i$ for $\{I_i\}_{i=1}^N \subseteq \mathcal{S}$; i.e.,

$$1 = \sum_{i=1}^N x_i \in \sum_{i=1}^N I_i.$$

Thus, $\sum_{i=1}^N I_i = R$, meaning $X\left(\sum_{i=1}^N I_i\right) = \varnothing$, so reversing the argument we see that $\{\operatorname{Spec} R \setminus X(I_i)\}_{i=1}^N$ will be a finite subcover. This finishes. ■

1.2.6 Projective Space

To define projective varieties, we need to define projective space first.

Definition 1.92 (Projective space)**.** Fix k a field and n a positive integer. Then we define n-dimensional *projective space* $\mathbb{P}^n(k)$ to be the one-dimensional subspaces of k^{n+1}.

Concretely, we will think about lines in homogeneous coordinates, in the form

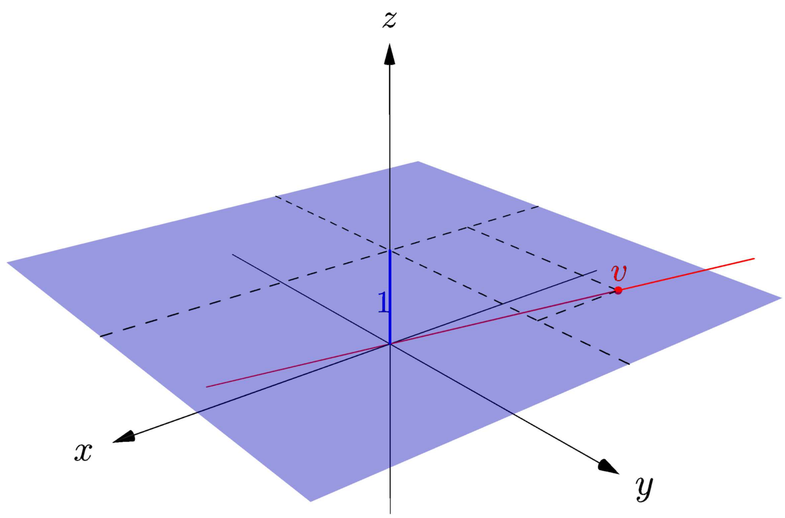
$$(a_0 : a_1 : \ldots : a_n) \in \mathbb{P}^n(k)$$

to represent the subspace $k(a_0, a_1, \ldots, a_n) \subseteq \mathbb{A}^{n+1}(k)$. As such multiplying the point $(a_0 : a_1 : \ldots : a_n)$ by some constant $c \in k^\times$ will give the same line and should be the same point in $\mathbb{P}^n(k)$. Additionally, we will ban the point $(0 : 0 : \ldots : 0)$ from projective space because it is not the basis for any line.

We would like to have a better geometry understanding of $\mathbb{P}^n(k)$. Note that we have a sort of embedding $\mathbb{A}^n(k) \hookrightarrow \mathbb{P}^n(k)$ by

$$(x_1, x_2, \ldots, x_n) \mapsto (x_1 : x_2 : \ldots : x_n : 1).$$

For geometric concreteness, we can imagine $\mathbb{A}^2(\mathbb{R}) \hookrightarrow \mathbb{P}^2(\mathbb{R})$ as the plane $z = 1$ in $\mathbb{R}^3$, where each point on the plane gives rise to a unique line in $\mathbb{R}^3$. Here is the image, with a chosen red line going through a point v on the $z = 1$ plane.



However, not all lines in $\mathbb{A}^3(\mathbb{R})$ can be described like this, for there are still lots of points of the form $(x : y : 0)$, which are "points at infinity." Nevertheless, we can collect the remaining points into $\mathbb{P}^2(\mathbb{R})$, which visually just means the lines that live on the xy-plane in the above diagram.

In general, we see that we can decompose $\mathbb{P}^n(k)$ into an $\mathbb{A}^n(k)$ component as a "$z = 1$ hyperplane" and then the points at infinity living on $\mathbb{P}^{n-1}(k)$. Namely,

$$\mathbb{P}^n(k) \approx \mathbb{A}^n(k) \sqcup \mathbb{P}^{n-1}(k).$$

Note that the above decomposition is not canonical: one has to choose which points to get to be infinity.

Anyways, as usual we interested in studying the algebraic sets but this time of projective space, but because of constant factors may wiggle, we see that we really should only be looking at homogeneous equations. More concretely, if $f \in k[x_0, \ldots, x_n]$, we want

$$f(a_0 : \ldots : a_n) = 0$$

to be unambiguous, so $f(a_0, \ldots, a_n) = 0$ should imply $f(ca_0, \ldots, ca_n) = 0$ for any $c \in k^\times$. The easiest way to ensure this is to force all monomials of f to have some fixed degree, say d, so that

$$f(cx_0, \ldots, cx_n) = c^d f(x_0, \ldots, x_n).$$

These polynomials are the homogeneous ones, and they give the following definition.

Definition 1.93 (Projective variety)**.** A subset $X \subseteq \mathbb{P}^n(k)$ is a *projective variety* if and only if it is the solution set to some set of homogeneous (!) polynomials equations of $k[x_0, \ldots, x_n]$.

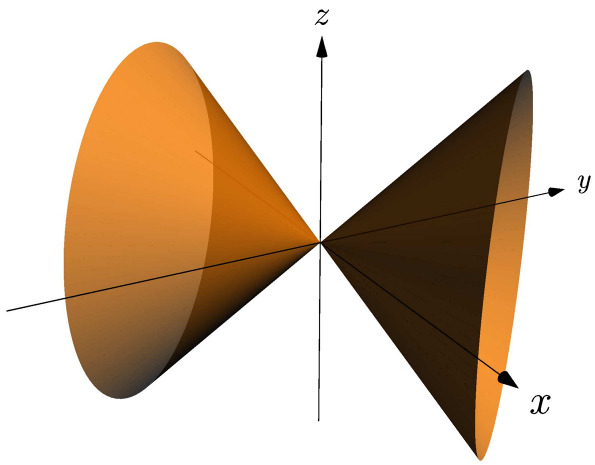
Here is an example.

Exercise 1.94. We view the solutions to $xy - 1 = 0$ in $\mathbb{A}^2(\mathbb{R}) \subseteq \mathbb{P}^2(\mathbb{R})$ in projective space.

Proof. More explicitly, we are viewing $\mathbb{A}^2(k) \subseteq \mathbb{P}^2(k)$ by sending $(x, y) \mapsto (x : y : 1)$. We can make the coordinates more familiar by setting $x, y \mapsto x/z, y/z$ so that we are looking for solutions $(x/z : y/z : 1) = (x : y : z)$ to the equation

$$xy = z^2.$$

In $\mathbb{R}^3$, this curve looks like the following.



The hyperbola for $xy = 1$ comes from slicing the $z = 1$ plane from this cone. ■

1.2.7 Graded Rings

We have the following definition.

Definition 1.95 (Graded ring)**.** A ring R is *graded* by the abelian groups $R_0, R_1, \ldots$ if and only if

$$R \cong \bigoplus_{d=0}^{\infty} R_d$$

as abelian groups and $R_i R_j \subseteq R_{i+j}$ for any $i, j \in \mathbb{N}$.

Remark 1.96 (Nir)**.** In fact, R_0 turns out to be a subring of R_0. We can check this directly, as follows.

- Certainly $0 \in R_0$ and $R_0 + R_0 \subseteq R_0$ because $R_0 \subseteq R$ is an additive subgroup.
- If $1_R \in R_i$, then $R_i \subseteq R_i R_i \subseteq R_{2i}$, so $i = 0$ or $R_i = R_{2i} = \{0\}$ by because distinct homogeneous components have trivial intersection. So either $1 \in R_0$ or $1 \in R_0 = \{0\}$ forces $R = \{0\}$, so $1 \in R_0$ anyways.
- We see $R_0 R_0 \subseteq R_0$, so R_0 is closed under multiplication.

Alternatively, we could set $I := \{0\} \oplus R_1 \oplus R_2 \cdots$, remark that I is an ideal, and then we see $R_0 \cong R/I$.

Example 1.97. The ring $R = k[x_1, \ldots, x_n]$ is "graded by degree" by setting R_d to be the space of all homogeneous n-variable polynomials of degree d (in addition to 0).

Remark 1.98 (Nir)**.** In fact, any ring R can be given a trivial grading: set $R_0 = R$ and $R_d = 0$ for $d > 0$. Then of course we have

$$R \cong R \oplus 0 \oplus 0 \oplus \cdots = R_0 \oplus R_1 \oplus R_2 \oplus \cdots .$$

On the other hand, for indices i and j, we see that $i = j = 0$ has $R_i R_j = R_0 R_0 = RR = R = R_0$; otherwise, one of $i > 0$ or $j > 0$, so $R_i R_j = \{0\} \subseteq R_{i+j}$.

With graded rings, it is natural to ask what other ring-theoretic constructions we can grade.

Definition 1.99 (Graded ideal)**.** Fix R a graded ring. We say that an ideal I is *graded* if and only if

$$I \cong \bigoplus_{d=0}^{\infty}(R_d \cap I),$$

where the isomorphism is the natural one (i.e., $(x_0, x_1, \ldots) \mapsto x_0 + x_1 + \cdots$).

Example 1.100. Given the graded ring $R = R_0 \oplus R_1 \oplus R_2 \oplus \cdots$, the ideal

$$I := \{0\} \oplus R_1 \oplus R_2 \oplus R_3 \oplus \cdots$$

is called the *irrelevant ideal*; it is graded because look at it. To check I is an ideal, it is closed under addition by construction; it is closed under multiplication by R because $R_iR_j \subseteq R_{i+j}$ for $i \geq 1$ implies $i + j \geq 1$.

Remark 1.101. The above ideal is called irrelevant because, in the case where $R = k[x_0, \ldots, x_n]$,

$$Z(I) = \{(a_0 : \ldots : a_n) \in \mathbb{P}^n(k) : f(a_0, \ldots, a_n) \text{ for each homogeneous } f \in I\} = \varnothing.$$

Indeed, any element of $Z(I)$ would have to satisfy $x_i = 0$ for each x_i, which is illegal in projective space.

The point of the definition of a graded ideal is that, when $I \subseteq R$ is a graded ideal,

$$\frac{R}{I} \cong \bigoplus_{d=0}^{\infty} \frac{R_d}{R_d \cap I}$$

will also be a graded ring, with the given grading. This isomorphism comes from combining the isomorphisms $R \cong \bigoplus_d R_d$ and $I \cong \bigoplus_d (R_d \cap I)$.

Here is another ring-theoretic construction which we can grade.

Definition 1.102 (Graded module)**.** Fix $R = R_0 \oplus R_1 \oplus \cdots$ a graded ring. Then an R-module M is *graded* if and only if we can write

$$M \cong \bigoplus_{d \in \mathbb{Z}} M_d$$

such that $R_iM_j \subseteq M_{i+j}$ for any $i \in \mathbb{N}$ and $j \in \mathbb{Z}$.

Remark 1.103 (Nir)**.** With our basic objects moved to a graded setting, we note that we can also talk about graded morphisms between graded rings and modules, which basically means that the grading is preserved. Explicitly, if $R = \bigoplus_{d \in \mathbb{N}} R_d$ and $R' = \bigoplus_{d \in \mathbb{N}} R'_d$ are graded rings, then a graded homomorphism $\varphi : R \to R'$ is a ring homomorphism such that

$$\varphi(R_d) \subseteq R'_d.$$

Replacing all Rs with Ms and the word "ring" with "module" in the above definition recovers the definition of a graded module homomorphism.

As a quick application, here is one reason to care about graded rings: they play nice with the Noetherian condition.

Proposition 1.104. A graded ring $R = R_0 \oplus R_1 \oplus \cdots$ is Noetherian if and only if R_0 is Noetherian and R is a finitely generated R_0-algebra.

Proof. The backwards direction is Proposition 1.53. For the forwards direction, take $R = R_0 \oplus R_1 \oplus \cdots$ a Noetherian, graded ring. We note that modding R out by the irrelevant ideal reveals that R_0 is a quotient of R, so R_0 is a Noetherian ring.

It remains to show that R is a finitely generated R_0-algebra. The idea is to imitate the Hilbert's finiteness theorem. Before doing anything, we adopt the convention that, for an arbitrary element

$$f = f_0 + f_1 + \cdots \in R,$$

we let $\deg f$ equal the largest d for which $f_d \neq 0$.

We now proceed with the proof. Because R is Noetherian, the irrelevant ideal

$$I \coloneqq R_1 \oplus R_2 \oplus \cdots$$

is finitely generated over R, so fix $I \coloneqq (r_1, \ldots, r_N)$. We claim that

$$R \stackrel{?}{=} R_0[r_1, \ldots, r_N].$$

For $\supseteq$, there is nothing to say. For $\subseteq$, pick up some $f \in R$, and we show that $f \in R_0[r_1, \ldots, r_N]$. By decomposing f into its grading $f = f_0 + f_1 + \cdots$, we may assume that f lives in one of the R_d.

So now we induct on d. For $d = 0$, we have $f \in R_0 \subseteq R_0[r_1, \ldots, r_N]$ and are done immediately. So take $d > 0$. Then $f \in I = (r_1, \ldots, r_N)$, so we may write

$$f = \sum_{i=1}^{N} g_i r_i$$

for some $g_1, \ldots, g_N \in R$. By decomposing the $g_\bullet$ into their gradings, we may assume that only the $\deg f - \deg r_i$ component is nonzero because all other components will cancel anyways.

In particular, g_i is homogeneous with degree $\deg f - \deg r_i$, so $g_i \in R_i$ with $i < d$. So by our induction, $g_i \in R_0[r_1, \ldots, r_N]$, and $f \in R_0[r_1, \ldots, r_N]$ by the decomposition of f in I. This finishes the proof. ■

1.2.8 The Hilbert Function

For this subsection, let $R \coloneqq k[x_0, \ldots, x_n]$ (note the zero-indexing!) be a ring graded by degree, and let $M = \cdots \oplus M_{-1} \oplus M_0 \oplus M_1 \oplus \cdots$ be a finitely generated graded R-module. It follows that

$$\dim_k M_d < \infty$$

for each $d \in \mathbb{Z}$. Indeed, R is Noetherian, so M is Noetherian (M is finitely generated over R), so we note that the R-submodule

$$M_d' \coloneqq \bigoplus_{e \geq d} M_e \subseteq M$$

is a finitely generated as an R-module. (This is an R-submodule because it is closed under addition, and $R_i M_j \subseteq M_{i+j}$ for $i \in \mathbb{N}$ and $j \in \mathbb{Z}$ gives closure under R-multiplication.) But the only way $rm \in M_d$ for $r \in R$ and $m \in M_d'$ is for $r \in R_0 = k$ and $m \in M_d$, so the (finite number of) generators of M_d' in M_d will generate M_d as a k-module.

This gives us the following definition.

Definition 1.105 (Hilbert function)**.** Let M be a finitely generated module over $R \coloneqq k[x_0, \ldots, x_n]$, where R is graded by degree. Then we define the *Hilbert function* of M as

$$H_M(d) \coloneqq \dim_k M_d.$$

Exercise 1.106. Let $M = R = k[x_0, \ldots, x_n]$; i.e., view R as an R-module. Then we compute $H_M(d)$.

Proof. Here, M and R have the same grading (because $M = R$), so we are computing

$$H_M(d) = \dim_k R_d.$$

To see this, we note that we can expand any polynomial $f \in R_d$ as a unique k-linear combination of the degree-d monomials: after all, we can express generic polynomials in a unique k-linear combination of monomials, and R_d requires everything involved to have degree d.

Thus, $\dim_k R_d$ has basis consisting of the degree-d monomials in $k[x_0, \ldots, x_n]$. Thus, we are counting tuples $(a_0, \ldots, a_n)$ of nonnegative integers (uniquely) associated to the monomial

$$x_0^{a_0} \cdots x_n^{a_n}$$

such that $a_0 + \cdots + a_n = d$. But this is now merely a combinatorics problem! We claim that this is $\binom{n+d}{d}$.

Indeed, for any such tuple $(a_0, \ldots, a_n)$, imagine placing (in a single row) a_0 stones, then a stick, then a_1 stones, then a stick, and so on, ending by placing the last a_n stones. In total, we are placing d stones and n sticks, and the arrangement of sticks and stones uniquely describes the tuples. So now we see there are

$$\binom{n+d}{d}$$

ways to put down d sticks among $n + d$ "slots" of either sticks or stones. So indeed, we find that

$$\boxed{H_M(d) = \binom{n+d}{d}},$$

as desired. ■

The above example found that $H_m(d)$ is a polynomial in d of degree r. This happens in general.

Theorem 1.107. Let M be a finitely generated graded module over the ring $R := k[x_0, \ldots, x_n]$, where R is graded by degree. Then there exists a polynomial $P_M(d)$ of degree at most $n - 1$ which agrees with $H_M(d)$ for sufficiently large d.

Proof. The proof is by induction on n, where we will apply dimension-shifting of the grading for the inductive step. Our base case is $n = -1$, which makes M into a graded $R = R_0 = k$-vector space. But M is thus finite-dimensional, the summation

$$M = \bigoplus_{d \in \mathbb{Z}} M_d$$

of $R_0 = k$-vector spaces M_d must have only finitely many nonzero terms, so $H_M(d) = 0$ for sufficiently large d. So indeed, H_M agrees with the polynomial $P_M \equiv 0$ of degree $-\infty \le -1$ for sufficiently large inputs.

Now, we will need to dimension-shift our grading in the proof that follows, so we have the following definition.

Definition 1.108 (Twist)**.** Given a graded R-module M, we define the dth *twist* $M(d)$ of M to be the same underlying module but with grading given by

$$M(d)_e := M_{d+e}.$$

To sanity check, we remark that $M = \bigoplus_{e \in \mathbb{Z}} M(d)_e = \bigoplus_{e \in \mathbb{Z}} M_{d+e}$ and $R_i M(d)_e = R_i M_{d+e} \subseteq M_{i+d+e} = M(d)_{i+e}$ verifies that we have in fact graded M.

Note the Hilbert function is well-behaved by shifting: $H_{M(d)}(e) = \dim_k M(d)_e = \dim_k M_{d+e} = H_M(e + d)$.

For the inductive step, the main point is to kill the x_n coordinate in creative ways. Namely, M being finitely generated over $k[x_0, \ldots, x_n]$ implies that $M/x_n M$ will be finitely generated over $k[x_0, \ldots, x_{n-1}]$ because any summation involving the x_n letter got killed. So we start with exact sequence

$$M \to M/x_n M \to 0.$$

We do take a moment to remark M/x_rM is in fact a graded module by

$$\frac{M}{x_nM}\cong\frac{\bigoplus_{d\in\mathbb{Z}}M_d}{\bigoplus_{d\in\mathbb{Z}}x_nM_d}=\frac{\bigoplus_{d\in\mathbb{Z}}M_d}{\bigoplus_{d\in\mathbb{Z}}x_nM_{d-1}}\cong\bigoplus_{d\in\mathbb{Z}}\frac{M_d}{x_nM_{d-1}},$$

so $M\twoheadrightarrow M/x_nM$ is a map of graded modules. In particular, by disjointness, the pre-image of M_d under multiplication by x_n lives in M_{d-1}; note $x_nM_{d-1}\subseteq M_d$.

Now, to take our sequence backwards, we would like to prepend by $M\stackrel{x_n}{\to}$, but this is not legal because multiplication by x_n map will change the grading: we have $x_nM_{d-1}\subseteq M_d$. So instead we have to write down

$$M(-1)\stackrel{x_n}{\to}M\to M/x_nM\to 0.$$

This is in fact exact as graded modules because $M(-1)_d=M_{d-1}$ goes to x_nM_{d-1} goes to 0 in M_d/x_nM_{d-1}.

To finish our short exact sequence, we let $K(-1)$ be the (twisted) kernel of $M(-1)\stackrel{x_n}{\to}M$ multiplication by x_n, and we get to write

$$0\to K(-1)\to M(-1)\stackrel{x_n}{\to}M\to M/x_rM\to 0. \tag{$*$}$$

We take a moment to recognize $K(-1)\subseteq M(-1)$ is finitely generated over $k[x_0,\ldots,x_n]$ because it is a submodule of the Noetherian module $M(-1)$. But any generator of $K(-1)$ multiplied by x_n will simply vanish, so the same generators will finitely generate $K(-1)$ over $k[x_0,\ldots,x_{n-1}]$.

Now, taking the Hilbert function everywhere in ($*$), counting dimensions gives

$$H_{K(-1)}(d)-H_{M(-1)}(d)+H_M(d)-H_{M/x_rM}(d)=0.$$

We can rewrite this as

$$H_M(d)-H_M(d-1)=H_{M/x_nM}(d)-H_K(d-1),$$

so we see that the first finite difference of H_M agrees with $H_{M/x_nM}(d)-H_K(d-1)$, and the latter agrees with a polynomial of degree at most $n-1$ for sufficiently large d by inductive hypothesis. So theory of finite differences tells us that $H_M(d)$ will agree with a polynomial of degree at most n, finishing the induction. ■

Remark 1.109 (Nir)**.** At this point we can remark that we grade our modules M by $\mathbb{Z}$ instead of $\mathbb{N}$ so that we could write down $M(-1)$ in the above proof, which does not make sense when grading by $\mathbb{N}$.

Theorem 1.107 justifies the following definition.

Definition 1.110 (Hilbert polynomial)**.** Let M be a finitely generated graded module over the ring $R:=k[x_0,\ldots,x_n]$, where R is graded by degree. The polynomial promised by Theorem 1.107 is called the *Hilbert polynomial* of M.

Remark 1.111. Geometrically, most of the time M will end up being the coordinate ring of a projective variety, in which case the degree of the above Hilbert polynomial is the "degree" of the projective variety. So heuristically, most of the time the degree of the Hilbert polynomial will not achieve its maximum.

Let's do some examples.

Exercise 1.112. Take $M:=k[x,y,z]/\left(x^2+y^2+z^2\right)$ as an $R:=k[x,y,z]$-submodule. We compute the Hilbert function for M.

Proof. For brevity, set $I:=\left(x^2+y^2+z^2\right)$. Note that I is a graded ideal: if $fink[x,y,z]$ is divisible by $x^2+y^2+z^2$, then we can write $f(x,y,z)=\left(x^2+y^2+z^2\right)q(x,y,z)$. Expanding $q=q_0+q_1+\cdots$ into its homogeneous parts, we see that

$$f(x,y,z)=\sum_{d=2}^{\infty}\left(x^2+y^2+z^2\right)q_{d-2}$$

provides a decomposition of f into homogeneous parts, and by uniqueness this must be the decomposition of f. But each of these parts is manifestly divisible by $(x^2+y^2+z^2)$, so we have decomposed f into $(I \cap R_0) \oplus (I \cap R_1) \oplus \cdots$.

We have the following.

- We see $M_0 = R_0/(I \cap R_0)$ is simply k, so $\dim M_0 = 1$.
- Similarly, we see $M_1 = R_1/(I \cap R_1)$ has basis $\{x, y, z\}$ because I hasn't killed anything yet, so it has dimension $\dim M_1 = 3$.
- Lastly, we see R_2 has basis $\{xy, yz, zx, x^2, y^2, z^2\}$, but $z^2 \equiv -x^2 - y^2 \pmod I$ means that in $M_2 = R_2(I \cap R_2)$, we can kill z^2. However, we can do this anywhere else (more rigorous justification below), so $\dim M_2 = 5$.

For the general case, fix a degree $d \geq 2$. We note that there is a short exact sequence

$$0 \to R_{d-2} \overset{x^2+y^2+z^2}{\to} R_d \to \frac{R_d}{(x^2+y^2+z^2)\,R_{d-2}} \to 0.$$

Note the first map is well-defined because $(x^2+y^2+z^2)\,R_{d-2} \subseteq R_2 R_{d-2} \subseteq R_d$. In fact, we claim that $(x^2+y^2+z^2)\,R_{d-2} = I \cap R_d$, for any $f \in I \cap R_d$ has $f(x,y,z)/(x^2+y^2+z^2)$ homogeneous of degree $d-2$. So this short exact sequence is actually

$$0 \to R_{d-2} \to R_d \to M_d \to 0.$$

Thus, the short exact sequence gives $\dim M_d = \dim R_d - \dim R_{d-2}$, which by Exercise 1.106 is $\binom{n+2}{2} - \binom{n}{2} = \frac{n^2+3n+2}{2} - \frac{n^2-n}{2} = 2n+1$. ■

Remark 1.113. Continuing with the previous remark, we see the degree of the Hilbert polynomial of M above is 1, so the associated projective variety $Z(x^2+y^2+z^2)$ ought to have dimension 1. Well, $x^2+y^2+z^2 = 0$ defines a cone in affine 3-space (more or less), which is dimension one of projective 2-space upon recalling that lines becomes points.

Exercise 1.114 (Eisenbud 1.19)**.** Define $M := k[x,y,z]/(xz-y^2, yx-z^2, xw-yz)$ as an $R := k[x,y,z]$-module. We compute the Hilbert function for M.

Proof. We outline. For brevity, we set $I := (xz-y^2, yx-z^2, xw-yz)$. The key observation is that it happens that I is a free $k[x,w]$-module, with basis $\{1, y, z\}$.

Thus, viewing M as a $T := k[x,w]$-module, checking the basis, gives that $M = T \oplus T(-1) \oplus T(-1)$ corresponding to our basis elements $\{1, y, z\}$. (Multiplication by y or z will shift the grading, hence $T(-1)$.) It follows that the Hilbert function is $H_M(n) = 3n+1$. ■

We will start with localization next class.

THEME 2
LOCAL STUDY

That something so small could be so beautiful.

—Anthony Doerr

2.1 January 25

Today we localize.

2.1.1 Geometric Motivation

Let's do an example from geometry.

Fix $X \subseteq \mathbb{A}^n(k)$ an algebraic set and $U \subseteq X$ an open subset. We want to define functions on U.

Example 2.1. Concretely, we might take $X = \mathbb{A}^1(k)$ and $U = X \setminus \{0\}$. In this case, we have $A(X) = k[x]$, but we see that upon removing 0 allows $\frac{1}{x}$ to be a function, giving

$$A(U) = k[x, 1/x].$$

These turn out to be all the functions "we care about."

An alternative way to do this construction is to simply add a new function y to $A(X)$ and then mod out in the freest possible way by the requirement $xy = 1$, giving

$$A(U) = \frac{k[x, y]}{(xy - 1)}.$$

Magically, these are the functions out of the hyperbola $xy = 1$ in the plane $\mathbb{A}^2(k)$, so amazingly localization has turned into functions from the open set $\mathbb{A}^1(k) \setminus \{0\}$ to functions from the closed subset $\{(x, y) \in \mathbb{A}^2(k) : xy = 1\}$. This magic, however, is special: it does not happen if we take $X = \mathbb{A}^2(k)$ and $U = X \setminus \{(0, 0)\}$.

Anyways, our point is that localization is one way we can talk about functions of spaces, especially of open sets. More generally, if we want to describe the space of functions out of the open set $\mathbb{A}^n(k) \setminus Z(I) \subseteq \mathbb{A}^n(k)$ for some $I \subseteq k[x_1, \ldots, x_n]$, then again "the only functions we care about" are

$$A\left(\mathbb{A}^n(k) \setminus Z(I)\right) = A\left(\mathbb{A}^n(k)\right)[1/f \text{ for each } f \in I].$$

In particular, we are allowed to append inverses of I because the points on which I vanishes are no longer in the space of interest. This process of appending inverses is "localization."

2.1.2 Localization of Rings

Let's build towards the definition of localization.

Definition 2.2 (Multiplicatively closed)**.** Fix R a ring. Then a subset $U \subseteq R$ is *multiplicatively closed* or just *multiplicative* if any (finite) product of elements in U also lives in U.

Note that, by convention, the empty product 1 will need to live in U. So, by induction, U is multiplicatively closed if and only if $1 \in U$ and for $x, y \in U$ to imply $xy \in U$.

Remark 2.3. We do permit $0 \in U$ and more generally zero-divisors to live in U. This tends to not be very interesting for localization.

And here is our main character.

Definition 2.4 (Localization, rings)**.** Fix R a ring and $U \subseteq R$ multiplicatively closed. Then we define $R\left[U^{-1}\right]$ to be the set of ordered pairs $(r, u) \in R \times U$ notated $\frac{r}{u}$ (with $r \in R$ and $u \in U$) modded out by the equivalence relation

$$\frac{r_1}{u_1} = \frac{r_2}{u_2} \iff \text{there exists } v \in U \text{ such that } v(u_2r_1 - u_1r_2) = 0.$$

In the discussion that follows, R will be a ring and U will always be multiplicatively closed.

Remark 2.5 (Nir)**.** One needs the v in the definition above to make $\equiv$ transitive. We run the checks.

- Reflexive: $\frac{r}{u} \equiv \frac{r}{u}$ because $1(ur - ur) = 0$.
- Symmetric: $\frac{r_1}{u_1} \equiv \frac{r_2}{u_2}$ implies some $v \in U$ has $vu_2r_1 = vu_1r_2$ implies $vu_1r_2 = vu_2r_1$ implies $\frac{r_2}{u_2} = \frac{r_1}{u_1}$.
- Transitive: $\frac{r_1}{u_1} \equiv \frac{r_2}{u_2}$ implies some $v_1 \in U$ has $v_1u_2r_1 = v_1u_1r_2$, and $\frac{r_2}{u_2} \equiv \frac{r_3}{u_3}$ implies some $v_2 \in U$ has $v_2u_3r_2 = v_2u_2r_3$. Thus,

  $$(v_1v_2u_2)u_3r_1 = (v_2u_3)v_1u_2r_1 = (v_2u_3)v_1u_1r_2 = (v_1u_1)v_2u_3r_2 = (v_1u_1)v_2u_2r_3 = (v_1v_2u_2)u_1r_3,$$

  so $\frac{r_1}{u_1} \equiv \frac{r_3}{u_3}$.

We can turn $R\left[U^{-1}\right]$ into a ring by using the standard addition and multiplication operations of these numbers. Namely, we define

$$\frac{r}{u} + \frac{s}{v} := \frac{vr + us}{uv} \qquad \text{and} \qquad \frac{r}{u} \cdot \frac{s}{v} := \frac{rs}{uv}.$$

For completeness, we check that these operations do not depend on the exact operation.

- Suppose $\frac{r_1}{u_1} = \frac{r_2}{u_2}$ and $\frac{s_1}{v_1} = \frac{s_2}{v_2}$ so that we are promised $u, v \in U$ such that $uu_2r_1 = uu_1r_2$ and $vv_2s_1 = vv_1s_2$. Now we observe that

  $$\begin{aligned}(uv)(u_2v_2)(v_1r_1 + u_1s_1) &= (vv_1v_2)(uu_2r_1) + (uu_1u_2)(vv_2s_1)\\ &= (vv_1v_2)(uu_1r_2) + (uu_1u_2)(vv_1s_2)\\ &= (uv)(u_1v_1)(v_2r_2 + u_2s_2),\end{aligned}$$

  so it follows $\frac{r_1}{u_1} + \frac{s_1}{v_1} = \frac{v_1r_1+u_1s_1}{u_1v_1} = \frac{v_2r_2+u_2s_2}{u_2v_2} = \frac{r_1}{u_1} + \frac{s_1}{v_1}$.

- Again suppose $\frac{r_1}{u_1} = \frac{r_2}{u_2}$ and $\frac{s_1}{v_1} = \frac{s_2}{v_2}$ so that we are promised $u, v \in U$ such that $uu_2r_1 = uu_1r_2$ and $vv_2s_1 = vv_1s_2$. But now we have
$$(uv)(u_2v_2)(r_1s_1) = (uu_2r_1)(vv_2s_1) = (uu_1r_2)(vv_1s_2) = (uv)(u_1v_1)(r_2s_2),$$
so it follows $\frac{r_1}{u_1} \cdot \frac{s_1}{v_1} = \frac{r_1s_1}{u_1v_1} = \frac{r_2s_2}{u_2v_2} = \frac{r_2}{u_2} \cdot \frac{s_2}{v_2}$.

Now, one can also show that by hand that these operations do in fact form a ring, but this is essentially by construction given how we already know how addition and multiplication of fractions should work. We will not do this check.

Remark 2.6. Observe that because $1 \in U$, there is a canonical map $R \to R\left[U^{-1}\right]$ by $r \mapsto r/1$. This need not be injective; e.g., take $U = \{0, 1\}$, in which case $\frac{r}{1} = \frac{0}{1}$ for each $r \in R$ because $0(1r - 0 \cdot 1) = 0$.

We might also want to localize by sets which are not multiplicatively closed.

Definition 2.7 (Multiplicative closure)**.** Fix R a ring. Then for any $U \subseteq R$, we define the *multiplicative closure* $\overline{U}$ to be the set of all (finite) products of U.

We quickly note that, for any subset $U \subseteq R$, the multiplicative closure $\overline{U}$ is multiplicatively closed. Indeed, any finite product in $\overline{U}$ is a finite product of finite products of U, which can be strung together into just a very large finite product of U. It follows that finite products in $\overline{U}$ stay in $\overline{U}$.

The multiplicative closure lets us adopt the following definition.

Definition 2.8 (Localization, again)**.** Fix R a ring and $U \subseteq R$ an arbitrary subset. We define $R\left[U^{-1}\right] := R\left[\overline{U}^{-1}\right]$.

2.1.3 Examples of Localization

Here are some standard examples of localization.

For our first example, we note that when R is an integral domain, the subset $U = R \setminus \{0\}$ is multiplicatively closed: $a \neq 0$ and $b \neq 0$ implies $ab \neq 0$ because R is an integral domain. So we have the following.

Definition 2.9 (Field of fractions)**.** If R is an integral domain, then $R \setminus \{0\}$ is multiplicatively closed. So we define the *field of fractions*
$$K(R) := R\left[(R \setminus \{0\})^{-1}\right].$$

Example 2.10. We have that $K(\mathbb{Z}) = \mathbb{Q}$.

Example 2.11. We have that $K(k[x]) = k(x)$.

What makes the above example work is that (0) is a prime ideal of R when R is an integral domain (indeed, $ab \in (0)$ implies $ab = 0$ implies $a = 0 \in (0)$ or $b = 0 \in (0)$).

More generally, for $\mathfrak{p} \subseteq R$ a prime ideal, we see that $a, b \notin \mathfrak{p}$ implies $ab \notin \mathfrak{p}$, so $R \setminus \mathfrak{p}$ is multiplicatively closed. So we have the following.

Definition 2.12 (Localization at a prime)**.** Fix R a ring and $\mathfrak{p} \subseteq R$ a prime ideal. Then $R \setminus \mathfrak{p}$ is to be multiplicatively closed, so we define the *localization at a prime*
$$R_{\mathfrak{p}} := R\left[(R \setminus \mathfrak{p})^{-1}\right].$$

As mentioned above, we can realize the field of fractions from this construction.

Example 2.13. When R is an integral domain, (0) is prime, and $R_{(0)} = K(R)$.

Example 2.14. We have that

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

Here are some basic properties of $R_\mathfrak{p}$.

Proposition 2.15. Fix R a ring and $\mathfrak{p} \subseteq R$ a prime ideal. Then $R_\mathfrak{p}$ is a local ring; in particular, $R_\mathfrak{p}$ has unique maximal ideal

$$\mathfrak{p}R_\mathfrak{p} := \left\{ \frac{r}{u} : r \in \mathfrak{p} \text{ and } u \notin \mathfrak{p} \right\}.$$

Proof. Very quickly, we note that $\mathfrak{p}R_\mathfrak{p} \neq R_\mathfrak{p}$ because $\frac{1}{1} \notin \mathfrak{p}R_\mathfrak{p}$. Indeed, for any representative $\frac{1}{1} = \frac{r}{u}$, we see some $v \notin \mathfrak{p}$ has $vr = vu \notin \mathfrak{p}$, so $r \notin \mathfrak{p}$, implying $\frac{r}{u} \notin \mathfrak{p}$.

The main point is to show that all proper ideals are contained in $\mathfrak{p}R_\mathfrak{p}$. Equivalently, suppose that $I \subseteq R$ is an ideal not contained in $\mathfrak{p}R_\mathfrak{p}$, and we show that $I = R_\mathfrak{p}$. Well, we are promised some $\frac{x}{u} \in I \setminus \mathfrak{p}R_\mathfrak{p}$ where $x, u \notin \mathfrak{p}$. But then by closure if I under $R_\mathfrak{p}$-multiplication, we see

$$\frac{1}{1} = \frac{u}{x} \cdot \frac{x}{u} \in I,$$

so indeed, $I = R_\mathfrak{p}$.

We already checked that $\mathfrak{p}R_\mathfrak{p}$ is a proper ideal, so it immediately follows that $\mathfrak{p}R_\mathfrak{p}$ is a maximal ideal: any ideal I with $\mathfrak{p}R_\mathfrak{p} \subsetneq I \subseteq R_\mathfrak{p}$ will immediately force $I = R_\mathfrak{p}$ by the above. Further, $\mathfrak{p}R_\mathfrak{p}$ is the unique maximal ideal because any maximal ideal $\mathfrak{m}$ is proper, so it follows

$$\mathfrak{m} \subseteq \mathfrak{p}R_\mathfrak{p} \subseteq R_\mathfrak{p}.$$

This gives $\mathfrak{m} = \mathfrak{p}R_\mathfrak{p}$ by the maximality of $\mathfrak{m}$, so we are done. ■

Example 2.16. When R is an integral domain and $\mathfrak{p} = (0)$ is the (prime) zero ideal, we see that, indeed $\mathfrak{p}R_\mathfrak{p} = (0)$ is the unique maximal ideal in the field of fractions $K(R) = R_\mathfrak{p}$.

The uniquely special maximal ideal $\mathfrak{p}R_\mathfrak{p}$ gives rise to the following definition for these local rings.

Definition 2.17 (Residue field)**.** Fix R a local ring with unique maximal ideal $\mathfrak{m}$. Then we define the *residue field* to be $\kappa := R/\mathfrak{m}$.

Example 2.18. We have that $\mathbb{Z}_{(p)}/p\mathbb{Z}_{(p)} \cong \mathbb{Z}/p\mathbb{Z}$. Notably, the characteristic has changed.

Remark 2.19. Geometrically, we view primes $\mathfrak{p}$ as living in the "space" $\operatorname{Spec} R$. Then here $R_\mathfrak{p}$ is intended to look like a "neighborhood" or "germ" at the point $\mathfrak{p}$, giving the name localization.

As we hoped for in the motivation, we note that the above examples tend to feature $R\left[U^{-1}\right]$ as the ring R where the elements of U have become invertible. In fact, this notion can be formalized into a universal property for localization.

Proposition 2.20. Fix R a ring and $U \subseteq R$ a multiplicatively closed subset. Let $\varphi : R \to R\left[U^{-1}\right]$ be the canonical map. Now, suppose we are given a ring map $\psi : R \to S$ such that $\psi(U) \subseteq R^\times$. Then there is a unique ring morphism γ making the diagram commute.

$$\begin{tikzcd} R \arrow[r, "\varphi"] \arrow[dr, "\psi"'] & R\left[U^{-1}\right] \arrow[d, dashed, "\gamma"] \\ & S \end{tikzcd}$$

Proof. We tackle uniqueness and existence separately.

- We show that the map γ is unique. For any $r \in R$, observe that we are forced into
$$\gamma(r/1) = \gamma(\varphi(r)) = \psi(r),$$
so γ is forced on elements of the form $\frac{r}{1}$. Further, for any $\frac{r}{u} \in R\left[U^{-1}\right]$, we see that
$$\psi(u)\gamma\left(\frac{r}{u}\right) = \gamma\left(\frac{u}{1}\right)\gamma\left(\frac{r}{u}\right) = \gamma\left(\frac{r}{1}\right) = \psi(r),$$
so we see $\gamma\left(\frac{r}{u}\right) = \psi(u)^{-1}\psi(r)$ forces everything in $R\left[U^{-1}\right]$.
- We now show that the map
$$\gamma\left(\frac{r}{u}\right) := \psi(u)^{-1}\psi(r)$$
is in fact a well-defined R-module homomorphism. Note that $\psi(u) \in S^\times$ by definition of ψ, so at the very least the above expression makes physical sense.
  - We show γ is well-defined. Suppose that $\frac{r_1}{u_1} = \frac{r_2}{u_2}$ so that we need to show $\gamma\left(\frac{r_1}{u_1}\right) = \gamma\left(\frac{r_2}{u_2}\right)$. In other words, we need to show
  $$\psi(u_1)^{-1}\psi(r_1) \stackrel{?}{=} \psi(u_2)^{-1}\psi(r_2).$$
  This is equivalent to showing that
  $$\psi(u_2r_1) = \psi(u_2)\psi(r_1) \stackrel{?}{=} \psi(u_1)\psi(r_2) = \psi(u_1r_2).$$
  Now, we know $\frac{r_1}{u_1} = \frac{r_2}{u_2}$, so there is $u \in U$ such that $uu_2r_1 = uu_1r_2$, so it follows that
  $$\psi(u)\psi(u_2r_1) = \psi(u)\psi(u_1r_2),$$
  so multiplying both sides by $\psi(u)^{-1}$ finishes.
  - We show γ is a ring homomorphism. Quickly, we see $\gamma\left(\frac{1}{1}\right) = \psi(1)^{-1}\psi(1) = 1$. Additionally, for any $\frac{r}{u}, \frac{s}{v} \in R\left[U^{-1}\right]$, we see
  $$\begin{aligned}\gamma\left(\frac{r}{u} + \frac{s}{v}\right) &= \gamma\left(\frac{vr + us}{uv}\right) \\ &= \psi(uv)^{-1}\psi(vr + us) \\ &= \psi(v)^{-1}\psi(v)\psi(u)^{-1}\psi(r) + \psi(u)^{-1}\psi(u)\psi(v)^{-1}\psi(s) \\ &= \gamma\left(\frac{r}{u}\right) + \gamma\left(\frac{s}{v}\right).\end{aligned}$$

Similarly,

$$\begin{aligned}\gamma\left(\frac{r}{u}\cdot\frac{s}{v}\right) &= \gamma\left(\frac{rs}{uv}\right)\\ &= \psi(uv)^{-1}\psi(rs)\\ &= \psi(u)^{-1}\psi(r)\cdot\psi(v)^{-1}\psi(s)\\ &= \gamma\left(\frac{r}{u}\right)\cdot\gamma\left(\frac{s}{v}\right).\end{aligned}$$

This finishes our checks. ■

2.1.4 Localization of Modules

We can also localize modules, in essentially the same way.

Definition 2.21 (Localization, modules)**.** Fix R a ring and $U \subseteq R$ a multiplicatively closed subset. Then, given an R-module M, we define $M\left[U^{-1}\right]$ to be the set of ordered pairs notated $\frac{m}{u}$ (with $m \in M$ and $u \in U$) modded out by the equivalence relation

$$\frac{m_1}{u_1} = \frac{m_2}{u_2} \iff \text{there exists } v \in U \text{ such that } v(u_2m_1 - u_1m_2) = 0.$$

Again, the extra v in the definition is to make $\equiv$ an equivalence relation; this check is the same as the check in Remark 2.5 by replacing all rs with ms.

One can define addition by fractions in the same by-hand way, writing

$$\frac{m_1}{u_1} + \frac{m_2}{u_2} = \frac{u_1m_2 + u_2m_1}{u_1u_2}.$$

Again, it is not too hard to check that this is well-defined (it is essentially the same as the check we did earlier) and gives an abelian group law (which we will actively choose to not write out). Further, $M\left[U^{-1}\right]$ even has an $R\left[U^{-1}\right]$ structure by

$$\frac{r}{v}\cdot\frac{m}{u} := \frac{rm}{vu}.$$

Thus, localizing at U will be able to define a functor from R-modules to $R\left[U^{-1}\right]$-modules.

We remark that we still have a canonical R-module homomorphism $\varphi : M \to M\left[U^{-1}\right]$ by $\varphi : m \mapsto m/1$: to check this is an R-module homomorphism, pick up $r_1, r_2 \in R$ and $m_1, m_2 \in M$, and we see that

$$\varphi(r_1m_1 + r_2m_2) = \frac{r_1m_1 + r_2m_2}{1} = \frac{r_1}{1}\cdot\frac{m_1}{1} + \frac{r_2}{1}\cdot\frac{m_1}{1} = \frac{r_1}{1}\cdot\varphi(m_1) + \frac{r_2}{1}\cdot\varphi(m_2).$$

Again, the canonical map φ need not be injective, but we can describe its kernel.

Lemma 2.22. Fix an R-module M and $U \subseteq R$ a multiplicatively closed subset. Then the kernel of the canonical map $\varphi : M \to M\left[U^{-1}\right]$ is

$$\ker\varphi = \{m \in M : um = 0 \text{ for some } u \in U\}.$$

Proof. We see $m \in \ker\varphi$ if and only if $\frac{m}{1} = \frac{0}{1}$ if and only if there exists $u \in U$ such that $um = 0$. ■

Concretely, viewing a ring R as an R-module, we see the kernel of the canonical map $R \to R\left[U^{-1}\right]$ consists of the $r \in R$ such that $ru = 0$ for some $u \in U$.

Example 2.23. If $0 \in U$, then all of R lives in the kernel of the canonical map $R \to R\left[U^{-1}\right]$.

Example 2.24. If R is an integral domain, then the map $R \to K(R)$ is injective because $ru = 0$ for $r \in R$ and $u \in R \setminus \{0\}$ implies $r = 0$.

2.1.5 Localization of Ideals

We would like to classify ideals under localization. Recall that, given a morphism $\varphi : R \to S$, the pre-image of an ideal $J \subseteq S$ will be an ideal $\varphi^{-1}(J) \subseteq R$.[1]

Remark 2.25. In contrast, given an ideal $I \subseteq R$, we need not have $\varphi(I)$ an ideal of S. Indeed, in the inclusion $\mathbb{Z} \hookrightarrow \mathbb{Q}$, we have $\mathbb{Z} \subseteq \mathbb{Z}$ is an ideal, but the image $\mathbb{Z} \subseteq \mathbb{Q}$ is not an ideal because the image contains 1 but is not the full ring $\mathbb{Q}$.

In fact, we discussed above that prime ideals go to prime ideals. We can also show that this map of ideals preserves inclusions and unions and intersections, which holds on the level that φ is a function of sets.

Lemma 2.26. Fix $f : A \to B$ a function and $S, T \subseteq B$. Then the following are true.

- $f^{-1}(S \cap T) = f^{-1}(S) \cap f^{-1}(T)$.
- $f^{-1}(S \cup T) = f^{-1}(S) \cup f^{-1}(T)$.
- If $S \subseteq T$, then $f^{-1}(S) \subseteq f^{-1}(T)$.

Proof. We take these one at a time.

- Note $x \in f^{-1}(S \cap T)$ if and only if $f(x) \in S \cap T$ if and only if $f(x) \in S$ and $f(x) \in T$ if and only if $x \in f^{-1}(S)$ and $x \in f^{-1}(T)$ if and only if $\in f^{-1}(S) \cap f^{-1}(T)$.
- Rewrite the above argument replacing all $\cap$ with $\cup$ and all "and" with "or."
- Note $S \subseteq T$ is equivalent to $S = S \cap T$, which gives
$$f^{-1}(S) = f^{-1}(S \cap T) = f^{-1}(S) \cap f^{-1}(T) \subseteq f^{-1}(T),$$
finishing. ■

Now, in our case, we are focusing on the canonical morphism $\varphi : R \to R\left[U^{-1}\right]$. We have the following sequence of propositions.

Lemma 2.27. Fix R a ring and $U \subseteq R$ a multiplicatively closed set, and let $\varphi : R \to R\left[U^{-1}\right]$ be the canonical map.

Then given any $R\left[U^{-1}\right]$-ideal I, pre-image followed by localization does nothing:
$$I = \varphi^{-1}(I)\left[U^{-1}\right].$$
It follows that the map from $R\left[U^{-1}\right]$-ideals to R-ideals by $I \mapsto \varphi^{-1}(I)$ is injective.

Proof. Fix $I \subseteq R\left[U^{-1}\right]$ an ideal. Formally, $\varphi^{-1}(I)$ is the set of elements $x \in R$ such that $\frac{x}{1} \in I$, so
$$\varphi^{-1}(I)\left[U^{-1}\right] = \left\{\frac{x}{u} : \frac{x}{1} \in I \text{ and } u \in U\right\}.$$
We identify this with a subset of $R\left[U^{-1}\right]$ in the obvious way, and we note that this identification preserves the $R\left[U^{-1}\right]$-module structure because we defined localization of modules with the same $R\left[U^{-1}\right]$-action and addition law as the ring $R\left[U^{-1}\right]$ itself.

Now, we show $I = \varphi^{-1}(I)\left[U^{-1}\right]$ by taking the inclusions separately.

- We show that $\varphi^{-1}(I)\left[U^{-1}\right] \subseteq I$. Indeed, any $\frac{x}{u} \in \varphi^{-1}(I)\left[U^{-1}\right]$ will have $\frac{x}{1} \in I$, so $\frac{x}{u} = \frac{1}{u} \cdot \frac{x}{1} \in I$ because I is closed under $R\left[U^{-1}\right]$.

[1] If r_1, r_2 and $x_1, x_2 \in \varphi^{-1}(J)$, then $\varphi(r_1x_1 + r_2x_2) = r_1\varphi(x_1) + r_2\varphi(x_2) \in J$ by closure, so $r_1x_1 + r_2x_2 \in \varphi^{-1}(J)$.

- It remains to show $I \subseteq \varphi^{-1}(I)\left[U^{-1}\right]$. Well, fix some $\frac{r}{u} \in I$. Then, because I is an $R\left[U^{-1}\right]$-ideal, we see
$$\frac{r}{1} = \frac{u}{1} \cdot \frac{r}{u} \in I,$$
so it follows that $r \in \varphi^{-1}(I)$, and so $\frac{r}{u} \in \varphi^{-1}(I)\left[U^{-1}\right]$. This finishes.

We finish by showing that $I \mapsto \varphi^{-1}(I)$ is injective. Indeed, if $I, J \subseteq R\left[U^{-1}\right]$ are ideals such that $\varphi^{-1}(I) = \varphi^{-1}(J)$ implies that
$$I = \varphi^{-1}(I)\left[U^{-1}\right] = \varphi^{-1}(J)\left[J^{-1}\right] = J,$$
so we are done. ■

Lemma 2.28. Fix R a ring and $U \subseteq R$ a multiplicatively closed set, and let $\varphi : R \to R\left[U^{-1}\right]$ be the canonical map.

Further, fix an R-ideal J. The following are equivalent.

(i) $J = \varphi^{-1}(I)$ for some $R\left[U^{-1}\right]$-ideal I.

(ii) $J = \varphi^{-1}\left(J\left[U^{-1}\right]\right)$.

(iii) If $ru \in J$ for some $r \in R$ and $u \in U$, then $r \in J$. In other words, $U \cap J = \varnothing$ and $U/J \subseteq R/J$ contains no zero-divisors.

Proof. We show our implications separately.

- We show that (ii) implies (i). For this, we only need to show that $J\left[U^{-1}\right]$ is an ideal of $R\left[U^{-1}\right]$. But this is true because $J\left[U^{-1}\right]$ is an $R\left[U^{-1}\right]$-module, and we can see set-wise that it is a subset of $R\left[U^{-1}\right]$, and the operations match up by how $J\left[U^{-1}\right]$ is defined.

  Thus, $J\left[U^{-1}\right]$ is an $R\left[U^{-1}\right]$-submodule of $R\left[U^{-1}\right]$, which is exactly an $R\left[U^{-1}\right]$-ideal.

- We show that (i) implies (ii). Fix $I \subseteq R\left[U^{-1}\right]$ an ideal, and let $J := \varphi^{-1}(I)$. Then we claim that $J = \varphi^{-1}\left(J\left[U^{-1}\right]\right)$. Well, we see
$$J\left[U^{-1}\right] = \varphi^{-1}(I)\left[U^{-1}\right] = I$$
by Lemma 2.27, so it follows $J = \varphi^{-1}(U) = \varphi^{-1}\left(J\left[U^{-1}\right]\right)$.

- We show that (ii) implies (iii). We are given an R-ideal J such that $J = \varphi^{-1}\left(J\left[U^{-1}\right]\right)$. Now, given any $u \in U$, we show that $[u]_J \in R/J$ is not a zero-divisor.

  Indeed, suppose that $ru \in J$ for any $r \in R$ and $u \in U$. But then
$$\frac{r}{1} = \frac{ru}{u} \in J\left[U^{-1}\right],$$
so it follows $r \in \varphi^{-1}\left(J\left[U^{-1}\right]\right) = J$. This finishes.

- We show that (iii) implies (ii). Fix an R-ideal J such that $ru \in J$ with $r \in R$ and $u \in U$ implies $r \in J$. We show that $J = \varphi^{-1}\left(J\left[U^{-1}\right]\right)$.

  We can show $J \subseteq \varphi^{-1}\left(J\left[U^{-1}\right]\right)$ without the hypothesis: any $x \in J$ has $\frac{x}{1} \in J\left[U^{-1}\right]$, so $x \in \varphi^{-1}\left(J\left[U^{-1}\right]\right)$.

  The reverse inclusion is harder. Fix some $x \in \varphi^{-1}\left(J\left[U^{-1}\right]\right)$, which implies $\frac{x}{1} \in J\left[U^{-1}\right]$. But then we can find some $\frac{y}{u} \in J\left[U^{-1}\right]$ such that
$$\frac{x}{1} = \frac{y}{u},$$
so it follows there is some $v \in U$ such that $v(ux - y) = 0 \in J$. So by hypothesis on J and U, we see that $ux - y \in J$ is forced, so $ux \in J$, so $x \in J$. This finishes. ■

And finally here is our classification of ideals under localization.

Theorem 2.29. Fix R a ring and $U \subseteq R$ a multiplicatively closed set, and let $\varphi : R \to R\left[U^{-1}\right]$ be the canonical map. Then φ^{-1} provides a bijection between the prime ideals of R which are disjoint from U and the prime ideals of $R\left[U^{-1}\right]$.

Proof. This will follow from the above properties. Observe that φ^{-1} will indeed send prime ideals of $R\left[U^{-1}\right]$ to prime ideals of R, and this mapping is injective.

Thus, it remains to show that the image of φ^{-1} on $\operatorname{Spec} R\left[U^{-1}\right]$ is as described. Well, by Lemma 2.28, these are exactly the prime R-ideals $\mathfrak{p}$ such that, if $ru \in \mathfrak{p}$ for some $r \in \mathfrak{p}$ and $u \in U$, then $r \in \mathfrak{p}$. Call these primes "good," which we want to show is equivalent to being disjoint from U.

Certainly, if $\mathfrak{p}$ is a prime disjoint from U, then $ru \in \mathfrak{p}$ for $r \in \mathfrak{p}$ and $u \in U$, then $u \notin \mathfrak{p}$ will force $r \in \mathfrak{p}$; thus, $\mathfrak{p}$ is good. So conversely, if $\mathfrak{p}$ is not disjoint from U, then set $u \in U \cap \mathfrak{p}$, and we see

$$1u \in \mathfrak{p}$$

while $1 \notin \mathfrak{p}$ (prime ideals are proper), so it follows that $\mathfrak{p}$ is not good. ■

Here is a reason to care about the above our study of ideals under localization.

Corollary 2.30. Any localization of a Noetherian ring R is still a Noetherian ring.

Proof. Fix an ideal $I \subseteq R\left[U^{-1}\right]$, and we show that it is finitely generated. Well, $\varphi^{-1}(I) \subseteq R$ is an ideal, which is finitely generated because R is Noetherian, so fix generators

$$\varphi^{-1}(I) = (x_1, \ldots, x_n).$$

Now we claim that

$$I = (x_1/1, \ldots, x_n/1)$$

as an $R\left[U^{-1}\right]$-ideal. Certainly $(x_1/1, \ldots, x_n/1) \subseteq I$. In the other direction, given any $\frac{x}{u} \in I$, we see that $\frac{x}{1} = \frac{u}{1} \cdot \frac{x}{u} \in I$, so $x \in \varphi^{-1}(I)$. But then we can write

$$x = \sum_{k=1}^{n} r_k x_k$$

for some constants r_k. It follows

$$\frac{x}{u} = \sum_{k=1}^{n} \frac{r_k}{u} \cdot \frac{x_k}{1} \in (x_1/1, \ldots, x_n/1),$$

finishing. ■

2.1.6 The Hom-Functor

Later in life we will discuss localization as a tensor product, but before then we must talk about the tensor product, so for now we will talk about the Hom-functor.

Warning 2.31. The following two subsections do not contain many proofs. This is mostly due to laziness; the interested are referred to my 250A notes or any other standard algebra reference.

Here is our definition.

Definition 2.32 (Hom)**.** Fix R a ring. Then, for R-modules M and N, we define $\operatorname{Hom}_R(M, N)$ to be the abelian group of R-module homomorphisms $M \to N$.

In fact, we can endow $\operatorname{Hom}_R(M, N)$ with an R-module structure, essentially because our rings are commutative. Namely, we define

$$(r\varphi)(m) := r \cdot \varphi(m).$$

It is not too hard to verify that this does in fact define a ring action.

Definition 2.33 (End)**.** Fix R a ring and M an R-module. Then we define the *endomorphisms* of M to be $\operatorname{End}_R(M) := \operatorname{Hom}_R(M, M)$.

Note that $\operatorname{End}_R(M)$ is in fact a (non-commutative) R-algebra, where our multiplication is given by composition.

Here are some basic facts with short explanations as is necessary.

1. We have that $\operatorname{Hom}_R(R, M) \cong M$ canonically by $\varphi \mapsto \varphi(1)$.

2. Given two morphisms $\alpha : M_2 \to M_1$ and $\beta : N_1 \to N_2$, then we have a map $\operatorname{Hom}_R(M_1, N_1) \to \operatorname{Hom}_R(M_2, N_2)$ by $\varphi \mapsto \beta \circ \varphi \circ \alpha$. In fact, this is an R-module homomorphism.

3. We have that
$$\operatorname{Hom}_R\left(\bigoplus_{\alpha \in I} M_\alpha, N\right) \cong \prod_{\alpha \in I} \operatorname{Hom}_R(M_\alpha, N)$$
for any collection of R-modules $\{M_\alpha\}_{\alpha \in I}$. The main point is that, to define a map $\bigoplus_\alpha M_\alpha \to N$, is exactly the same information as describing what to do with each $M_\beta \hookrightarrow \bigoplus_\alpha M_\alpha \to N$ copy.

4. In fact, Hom is a left-exact functor. Namely, exact sequences
$$0 \to A \to B \to C$$
yields the exact sequence
$$0 \to \operatorname{Hom}_R(M, A) \to \operatorname{Hom}_R(M, B) \to \operatorname{Hom}_R(M, C).$$
Similarly,
$$0 \to \operatorname{Hom}_R(C, M) \to \operatorname{Hom}_R(B, M) \to \operatorname{Hom}_R(A, M)$$
is exact. Note the reversed direction of arrows here. The easiest way to see this is by the tensor-hom adjuction: Hom is a right adjoint, so it preserves limits, so it preserves kernels, so it is left-exact.

Remark 2.34. However, Hom_R does not fully preserve short exact sequences. In the first, case we are saying that a morphism $\operatorname{Hom}_R(M, C)$ might not be extendable to a map $\operatorname{Hom}_R(M, B)$. By way of example, consider the short exact sequence of $\mathbb{Z}$-modules

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

Then taking $\operatorname{Hom}_{\mathbb{Z}}(\mathbb{Z}/2\mathbb{Z}, -)$ gives

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

which is not exact in the last term.

Remark 2.35 (Nir)**.** Many of these isomorphisms are "functorial" in a suitable sense. For example, the isomorphism $\operatorname{Hom}_R(R, M) \cong M$ is functorial as follows: given $\varphi : M \to N$, the following diagram commutes.

$$\begin{tikzcd} \operatorname{Hom}_R(R,M) \arrow[r, "\varphi"] \arrow[d, "\cong"'] & \operatorname{Hom}_R(R,M) \arrow[d, "\cong"] \\ M \arrow[r, "\varphi"] & N \end{tikzcd}$$

Here the map $\varphi : \operatorname{Hom}_R(R, M) \to \operatorname{Hom}_R(R, N)$ is by $f \mapsto \varphi \circ f$. To see that this diagram commutes, note that some $f \in \operatorname{Hom}_R(R, M)$ goes $f \mapsto \varphi f \mapsto (\varphi \circ f)(1)$ along the top; similarly it goes $f \mapsto f(1) \mapsto \varphi(f(1))$ along the bottom.

2.1.7 Tensor Product

We should probably start by defining tensor products, which requires defining bilinear maps.

Definition 2.36 (Bilinear)**.** Fix A, B, C as R-modules for some ring R. Then a map $\varphi : A \times B \to C$ is R-*bilinear* if and only if is R-linear in both arguments. Namely, we require

$$\varphi(r_1a_1 + r_2a_2, b) = r_1\varphi(a_1, b) + r_2\varphi(a_2, b)$$

and

$$\varphi(a, r_1b_1 + r_2b_2) = r_1\varphi(a, b_1) + r_2\varphi(a, b_2).$$

This lets us define the tensor product to more or less be the object universal with respect to giving bilinear maps.

Definition 2.37 (Tensor product)**.** Fix R a ring and A and B as R-modules. Then we define $A \otimes_R B$ to be the free module generated by $a \otimes b$ for $a \in A$ and $b \in B$ modulo the relation

$$(a_1m_1 + a_2m_2) \otimes (b_1n_1 + b_2n_2) = a_1b_1(m_1 \otimes n_1) + a_1b_2(m_1 \otimes n_2) + a_2b_1(m_2 \otimes n_1) + a_2b_2(m_2 \otimes n_2).$$

Elements of the tensor product $A \otimes B$ are in general not very easy to understand and in general they can be described as being some finite sum of elements $a \otimes b$ for various $a \in A$ and $b \in B$. In the case where A and B are vector spaces over a field, then the tensor of two basis vectors will create a basis (we will prove this below), but this is essentially the only general example.

Nevertheless, let's do an example.

Example 2.38. We work in $\mathbb{Z}$-mod, and we compute $\mathbb{Z}/2\mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Z}/3\mathbb{Z}$. It will be enough to consider elements of the form $m \otimes n$. The main point is that

$$2(m \otimes n) = 2m \otimes n = 0 \qquad \text{and} \qquad 3(m \otimes n) = m \otimes 3n = 0,$$

so $m \otimes n = 0$ follows. Thus, $\mathbb{Z}/2\mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Z}/3\mathbb{Z} = 0$.

As with Hom_R, the tensor product $\otimes_R$ has the following list of nice properties. Again, we provide short explanations as is necessary.

1. We have that $M \cong R \otimes_R M$ by $m \mapsto 1 \otimes m$. We can see that the inverse map is $r \otimes m \mapsto rm$.
2. Given morphisms $\alpha : M_1 \to M_2$ and $\beta : N_1 \to N_2$, we can define a map

   $$\alpha \otimes \beta : M_1 \otimes_R N_1 \to M_2 \otimes_R N_2$$

   by extending $m \otimes n \mapsto \alpha m \otimes \beta n$ linearly to the full tensor product. The map $\alpha \otimes \beta$ can be checked to be an R-module homomorphism.

3. We have that $M \otimes_R N \cong N \otimes_R M$ by $m \otimes n \mapsto n \otimes m$.
4. We have that
$$\left(\bigoplus_{\alpha \in I} M_\alpha\right) \otimes_R N \cong \bigoplus_{\alpha \in I}(M_\alpha \otimes_R N).$$
The most hands-free way to see this is the tensor-hom adjuction: tensoring is a left adjoint, so it preserves colimits, so it preserves coproducts.
5. The functor $- \otimes_R M$ is right-exact: given an exact sequence
$$A \to B \to C \to 0,$$
we have an exact sequence
$$A \otimes_R M \to B \otimes_R M \to C \otimes_R M \to 0.$$
Here the maps are the induced ones. The easiest way to see this is by the tensor-hom adjuction: tensoring is a left adjoint, so it preserves colimits, so it preserves cokernels, so it is right-exact.

Remark 2.39 (Nir). As in Remark 2.35, many of the above isomorphisms are functorial. For example, the isomorphism $R \otimes_R M \cong M$ is functorial as follows: given $\varphi : M \to N$, the following diagram commutes.
$$\begin{tikzcd} M \arrow[r, "\varphi"] \arrow[d, "\cong"'] & N \arrow[d, "\cong"] \\ R \otimes_R M \arrow[r, "\varphi"'] & R \otimes_R N \end{tikzcd}$$
Here the map $\varphi : R \otimes_R M \to R \otimes_R N$ is induces as $r \otimes m \mapsto r \otimes \varphi(m)$. To see the commutativity, note that some $m \in M$ will go $m \mapsto \varphi(m) \mapsto 1 \otimes \varphi(m)$ along the top, and similarly it will go $m \mapsto 1 \otimes m \mapsto 1 \otimes \varphi(m)$ along the bottom.

Here are some example applications.

Exercise 2.40. Fix a and b integers. Then
$$\mathbb{Z}/a\mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Z}/b\mathbb{Z} \cong \mathbb{Z}/\gcd(a,b)\mathbb{Z}.$$

Proof. Tensoring the right-exact sequence
$$\mathbb{Z} \stackrel{\times a}{\to} \mathbb{Z} \to \mathbb{Z}/a\mathbb{Z} \to 0$$
by $\mathbb{Z}/b\mathbb{Z}$ gives the right-exact sequence
$$\mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Z}/b\mathbb{Z} \stackrel{\times a}{\to} \mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Z}/b\mathbb{Z} \to \mathbb{Z}/a\mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Z}/b\mathbb{Z} \to 0.$$
Using the canonical isomorphisms $\mathbb{Z} \otimes_{\mathbb{Z}} M \cong M$ for abelian groups M and tracking our morphisms through, we get the right-exact sequence
$$\mathbb{Z}/b\mathbb{Z} \stackrel{\times a}{\to} \mathbb{Z}/b\mathbb{Z} \to \mathbb{Z}/a\mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Z}/b\mathbb{Z} \to 0.$$
It follows that
$$\mathbb{Z}/a\mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Z}/b\mathbb{Z} \cong \frac{\mathbb{Z}/b\mathbb{Z}}{a\mathbb{Z}/b\mathbb{Z}} = \frac{\mathbb{Z}/b\mathbb{Z}}{(a\mathbb{Z}+b\mathbb{Z})/b\mathbb{Z}} \cong \frac{\mathbb{Z}}{a\mathbb{Z}+b\mathbb{Z}}.$$
This finishes. ■

Remark 2.41. The above example also shows that the functor $-\otimes_R M$ need not be fully exact. For example, tensoring

$$0 \to \mathbb{Z} \stackrel{\times 2}{\to} \mathbb{Z}$$

by $\mathbb{Z}/2\mathbb{Z}$ gives the sequence of maps

$$0 \to \mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Z}/2\mathbb{Z} \stackrel{\times 2}{\to} \mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Z}/2\mathbb{Z}.$$

However, the map $\stackrel{\times 2}{\to}$ now takes $k \otimes \ell \mapsto 2k \otimes \ell = k \otimes 2\ell = 0$, so this sequence is not exact.

Example 2.42. Let V and W to be two k-vector spaces with bases $\{v_\alpha\}_{\alpha \in I}$ and $\{w_\beta\}_{\beta \in J}$. This means that

$$V \cong \bigoplus_{\alpha \in I} k v_\alpha \qquad \text{and} \qquad W \cong \bigoplus_{\beta \in J} k w_\beta,$$

so the above facts let us write

$$V \otimes_k W \cong \bigoplus_{\alpha \in I, \beta \in J} (k v_\alpha \otimes_k k w_\beta).$$

Now, $kv_\alpha \otimes_k kw_\beta \cong kv_\alpha \cong k$ canonically by $xv_\alpha \otimes w_\beta \mapsto xv_\alpha \mapsto x$, so we can view each $kv_\alpha \otimes_k kw_\beta$ as a one-dimensional k-vector space. Tracking the above isomorphism forwards, we see that the elements $v_\alpha \otimes w_\beta \in V \otimes_k W$ are forming a k-basis.

Next time we will show $M\left[U^{-1}\right]$ is canonically isomorphic to $R\left[U^{-1}\right] \otimes_R M$ to continue our discussion of localization.

2.2 January 27

We localize more.

2.2.1 Flat Modules

Last time we left off with the right-exactness of the tensor product: a right-exact sequence of R-modules

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

becomes a right-exact sequence

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

for any other R-module M. More formally, we have the following statement.

Proposition 2.43. Fix R a ring and M an R-module. Then the functor $M \otimes_R - : \operatorname{Mod}_R \to \operatorname{Mod}_R$ is right-exact.

Proof. This is a restatement of the discussion above. ■

However, it is not true that a short exact sequence

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

will always become a short exact sequence

$$0 \to M \otimes_R A \to M \otimes_R B \to M \otimes_R C \to 0.$$

In fact, this is rather rare! Explicitly, the problem is that $M \otimes_R A \to M \otimes_R B$ might not be injective, ruining exactness at the front, and this is the only obstruction by right-exactness.

Example 2.44. We work in $\mathrm{Mod}_{\mathbb{Z}}$, and let n be a positive integer. Then tensoring the short exact sequence

$$0 \to \mathbb{Z} \stackrel{\times n}{\to} \mathbb{Z} \to \mathbb{Z}/n\mathbb{Z} \to 0$$

with $\mathbb{Z}/n\mathbb{Z}$ will give the commutative diagram

$$\begin{tikzcd}
\mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Z}/n\mathbb{Z} \arrow[r, "\times n"] \arrow[d] & \mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Z}/n\mathbb{Z} \arrow[r] \arrow[d] & \mathbb{Z}/n\mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Z}/n\mathbb{Z} \arrow[r] \arrow[d] & 0 \\
\mathbb{Z}/n\mathbb{Z} \arrow[r, "f"] & \mathbb{Z}/n\mathbb{Z} \arrow[r] & \mathbb{Z}/n\mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Z}/n\mathbb{Z} \arrow[r] & 0
\end{tikzcd}$$

after tracking through the canonical isomorphisms $\mathbb{Z} \otimes_{\mathbb{Z}} M \cong M$. But we can see that f here sends $[k]_n$ lifts to $1 \otimes [k]_n$, which goes to $n \otimes [k]_n = 1 \otimes [0]_n$ and therefore is $[0]_n$ downstairs. So f is the zero map and not injective for any $n > 1$.

But sometimes left-exactness will be preserved, and this is a property worthy of a name.

Definition 2.45 (Flat)**.** Fix R a ring. Then an R-module M is *flat* if and only if the functor $M \otimes_R -$ is exact.

Remark 2.46. As above, we note that $M \otimes_R -$ will always be right-exact, so M will be flat if and only if it preserves the injectivity at the end of a short exact sequence. In other words, $A \hookrightarrow B$ induces $M \otimes_R A \hookrightarrow M \otimes_R B$.

Example 2.47. The ring R is a flat module because $R \otimes_R M \cong M$ (canonically). Explicitly, the following diagram commutes because the map $M \cong R \otimes_R M$ is $m \mapsto 1 \otimes m$.

$$\begin{tikzcd}
A \arrow[r] \arrow[d] & B \arrow[d] \\
R \otimes_R A \arrow[r] & R \otimes_R B
\end{tikzcd}$$

It follows $R \otimes_R A \to R \otimes_R B$ is injective when $A \hookrightarrow B$ is injective because this map is the composite $R \otimes_R A \cong A \hookrightarrow B \cong R \otimes_R B$, which is injective as the composite of injective maps.

Example 2.48. Any free R-module R^n is also flat by using direct sums. In particular, if we have $A \to B$, then the following diagram commutes.

$$\begin{tikzcd}
R^n \otimes_R A \arrow[r] \arrow[d] & R^n \otimes_R B \arrow[d] \\
(R \otimes_R A)^n \arrow[r] & (R \otimes_R B)^n
\end{tikzcd}$$

Indeed, the map $R^n \otimes_R A \to (R \otimes_R A)^n$ is by $(r_k)_{k=1}^n \otimes a \mapsto (r_k \otimes a)_{k=1}^n$, so the commutativity follows. But we see that $A \hookrightarrow B$ means the individual maps $R \otimes_R A \to R \otimes_R B$ are injective, so the bottom row is injective. Tracking the isomorphisms through, we see the top row is also forced to be injective.

2.2.2 Localization via Tensoring

Now let's return to discussing localization, which plays nicely with the tensor product and flatness.

Proposition 2.49. Fix R a ring and $U \subseteq R$ a multiplicatively closed subset. Then, for any R-module M, we have a canonical $R\left[U^{-1}\right]$-module isomorphism

$$R\left[U^{-1}\right] \otimes_R M \cong M\left[U^{-1}\right]$$

by $r/u \otimes m \mapsto r/u \cdot m$. (Here, $R\left[U^{-1}\right] \otimes_R M$ is given $R\left[U^{-1}\right]$ by multiplication on the left coordinate.)

Proof. We define our maps in both directions explicitly. To go $\varphi : M\left[U^{-1}\right] \to R\left[U^{-1}\right] \otimes_R M$, we define

$$\boxed{\varphi : m/u \mapsto 1/u \otimes m}.$$

For now, we have to check that this is well-defined and an $R\left[U^{-1}\right]$-module homomorphism.

- Well-defined: suppose that $\frac{m_1}{u_1} = \frac{m_2}{u_2}$. Then there is $u \in U$ so that $uu_2m_1 = uu_1m_2$. It follows that

$$\frac{1}{u_1} \otimes m_1 = \left(\frac{1}{uu_1u_2} \cdot uu_2\right) \otimes m_1 = \frac{1}{uu_1u_2} \otimes uu_2m_1 = \frac{1}{uu_1u_2} \otimes uu_1m_2,$$

  and now running this in reverse shows $\frac{1}{u_1} \otimes m_1 = \frac{1}{u_2} \otimes m_2$.

- Homomorphic: fix $\frac{m_1}{u_1}, \frac{m_2}{u_2} \in M\left[U^{-1}\right] \otimes_R M$ and $\frac{s_1}{v_1}, \frac{s_2}{v_2} \in R\left[U^{-1}\right]$. Then we compute

$$\begin{aligned}
\varphi\left(\frac{s_1}{v_1} \cdot \frac{m_1}{u_1} + \frac{s_2}{v_2} \cdot \frac{m_2}{u_2}\right) &= \varphi\left(\frac{s_1m_1}{v_1u_1} + \frac{s_2m_2}{v_2u_2}\right) \\
&= \varphi\left(\frac{v_2u_2s_1m_1 + v_1u_1s_2m_2}{v_1u_1v_2u_2}\right) \\
&= \frac{1}{v_1u_1v_2u_2} \otimes (v_2u_2s_1m_1 + v_1u_1s_2m_2) \\
&= \frac{1}{v_1u_1v_2u_2} \otimes v_2u_2s_1m_1 + \frac{1}{v_1u_1v_2u_2} \otimes v_1u_1s_2m_2 \\
&= \frac{s_1}{v_1u_1} \otimes m_1 + \frac{s_2}{v_2u_2} \otimes m_2 \\
&= \frac{s_1}{v_1}\left(\frac{1}{u_1} \otimes m_1\right) + \frac{s_2}{v_2}\left(\frac{1}{u_2} \otimes m_2\right) \\
&= \frac{s_1}{v_1}\varphi\left(\frac{m_1}{u_1}\right) + \frac{s_2}{v_2}\varphi\left(\frac{m_2}{u_2}\right),
\end{aligned}$$

  which is what we wanted.

In the other direction, we note that we have an R-bilinear map $\psi : R\left[U^{-1}\right] \times M \to M\left[U^{-1}\right]$ by

$$(r/u, m) \mapsto rm/u.$$

Quickly, this is well-defined because $\frac{r_1}{u_1} = \frac{r_2}{u_2}$ promises u such that $uu_2r_1 = uu_1r_2$, so $uu_2r_1m = uu_1r_2m$, so $\frac{r_1m}{u_1} = \frac{r_2m}{u_2}$. Now, to check R-bilinearity, it suffices to check that

$$\psi(r/u, r_1m_1 + r_2m_2) = \frac{r(r_1m_1 + r_2m_2)}{u} = r_1 \cdot \frac{rm_1}{u} + r_2 \cdot \frac{rm_2}{u_2} = r_1\psi(r/u, m_1) + \psi(r/u, m_2),$$

and

$$\psi\left(s_1 \cdot \frac{r_1}{u_1} + s_2 \cdot \frac{r_2}{u_2}, m\right) = \psi\left(\frac{u_2s_1r_1 + u_1s_2r_2}{u_1u_2}, m\right) = s_1 \cdot \frac{r_1}{u_1} \cdot m + \frac{r_2}{u_2} \cdot m$$

after some moving around, which is what we needed.

The point is that we are promised an R-module homomorphism $\psi : R\left[U^{-1}\right] \otimes_R M \to M\left[U^{-1}\right]$ by

$$\boxed{\psi : r/u \otimes m \mapsto rm/u}$$

and extending linearly to the full tensor product. It suffices to show ψ is inverse to φ, which will show φ is an $R\left[U^{-1}\right]$-module isomorphism, and the same will hold for ψ, finishing

- Given $m/u \in M\left[U^{-1}\right]$, we note that $(\psi \circ \varphi)(m/u) = \psi(1/u \otimes m) = 1m/u = m/u$, so $\psi \circ \varphi = \mathrm{id}_{M[U^{-1}]}$.
- Given $\sum_{k=1}^n (r_k/u_k \otimes m_k) \in R\left[U^{-1}\right] \otimes_R M$, we see that

$$(\varphi \circ \psi)\left(\sum_{k=1}^n \frac{r_k}{u_k} \otimes m_k\right) = \varphi\left(\sum_{k=1}^n \frac{r_k m_k}{u_k}\right) = \sum_{k=1}^n \frac{1}{u_k} \otimes r_k m_k = \sum_{k=1}^n \frac{r_k}{u_k} \otimes m_k,$$

so $\varphi \circ \psi = \mathrm{id}_{R[U^{-1}]\otimes_R M}$. ■

Remark 2.50. The above canonical isomorphism is functorial in the following sense. If we have a map $\varphi : A \to B$, then the following diagram commutes, where all arrows are the induced maps.

$$\begin{tikzcd} R\left[U^{-1}\right] \otimes_R A \arrow[r] \arrow[d] & R\left[U^{-1}\right] \otimes_R B \arrow[d] \\ A\left[U^{-1}\right] \arrow[r] & B\left[U^{-1}\right] \end{tikzcd}$$

Indeed, we take $\frac{r}{u} \otimes a \mapsto \frac{r}{u} \otimes \varphi(a) \mapsto \frac{r\varphi(a)}{u}$ along the top, and we take $\frac{r}{u} \otimes a \mapsto \frac{ra}{u} \mapsto \frac{\varphi(ra)}{u} = \frac{r\varphi(a)}{u}$ along the bottom.

The above is nice because it means we technically would only need to check that $R\left[U^{-1}\right]$ exists in order to define localization of general modules. In other words, we have a somewhat unified paradigm to think about localization by merely focusing on tensor products.

As a quick example, we can see that localization commutes with direct sums.

Proposition 2.51. Fix R a ring and $U \subseteq R$ a multiplicatively closed subset with $\mathcal{M}$ a collection of R-modules. Then

$$\left(\bigoplus_{M\in\mathcal{M}} M\right)\left[U^{-1}\right] \cong \bigoplus_{M\in\mathcal{M}} M\left[U^{-1}\right]$$

by sending $\frac{1}{u}(m_M)_{M\in\mathcal{M}} \mapsto \left(\frac{m_M}{u}\right)_{M\in\mathcal{M}}$.

Proof. The main point is that tensor products commute with direct sums. Indeed, we have the canonical isomorphisms

$$\left(\bigoplus_{M\in\mathcal{M}} M\right)[U^{-1}] \cong \left(\bigoplus_{M\in\mathcal{M}} M\right) \otimes_R R[U^{-1}] \stackrel{*}{\cong} \bigoplus_{M\in\mathcal{M}} M \otimes_R R[U^{-1}] \cong \prod_{i=1}^n M\left[U^{-1}\right],$$

where in $\stackrel{*}{\cong}$ we used the fact that tensor products commute with arbitrary direct sums. Actually tracking these isomorphisms through, we see that $\frac{1}{u}(m_M)_{M\in\mathcal{M}}$ goes to $(m_M)_{M\in\mathcal{M}} \otimes 1/u$ goes to $(m_M \otimes 1/u)_{M\in\mathcal{M}}$ goes to $(m_M/u)_{M\in\mathcal{M}}$, which is what we wanted. ■

2.2.3 Localization via Flatness

The following result looks like it's about localization but is actually about flatness.

Proposition 2.52. Fix R a ring and $U \subseteq R$ a multiplicatively closed subset. Then localization is an exact functor: given a short exact sequence of R-modules

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

then we have a short exact sequence of $R\left[U^{-1}\right]$-modules

$$0 \to A\left[U^{-1}\right] \to B\left[U^{-1}\right] \to C\left[U^{-1}\right] \to 0.$$

Proof. For visual reasons, note that we have the following commutative diagram where the vertical arrows are $R\left[U^{-1}\right]$-module isomorphisms. (The diagram commutes by Remark 2.50.)

$$\begin{tikzcd} 0 \arrow[r] & A\left[U^{-1}\right] \arrow[r] \arrow[d] & B\left[U^{-1}\right] \arrow[r] \arrow[d] & C\left[U^{-1}\right] \arrow[r] \arrow[d] & 0 \\ 0 \arrow[r] & R\left[U^{-1}\right] \otimes_R A \arrow[r] & R\left[U^{-1}\right] \otimes_R B \arrow[r] & R\left[U^{-1}\right] \otimes_R C \arrow[r] & 0 \end{tikzcd}$$

This is to say that it suffices to show that the bottom row is exact. The right-exactness of the bottom row follows from the fact that it is induced by the tensoring functor $R\left[U^{-1}\right] \otimes_R -$.

Thus, we only need to show that localization preserves embeddings. Letting $\varphi : A \hookrightarrow B$ be the original map and $\overline{\varphi} : A\left[U^{-1}\right] \to B\left[U^{-1}\right]$ be the induced map, then we need to check that $\ker \overline{\varphi}$ is trivial. Well, if $\overline{\varphi}\left(\frac{a}{u}\right) = 0$ for some $\frac{a}{u} \in A\left[U^{-1}\right]$, then we note

$$\frac{0}{1} = \overline{\varphi}\left(\frac{a}{u}\right) = \frac{\varphi(a)}{u},$$

so there exists $v \in U$ such that $\varphi(va) = v\varphi(a) = 0$. Because $\ker \varphi$ is trivial, we are forced to have $va = 0$, so $\frac{a}{u} = 0$. Thus, $\ker \overline{\varphi}$ is indeed trivial. ■

Corollary 2.53. Fix R a ring and $U \subseteq R$ a multiplicatively closed subset. Then $R\left[U^{-1}\right]$ is flat as an R-module.

Proof. The commutative diagram in the proof of Proposition 2.52 has been shown to have exact rows (over the course of the entire proof). The exactness of the bottom row shows $R\left[U^{-1}\right]$ is flat. ■

Corollary 2.54. Fix R a ring and $U \subseteq R$ a multiplicative subset. Then let $\varphi : A \to B$ be an R-module homomorphism and $\overline{\varphi} : A\left[U^{-1}\right] \to B\left[U^{-1}\right]$ be the localized morphism. Then

$$(\ker \varphi)\left[U^{-1}\right] \cong \ker \overline{\varphi} \quad \text{and} \quad (\operatorname{coker} \varphi)\left[U^{-1}\right] \cong \operatorname{coker} \overline{\varphi}.$$

In particular, if φ is injective/surjective/isomorphic, then $\overline{\varphi}$ is injective/surjective/isomorphic.

Proof. We deal with the kernel and the cokernel separately.

- The main point is that we have the short exact sequence

$$0 \to \ker \varphi \to A \xrightarrow{\varphi} \operatorname{im} \varphi \to 0.$$

Localizing, we get the short exact sequence

$$0 \to (\ker \varphi)\left[U^{-1}\right] \to A\left[U^{-1}\right] \xrightarrow{\overline{\varphi}} (\operatorname{im} \varphi)\left[U^{-1}\right] \to 0.$$

By exactness, we see that $(\ker \varphi)\left[U^{-1}\right] \cong \ker \overline{\varphi}$.
Thus, φ being injective implies $\ker \varphi = 0$ implies $\ker \overline{\varphi} = 0$ implies $\overline{\varphi}$ is injective.

- The main point is that we have the short exact sequence

$$0 \to A/\ker \varphi \xrightarrow{\varphi} B \to \operatorname{coker} \varphi \to 0,$$

where $\xrightarrow{\varphi}$ is actually the induced map. Localizing, we get the short exact sequence

$$0 \to (A/\ker \varphi)\left[U^{-1}\right] \xrightarrow{\overline{\varphi}} B\left[U^{-1}\right] \to (\operatorname{coker} \varphi)\left[U^{-1}\right] \to 0.$$

By exactness again, we see that $(\operatorname{coker} \varphi)\left[U^{-1}\right] \cong \operatorname{coker} \varphi$.
Thus, φ being surjective implies $\operatorname{coker} \varphi = 0$ implies $\operatorname{coker} \overline{\varphi} = 0$ implies $\overline{\varphi}$ is surjective.

Combining the two points implies that, if φ is isomorphic (namely, bijective), then $\overline{\varphi}$ will be as well. ■

Flatness also gives us the following result, which again looks like it's about localization but is really about flatness.

Corollary 2.55. Fix R a ring and $U \subseteq R$ a multiplicatively closed subset. Then, taking $M_1, \ldots, M_n \subseteq M$ finitely many R-modules of some R-module M, we get

$$\bigcap_{i=1}^n M_i\left[U^{-1}\right] = \left(\bigcap_{i=1}^n M_i\right)\left[U^{-1}\right].$$

Note these intersections make sense because the M_i all live inside M.

Proof. The main point is that intersections can be realized as a kernel. Namely, consider the left-exact sequence

$$0 \to \bigcap_{i=1}^n M_i \to M \to \prod_{i=1}^n M/M_i. \qquad (*)$$

It is not too hard to check manually that this sequence is in fact left-exact: the map $\bigcap M_i \to M$ is an embedding and hence injective, and $x \in \ker\left(M \to \prod M/M_i\right)$ if and only if $x \in M_i$ for each M_i if and only if $x \in \bigcap M_i$.

Now, we would like to localize $(*)$. Before doing so, we note that Proposition 2.51 gives us the canonical isomorphism

$$\left(\prod_{i=1}^n M/M_i\right)\left[U^{-1}\right] \cong \prod_{i=1}^n (M/M_i)\left[U^{-1}\right],$$

which is legal because finite products are in fact coproducts. (Here is where we use the finiteness condition!) As in Proposition 2.51, we can actually track through these isomorphisms as sending $\frac{1}{u}([x_k]_{M_i})_{i=1}^n$ to $\left(\frac{1}{u}[x_k]_{M_i}\right)_{i=1}^n$.

Continuing, we note that we can compute $(M/M_i)\left[U^{-1}\right]$ by localizing the short exact sequence

$$0 \to M_i \to M \to M/M_i \to 0,$$

which will tell us that $\frac{M}{M_i}\left[U^{-1}\right] \cong \frac{M\left[U^{-1}\right]}{M_i\left[U^{-1}\right]}$ by $\frac{1}{u}[x]_{M_i} \mapsto \left[\frac{x}{u}\right]_{M_i\left[U^{-1}\right]}$. Stitching these isomorphisms together gives us an isomorphism

$$\left(\prod_{i=1}^n M/M_i\right)\left[U^{-1}\right] \cong \prod_{i=1}^n \frac{M\left[U^{-1}\right]}{M_i\left[U^{-1}\right]}$$

by taking $\frac{1}{u}\left([x_k]_{M_i}\right)_{i=1}^n$ to $\left([\frac{x_k}{u}]_{M_i[U^{-1}]}\right)_{i=1}^n$.

Only now we do localize (∗). Upon localization, we get the left-exact sequence[2]

$$0 \to \left(\bigcap_{i=1}^n M_i\right)\left[U^{-1}\right] \to M\left[U^{-1}\right] \to \left(\prod_{i=1}^n M/M_i\right)\left[U^{-1}\right] \cong \prod_{i=1}^n \frac{M\left[U^{-1}\right]}{M_i\left[U^{-1}\right]},$$

By exactness, we see that to prove the result it remains to compute the kernel of the composite

$$M\left[U^{-1}\right] \to \left(\prod_{i=1}^n M/M_i\right)\left[U^{-1}\right] \cong \prod_{i=1}^n \frac{M\left[U^{-1}\right]}{M_i\left[U^{-1}\right]}.$$

Well, this map sends $\frac{x}{u}$ to $\frac{1}{u}([x]_{M_i})_{i=1}^n$ to $\left([\frac{x}{u}]\right)_{i=1}^n$, so the only way for to be in the kernel is for $\frac{x}{u} \in M_i\left[U^{-1}\right]$ for each M_i. It follows that the kernel is

$$\bigcap_{i=1}^n M_i\left[U^{-1}\right],$$

which is what we wanted. ■

We need to be careful because localization need not commute with infinite intersections.

Example 2.56. Set $R := k[x]$ and $U = R \setminus \{0\}$. The main issue is that

$$\bigcap_{a\in k}(x-a) = (0).$$

Now, on one hand, $(x-a)\left[U^{-1}\right] = k(x)$ because U is allowed to divide by $(x-a)$. On the other hand, $(0)\left[U^{-1}\right] = (0)$ because no amount of division can make 0 nonzero. Thus,

$$\left(\bigcap_{a\in k}(x-a)\right)\left[U^{-1}\right] = (0)\left[U^{-1}\right] = (0) \neq k(x) = \bigcap_{a\in k}(x-a)\left[U^{-1}\right].$$

2.2.4 Tensor–Restriction Adjunction

We start by discussing a particular adjuction. We have the following definition.

Definition 2.57 (Restriction)**.** Fix S an R-algebra, which means we are promised a ring homomorphism $\psi : R \to S$. Given an S-module N, we can give N an R-action by

$$r \cdot x := \psi(r)x.$$

The abelian group N with this R-action is the *restriction* $\operatorname{Res}_R^S N$.

In other words, the S-action on N is equivalent to a ring map $S \to \operatorname{End} N$, so we get an R-action by pre-composition: $R \xrightarrow{\psi} S \to \operatorname{End} N$.

Lemma 2.58. Fix S an R-algebra. Then the map $\operatorname{Res}_R^S : \operatorname{Mod}_S \to \operatorname{Mod}_R$ is a functor.

[2] Being exact implies being left-exact. If this causes discomfort, replace the left-exact sequence $0 \to A \to B \to C$ with the short exact sequence $0 \to A \to B \to \operatorname{im}(B \to C) \to 0$.

Proof. For concreteness, fix our map $\psi : R \to S$. We start by discussing how to restrict morphisms. Given an S-module morphism $f : M \to N$, we claim that the "function data" of φ in fact makes an R-module morphism $\operatorname{Res}_R^S(f) : \operatorname{Res}_S^R M \to \operatorname{Res}_S^R N$. In other words, we define

$$\operatorname{Res}_R^S(f)(m) := f(m).$$

Note this makes $\operatorname{Res}_R^S(f)$ at least a morphism of abelian groups, so in particular it is additive. So to check that $\operatorname{Res}_R^S(f)$ is an R-module morphism, we merely pick up $r \in R$ and $m \in M$ and note

$$\operatorname{Res}_R^S(f)(rm)f(\psi(r)m) = \psi(r)f(m) = r \cdot \operatorname{Res}_R^S(f)(m).$$

Now, to show functoriality, we note that $\operatorname{Res}_R^S(\mathrm{id}_M)(m) = m$ for any S-module M and $m \in M$. And for $f : A \to B$ and $g : B \to C$ morphisms of S-modules, we have $\operatorname{Res}_R^S(g \circ f)(a) = (g \circ f)(a) = \left(\operatorname{Res}_R^S(g) \circ \operatorname{Res}_R^S(g)\right)(a)$. ■

In the other direction, if M is an R-module, we can create an S-module the "induced" module $\operatorname{Ind}_R^S M := S \otimes_R M$, where we get an S-action by multiplying on the left coordinate.

Because tensoring is functorial, we get that $S \otimes_R -$ is automatically a functor $\mathrm{Mod}_R \to \mathrm{Mod}_R$. So to check that $S \otimes_R -$ is a functor $\mathrm{Mod}_R \to \mathrm{Mod}_S$, it suffices to show $f : A \to B$ in Mod_R can actually be a lifted to an S-module morphism $S \otimes_R A \to S \otimes_R B$. Well, f is already additive, so we merely check

$$f(s(x \otimes a)) = f(sx \otimes a) = sx \otimes f(a) = s(x \otimes f(a)) = s \cdot f(x \otimes a).$$

Thus, we do indeed have a functor $\mathrm{Mod}_R \to \mathrm{Mod}_S$.

With functors going in both directions introduced like this, they had better form an adjoint pair.

Proposition 2.59. Let S be an R-algebra. Then, given an R-module M and an S-module N, we have a canonical isomorphism (of abelian groups)

$$\operatorname{Hom}_R(M, \operatorname{Res}_R^S N) \cong \operatorname{Hom}_S(S \otimes_R M, N).$$

Proof. We construct forwards and backwards maps manually.

- Fix $f \in \operatorname{Hom}_R(M, \operatorname{Res}_R^S N)$. Then we define $\widetilde{f} \in \operatorname{Hom}_S(S \otimes_R M, N)$ by defining

  $$\widetilde{f}(s \otimes m) = sf(m).$$

  Note the computation $sf(m)$ in the above is viewing $f(m) \in N$ as an S-module. We have the following checks on $f \mapsto \overline{f}$.

  - Well-defined: to show there is a map $\widetilde{f} : S \otimes_R M \to N$ as described, we need to show that $\widetilde{f} : S \times R \to N$ defined by

    $$\widetilde{f}(s, m) := sf(m)$$

    is R-bilinear. Given $r_1, r_2 \in R$ and $s_1, s_2 \in S$ and $m \in M$,

    $$\widetilde{f}(r_1s_1 + r_2s_2, m) = (r_1s_1 + r_2s_2)f(m) = r_1\widetilde{f}(s_1, m) + r_2\widetilde{f}(s_2, m).$$

    Given $s \in S$ and $r_1, r_2 \in R$ and $m \in M$,

    $$\widetilde{f}(s, r_1m_1 + r_2m_2) = sf(r_1m_1 + r_2m_2) = r_1\widetilde{f}(s, m_1) + r_2\widetilde{f}(s, m_2).$$

    Thus, we have an R-module map $\widetilde{f} : S \otimes_R M \to N$. To check $\widetilde{f}$ is an S-module map, we note that $\widetilde{f}$ is already additive, so it suffices to pick up $s \in S$ and $x \otimes m \in S \otimes_R M$ and note

    $$\widetilde{f}(s(x \otimes m)) = \widetilde{f}((sx) \otimes m) = (sx)f(m) = s\widetilde{f}(x \otimes m).$$

- Homomorphic: we show that $f \mapsto \widetilde{f}$ is a homomorphism of (abelian) groups. Indeed, fix $f, g \in \operatorname{Hom}_R(M, \operatorname{Res}_R^S N)$ and $s \otimes m \in S \otimes_R M$ so that

$$\widetilde{f+g}(s \otimes m) = s(f+g)(m) = sf(m) + sg(m) = (\widetilde{f} + \widetilde{g})(s \otimes m).$$

- Injective: we show $f \mapsto \widetilde{f}$ has trivial kernel. Indeed, suppose $f \in \operatorname{Hom}_R(M, \operatorname{Res}_R^S N)$ has $\widetilde{f} = 0$. Then, for any $m \in M$, we see

$$f(m) = 1_S f(m) = \widetilde{f}(1_S \otimes m) = 0.$$

- In the other direction, motivated by the above injectivity check, we notice that we have an R-module map $\iota : M \to S \otimes_R M$ by $m \mapsto 1_S \otimes m$. Indeed, for $r_1, r_2 \in R$ and $m_1, m_2 \in M$, we see

$$\iota(r_1 m_1 + r_2 m_2) = 1_S \otimes (r_1 m_1 + r_2 m_2) = r_1 \iota(m_1) + r_2 \iota(m_2).$$

Now, suppose that we have some $g \in \operatorname{Hom}_S(S \otimes_R M, N)$. Note that the same underlying function g is an R-module map as well: g is already additive, so we need to check that $r \in R$ and $s \otimes m \in S \otimes_R M$ has

$$r \cdot g(s \otimes m) = r1_S \cdot g(s \otimes m) = g(r1_S \cdot s \otimes m) = g(r(s \otimes m)).$$

Thus, we are granted the map $g \mapsto g \circ \iota$ from $\operatorname{Hom}_S(S \otimes_R M, N)$ to $\operatorname{Hom}_R(M, \operatorname{Res}_R^S N)$.

Note that it merely remains to check the surjectivity of $f \mapsto \widetilde{f}$, so it suffices to show that, for any $g \in \operatorname{Hom}_S(S \otimes_R M, N)$, we have

$$\widetilde{g \circ \iota} = g.$$

Indeed, given $m \in M$,

$$\widetilde{g \circ \iota}(s \otimes m) = s(g \circ \iota)(m) = sg(1 \otimes m) = g(s \otimes m),$$

where in the last step we are viewing g as an S-module map. This finishes. ■

Remark 2.60. One can in fact show that the exhibited isomorphism makes tensoring left-adjoint to restriction. We will not run the checks to form an adjoint pair.

2.2.5 Base Change

Next let's discuss base change. Again, fix S an R-algebra. Given two R-modules named M and N, we can form S-modules

$$S \otimes_R \operatorname{Hom}_R(M, N) \qquad \text{and} \qquad \operatorname{Hom}_S(S \otimes_R M, S \otimes_R N),$$

where the functor $S \otimes_R - : \mathrm{Mod}_R \to \mathrm{Mod}_S$ was described in the previous subsection. In general, there need not be an isomorphism between these S-modules, but there is a canonical map from the left to the right.

Lemma 2.61. Fix S an R-algebra with R-modules M and N. Then there is a canonical S-module map

$$\alpha : S \otimes_R \operatorname{Hom}_R(M, N) \to \operatorname{Hom}_S(S \otimes_R M, S \otimes_R N).$$

Proof. The main idea is to use Proposition 2.59. To begin with, note that there is a function

$$\gamma : \operatorname{Hom}_R(M, N) \to \operatorname{Hom}_S(S \otimes_R M, S \otimes_R N)$$

by using the fact $S \otimes_R -$ is a functor. In particular, $f : M \to N$ has $\gamma(f)(s \otimes m) = s \otimes f(m)$. Observe that γ in fact induces a function

$$\gamma : \operatorname{Hom}_R(M, N) \to \operatorname{Res}_R^S \operatorname{Hom}_S(S \otimes_R M, S \otimes_R N)$$

because the underlying sets involved have not changed. We claim that γ is in fact an R-module morphism. Well, fix $r_1, r_2 \in R$ and $f_1, f_2 \in \operatorname{Hom}_R(M,N)$ with $s \otimes m \in S \otimes_R M$, and we see

$$\gamma(r_1f_1 + r_2f_2)(s\otimes m) = s \otimes (r_1f_1 + r_2f_2)(m) = r_1(s\otimes f_1(m)) + r_2(s \otimes f_2(m)) = \big(r_1\gamma(f_1) + r_2\gamma(f_2)\big)(s\otimes m).$$

Now, because γ is an R-module map, Proposition 2.59 promises a canonical map

$$\widetilde{\gamma} : S \otimes_R \operatorname{Hom}_R(M,N) \to \operatorname{Hom}(S\otimes_R M, S \otimes_R N).$$

In fact, we can compute $\widetilde{\gamma}$ by tracking Proposition 2.59 and γ through. Given $s \otimes f \in S \otimes_R \operatorname{Hom}_R(M,N)$ and $s_0 \otimes m_0 \in S \otimes_R M$, we have

$$\widetilde{\gamma}(s\otimes f)(s_0 \otimes m_0) = s \cdot \gamma(f)(s_0\otimes m_0) = s \cdot (s_0 \otimes f(m_0)) = (ss_0) \otimes f(m_0).$$

This finishes. ■

Remark 2.62 (Nir). We briefly remark that α is functorial in M: if we have a map $\varphi : M \to M'$, then the following diagram commutes, where the vertical maps are induced.

$$\begin{tikzcd}
S \otimes_R \operatorname{Hom}_R(M',N) \arrow[r, "\alpha"] \arrow[d, "\varphi"'] & \operatorname{Hom}_S(S\otimes_R M', S\otimes_R N) \arrow[d, "\varphi"] \\
S \otimes_R \operatorname{Hom}_R(M,N) \arrow[r, "\alpha"'] & \operatorname{Hom}_S(S\otimes_R M, S\otimes_R N)
\end{tikzcd}$$

To see this, track some $s \otimes f$ from the top-left.

- Moving along the top, $s \otimes f$ goes to $(s_0 \otimes m_0') \mapsto (ss_0 \otimes f(m_0'))$ goes to $(s_0 \otimes m_0) \mapsto (ss_0 \otimes f(\varphi m_0))$.
- Moving along the bottom, $s \otimes f$ goes to $s_0 \otimes f\varphi$ goes to $(s_0 \otimes m_0) \mapsto (ss_0 \otimes f(\varphi m_0))$.

We would like the above α to be an isomorphism, but this requires some hypotheses. To start, here is a special case, which we will generalize shortly.

Lemma 2.63. Work in the set-up of Lemma 2.61. If $M = R^n$ for some positive integer n, then α is an isomorphism.

Proof. We proceed by brute force. We will just show directly that $S \otimes_R \operatorname{Hom}_R(R^n, N) \cong \operatorname{Hom}_S(S \otimes_R R^n, S \otimes_R N)$, and tracking the isomorphism through will reveal that it is α. Pick up some $s \otimes f \in S \otimes_R \operatorname{Hom}_R(R^n, N)$ which we will track through.

- Note that $S \otimes_R \operatorname{Hom}_R(R^n, N) \cong S \otimes_R \operatorname{Hom}_R(R,N)^n \cong S \otimes_R N^n$ by sending $s \otimes f$ to $s \otimes (1_R \mapsto f(e_k))_{k=1}^n$ to $s \otimes (f(e_k))_{k=1}^n$.
  (Here, the $e_\bullet$ are the basis for R^n.)
- Note that $S \otimes_R N^n \cong (S \otimes N)^n$ by sending $s \otimes (f(e_k))_{k=1}^n$ to $(s \otimes f(e_k))_{k=1}^n$.
- Note that $(S \otimes_R N)^n \cong \operatorname{Hom}_S(S^n, S \otimes_R N)$ by sending $(s \otimes f(e_k))_{k=1}^n$ to the morphism

$$(s_k)_{k=1}^n \mapsto \sum_{k=1}^n ss_k \otimes f(e_k).$$

- Note that $\operatorname{Hom}_S(S^n, S\otimes_R N) \cong \operatorname{Hom}_S((S \otimes_R R)^n, S \otimes_R N)$ by sending the morphism $(s_k)_{k=1}^n \mapsto \sum_k ss_k \otimes f(e_k)$ to the morphism defined by $(s_k \otimes 1)_{k=1}^n \mapsto \sum_k ss_k \otimes f(e_k)$.
  In particular, the morphism in the codomain is

$$(s_k \otimes r_k)_{k=1}^n \mapsto \sum_{k=1}^n ss_k \otimes f(r_ke_k).$$

- Note that $\operatorname{Hom}_S((S \otimes_R R)^n, S \otimes_R N) \cong \operatorname{Hom}_S(S \otimes R^n, S \otimes_R N)$ by sending $(s_k \otimes r_k)_{k=1}^n \mapsto \sum_k ss_k \otimes r_k f(e_k)$ to

$$s_0 \otimes (r_k)_{k=1}^n \mapsto \sum_{k=1}^n ss_0 \otimes f(r_k e_k) = ss_0 \otimes f\left((r_k)_{k=1}^n\right).$$

So indeed, we have tracked our isomorphism, and we can see from the last point that $s \otimes f$ has gone to $s_0 \otimes m \mapsto ss_0 \otimes f(m)$, as needed by α. ■

We would like to extend the above argument to work more generally, but this will require some hypotheses. One condition will be that S is flat over R; for the other condition we have the following definition.

Definition 2.64 (Finitely presented). An R-module M is *finitely presented* if and only if there are M is finitely generated, and we can find R^m an R^n making the following right-exact sequence

$$R^m \to R^n \to M \to 0.$$

In other words, we need to be able to find some R^m which can surject onto the kernel of $R^n \twoheadrightarrow M$; i.e., the kernel of our map $R^n \twoheadrightarrow M$ is finitely generated.

Example 2.65. The free R-module R^n is finitely presented due to the sequence $0 \to R^n \to R^n \to 0$.

Example 2.66. Fix R a Noetherian ring and M a finitely generated module. Then there is R^n with a map $\varphi : R^n \to M$. Now, because R is Noetherian, R^n will be a Noetherian module (see Proposition 1.51), so the R-submodule $\ker\varphi \subseteq R^n$ will be finitely generated over R. Thus, M is finitely presented.

Non-Example 2.67. Let $R = k[x_1, x_2, \ldots]$ and $I = (x_1, x_2, \ldots)$. Then we claim R/I is finitely generated (because $R \twoheadrightarrow R/I$) but not finitely presented. Indeed, if R/I were finitely presented, then there would be a sequence $0 \to K \to R^m \to R/I \to 0$ where K is finitely generated; comparing this with $0 \to I \to R \to R/I \to 0$ will force I to be finitely generated, which is false.

This gives us the following commutative diagram.

$$\begin{tikzcd} 0 \arrow[r] & K \arrow[r] \arrow[d, dashed] & R^m \arrow[r] \arrow[d, dashed] & R/I \arrow[r] \arrow[d, equal] & 0 \\ 0 \arrow[r] & I \arrow[r] & R \arrow[r] & R/I \arrow[r] & 0 \end{tikzcd}$$

The middle arrow is induced by R^m being projective: we take the images of the basis vectors $R^m \to R/I$ and then pull them back in whatever way we want to R, defining a map $R^m \to R$. The diagram induces the map $K \to I$.

The snake lemma now tells us that $\operatorname{coker}(K \to I) \cong \operatorname{coker}(R^m \to R)$, which is finitely generated because R will surject onto it. But then the short exact sequence

$$0 \to \operatorname{im}(K \to I) \to I \to \operatorname{coker}(K \to I) \to 0$$

forces I to be finitely generated.

Now, here is the culmination of base change.

Proposition 2.68. Work in the set-up of Lemma 2.61. Then if S is flat and M is finitely presented, then the α from Lemma 2.61 is an isomorphism.

Proof. We begin by writing down the finite presentation

$$R^m \to R^n \to M \to 0$$

of M. The idea is to M is "close enough" to being R^n, allowing us to reduce to Lemma 2.63.

We now create two left-exact sequences.

- Taking $\operatorname{Hom}_R(-, N)$ gives us a left-exact sequence

$$0 \to \operatorname{Hom}_R(M, N) \to \operatorname{Hom}_R(R^n, N) \to \operatorname{Hom}_R(R^m, N),$$

and by flatness of S, we get another left-exact sequence

$$0 \to S \otimes_R \operatorname{Hom}_R(M, N) \to S \otimes_R \operatorname{Hom}_R(R^n, N) \to S \otimes_R \operatorname{Hom}_R(R^m, N). \tag{1}$$

- Alternatively, note that we directly have a right-exact sequence

$$S \otimes_R R^m \to S \otimes_R R^n \to S \otimes_R M \to 0,$$

upon which $\operatorname{Hom}_S(-, S \otimes_R N)$ gives the right-exact sequence

$$0 \to \operatorname{Hom}_S(S \otimes_R M, S \otimes_R N) \to \operatorname{Hom}_S(S \otimes_R R^n, S \otimes_R N) \to \operatorname{Hom}_S(S \otimes_R R^m, S \otimes_R N). \tag{2}$$

Now we can relate (1) and (2) by α: functoriality of α (see Remark 2.62) gives the following commutative diagram with exact rows.

$$\begin{tikzcd}
0 \arrow[r] & S \otimes_R \operatorname{Hom}_R(M, N) \arrow[r] \arrow[d, "\alpha"] & S \otimes_R \operatorname{Hom}_R(R^n, N) \arrow[r] \arrow[d, "\alpha"] & S \otimes_R \operatorname{Hom}_R(R^m, N) \arrow[d, "\alpha"] \\
0 \arrow[r] & \operatorname{Hom}_S(S \otimes_R M, S \otimes_R N) \arrow[r] & \operatorname{Hom}_S(S \otimes_R R^n, S \otimes_R N) \arrow[r] & \operatorname{Hom}_S(S \otimes_R R^m, S \otimes_R N)
\end{tikzcd}$$

But now the rightmost two vertical αs are isomorphisms by Lemma 2.63, so the leftmost α is also an isomorphism. This finishes. ■

Remark 2.69 (Nir)**.** When R is Noetherian and M is finitely generated (alternatively, only M is finitely presented), we note that M is finitely presented by Example 2.66. Further, for multiplicative U, we see $R\left[U^{-1}\right]$ is flat by Corollary 2.53. So Proposition 2.49 in addition to the above tells us

$$\operatorname{Hom}_R(M, N)\left[U^{-1}\right] \cong \operatorname{Hom}_{R[U^{-1}]}\left(M\left[U^{-1}\right], N\left[U^{-1}\right]\right).$$

This will be our chief application of Proposition 2.68.

Remark 2.70 (Nir)**.** I am really proud of the working out of the discussion in this subsection. There are a lot of moving parts.

2.2.6 Support of a Module

We have the following definition.

Definition 2.71 (Support)**.** Fix R a ring and M an R-module. Then we define the *support* of M to be

$$\operatorname{Supp} M := \{\mathfrak{p} \in \operatorname{Spec} R : M_{\mathfrak{p}} \neq 0\}.$$

There is an analogous notion of maximal support using maximal ideals instead of prime ideals.

We can provide a more concrete condition for $M_{\mathfrak{p}} = 0$. For this, we have the following definition.

Definition 2.72 (Annihilator)**.** Fix R a ring and M an R-module. Then, given an element $m \in M$, we define the *annihilator* of R to be

$$\operatorname{Ann} m := \{r \in R : rm = 0\}.$$

Analogously, we define $\operatorname{Ann} M := \{r \in R : rm = 0 \text{ for all } m \in M\} = \bigcap_{m \in M} \operatorname{Ann} m$.

Remark 2.73. It is not hard to check that these are ideals. If $r_1, r_2 \in R$ and $x_1, x_2 \in \operatorname{Ann} m$, then

$$(r_1 x_1 + r_2 x_2)m = r_1(x_1 m) + r_2(x_2 m) = 0$$

verifies that $r_1x_1 + r_2x_2 \in \operatorname{Ann} m$, so $\operatorname{Ann} m$ is closed under R-linear combination. So $\operatorname{Ann} m$ is an ideal, and the fact $\operatorname{Ann} M$ is an ideal follows by taking the (arbitrary) intersection.

So here is a characterization of $\operatorname{Supp} M$.

Proposition 2.74. Fix R a ring and M an R-module. Then, given $\mathfrak{p} \in \operatorname{Spec} R$, we have $M_\mathfrak{p} \neq 0$ if and only if $\operatorname{Ann} m \subseteq \mathfrak{p}$ for some $m \in M$. In other words,

$$\operatorname{Supp} M = \bigcup_{m \in M} \{\mathfrak{p} \in \operatorname{Spec} R : \operatorname{Ann} m \subseteq \mathfrak{p}\}.$$

Proof. We proceed by contraposition, showing that $M_\mathfrak{p} = 0$ if and only if $\operatorname{Ann} m \not\subseteq \mathfrak{p}$ for each $m \in M$.

Note that $M_\mathfrak{p} = 0$ if and only if $\frac{m}{u} = 0$ for each $m \in M$ and $u \in U$. But note that if $\frac{m}{1} = 0$ for each $m \in M$, then it follows

$$\frac{m}{u} = \frac{1}{u} \cdot \frac{1}{m} = 0$$

for any $u \in U$. Thus, it suffices to check that $\frac{m}{1} = 0$ for each $m \in M$.

Well, fixing any $m \in M$, we see that $\frac{m}{1} = \frac{0}{1}$ if and only if there is some $u \notin \mathfrak{p}$ such that $um = 0$. In other words, $\frac{m}{1} = \frac{0}{1}$ is equivalent to

$$(R \setminus \mathfrak{p}) \cap \operatorname{Ann} m \neq \varnothing,$$

which is equivalent to $\operatorname{Ann} m \not\subseteq \mathfrak{p}$. ■

The above characterization of the support is a bit annoying, geometrically speaking, because we are taking an arbitrary union of (Zariski) closed sets $\{\mathfrak{p} \in \operatorname{Spec} R : \operatorname{Ann} m \subseteq \mathfrak{p}\}$. In the case where M is finitely generated (which is essentially a size constraint on M), we can make this arbitrary union into a finite one.

Proposition 2.75. Fix R a ring and M a finitely generated R-module. Then

$$\operatorname{Supp} M = \{\mathfrak{p} \in \operatorname{Spec} R : \operatorname{Ann} M \subseteq \mathfrak{p}\}.$$

Proof. Of course, taking any $m \in M$, if $\operatorname{Ann} m \subseteq \mathfrak{p}$ for some $m \in M$, then $\operatorname{Ann} M \subseteq \operatorname{Ann} m \subseteq \mathfrak{p}$. So Proposition 2.74 tells us that

$$\operatorname{Supp} M = \bigcup_{m \in M} \{\mathfrak{p} \in \operatorname{Spec} R : \operatorname{Ann} m \subseteq \mathfrak{p}\} \subseteq \{\mathfrak{p} \in \operatorname{Spec} R : \operatorname{Ann} M \subseteq \mathfrak{p}\}.$$

The other direction requires using that M is finitely generated.

Well, let $\mathfrak{p} \notin \operatorname{Supp} M$, and we show that $\operatorname{Ann} M \not\subseteq \mathfrak{p}$. The fact that $\mathfrak{p} \notin \operatorname{Supp} M$ implies that $\operatorname{Ann} m \not\subseteq \mathfrak{p}$ for each $m \in M$; in particular, letting M be generated by $x_1, \ldots, x_n$, we see that each $x_k \in M$ promises u_k such that

$$u_k \in \operatorname{Ann} x_k \setminus \mathfrak{p}.$$

In other words, $u_k \notin \mathfrak{p}$ and $u_k x_k = 0$. But now (by finiteness!) we can set

$$u := \prod_{k=1}^{n} u_k.$$

Because each of the factors is not in $\mathfrak{p}$, we conclude $u \notin \mathfrak{p}$. However, $ux_k = 0$ for each of the generators x_k, so for any $m = \sum a_k x_k \in M$, we see

$$um = \sum_{k=1}^{n} ua_k x_k = \sum_{k=1}^{n} a_k \cdot 0 = 0.$$

It follows that $u \in \operatorname{Ann} M \setminus \mathfrak{p}$, so $\operatorname{Ann} M \not\subseteq \mathfrak{p}$. ■

In particular, this is a (Zariski) closed subset of $\operatorname{Spec} R$!

We close this subsection with some examples.

Example 2.76. Consider the ring $M := R$ as an R-module. Certainly $0 \in \operatorname{Ann} R$, but for $r \in R$ to kill 1, we need $r = 0$, so actually $\operatorname{Ann} R = (0)$. But (0) is contained in every prime ideal of R, so $\operatorname{Supp} R = \operatorname{Spec} R$. (Yes, $M = R$ is finitely generated over R.)

Example 2.77. Fix R a ring and $M = (0)$ the zero module. Then everyone in R will kill 0, so $\operatorname{Ann} 0 = R$. It follows from Proposition 2.74 that $\operatorname{Supp}(0) = \varnothing$ because no prime contains R.

Example 2.78. More generally, fix $I \subseteq R$ an ideal. Then we claim $\operatorname{Ann} R/I = I$. Indeed, if $x \in I$, then $x \cdot [r]_I = [rx]_I = [0]_I$, so $x \in \operatorname{Ann} R/I$. Conversely, if $x \in \operatorname{Ann} R/I$, then $x \cdot [1]_I = [x]_I$ must vanish, so $x \in I$.

To set up our last example, we have the following definition and then statement.

Definition 2.79 (Simple)**.** Fix R a ring. Then an R-module M is said to be *simple* if and only if all R-submodules of M are either (0) or M.

Exercise 2.80. Fix R a ring and M a simple nonzero R-module. Then the following are true.

(a) We have that $M \cong R/\operatorname{Ann} M$.

(b) We have that $\operatorname{Ann} M$ is a maximal ideal.

(c) We have that $\operatorname{Supp} M = \{\operatorname{Ann} M\}$.

Proof. We take the claims more or less one at a time.

(a) Because M is nonzero, we may find $x \in M \setminus \{0\}$. Now, x induces an R-module homomorphism map $R \to M$ by $r \mapsto rx$ (indeed, $rs \mapsto rsx$ and $r_1 + r_2 \mapsto r_1 x + r_2 x$), and the kernel of this map is $\{r \in R : rx = 0\} = \operatorname{Ann} x$. Thus, we have the left-exact sequence of R-modules

$$0 \to \operatorname{Ann} x \to R \to M.$$

However, M is simple! Thus, because the image of $R \to M$ will end up being an R-submodule of M—and nonzero because it contains $1x = x \neq 0$—we see that the image of $R \to M$ must be all of M. So in fact we have the short exact sequence

$$0 \to \operatorname{Ann} x \to R \to M \to 0.$$

In particular, we just showed that $M = \{rx : r \in R\} = Rx$. Of course, $\operatorname{Ann} M \subseteq \operatorname{Ann} x$, but in fact equality holds: each $a \in \operatorname{Ann} x$ will have $a(rx) = r(ax) = 0$ for each $rx \in Rx = m$.

Anyways, the point is that $R/\operatorname{Ann} M \cong M$ (non-canonically) by $r \mapsto rx$.

(b) We show that $I := \operatorname{Ann} M$ is a maximal ideal. Certainly $I \neq R$ because then $M \cong R/R = (0)$ would be zero. Thus, I is proper, so we can find a maximal ideal $\mathfrak{m}$ such that $I \subseteq \mathfrak{m}$. But then we consider the composite map $\varphi : M \to R/\mathfrak{m}$ by

$$M \cong R/I \to R/\mathfrak{m}.$$

Consider $\ker \varphi$. On one hand, note that $\ker \varphi \neq M$ because φ is the composite of surjective maps and therefore surjective, and $R/\mathfrak{m}$ is nonzero (M being nonzero forces R nonzero), so φ cannot send all of M to 0.

But $\ker \varphi$ is an R-submodule of M, so instead we must have $\ker \varphi = (0)$. So the composite φ is injective, so the map $R/I \to R/\mathfrak{m}$ is injective. But then $x \in \mathfrak{m}$ implies $[x]_I \mapsto [x]_\mathfrak{m} = [0]_\mathfrak{m}$, so $x \in I$ by injectivity. Thus, $\mathfrak{m} = I$, and so I is in fact maximal.

(c) Because $R \twoheadrightarrow R/\operatorname{Ann} M \cong M$, we see that M is finitely generated, so Proposition 2.75 tells us that

$$\operatorname{Supp} M = \{\mathfrak{p} \in \operatorname{Spec} R : \operatorname{Ann} M \subseteq \mathfrak{p}\}.$$

Now, $\operatorname{Ann} M$ is maximal, so $\operatorname{Ann} M \in \operatorname{Supp} M$, but any prime ideal containing $\operatorname{Ann} M$ must equal $\operatorname{Ann} M$ by maximality. So $\operatorname{Supp} M = \{\operatorname{Ann} M\}$. ■

Remark 2.81. We can complete our classification of simple R-modules: for each maximal ideal $\mathfrak{m} \subseteq R$, we can see $R/\mathfrak{m}$ is a simple R-module. Indeed, any R-submodule $M \subseteq R/\mathfrak{m}$ is in fact an $R/\mathfrak{m}$-module, for each $x \in \mathfrak{m}$ and $m \in M$ has $xm = [0]_\mathfrak{m} = 0$. Thus, M is an $(R/\mathfrak{m})$-subspace of $R/\mathfrak{m}$, so for dimension reasons, $M = (0)$ or $M = R/\mathfrak{m}$.

2.2.7 New Supports from Old

Let's see how the support behaves with some of our module constructions. For example, the support behaves well in short exact sequences.

Proposition 2.82. Fix R a ring. Suppose we have a short exact sequence

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

of R-modules. Then $\operatorname{Supp} B = \operatorname{Supp} A \cup \operatorname{Supp} C$.

Proof. The main point is that localization is an exact functor. Namely, if $\mathfrak{p}$ is any prime of R, then we get a short exact sequence

$$0 \to A_\mathfrak{p} \to B_\mathfrak{p} \to C_\mathfrak{p} \to 0.$$

In particular, $A_\mathfrak{p} = C_\mathfrak{p} = 0$ implies $B_\mathfrak{p} = 0$; and conversely, $B_\mathfrak{p} = 0$ implies $A_\mathfrak{p} = C_\mathfrak{p} = 0$. Thus, $B_\mathfrak{p} \neq 0$ if and only if $A_\mathfrak{p} \neq 0$ or $C_\mathfrak{p} \neq 0$, which is exactly the claim that $\operatorname{Supp} B = \operatorname{Supp} A \cup \operatorname{Supp} C$. ■

And here we can see that supports behave with (arbitrary!) direct sums.

Proposition 2.83. Fix R a ring and $\mathcal{M}$ a collection of R-modules. Then

$$\operatorname{Supp} \bigoplus_{M \in \mathcal{M}} M = \bigcup_{M \in \mathcal{M}} \operatorname{Supp} M.$$

Proof. Fix a prime $\mathfrak{p}$. By Proposition 2.51, we see that

$$\left(\bigoplus_{M\in\mathcal{M}} M\right)_{\mathfrak{p}} \cong \bigoplus_{M\in\mathcal{M}} M_{\mathfrak{p}}.$$

In particular, $\left(\bigoplus_{M\in\mathcal{M}} M\right)_{\mathfrak{p}}$ will be nonzero if and only if at least one of the individual $M_{\mathfrak{p}}$ are nonzero. This is exactly the claim. ■

Additionally, we can learn something from the module itself by studying the support.

Proposition 2.84. Fix an R-module M. Then $M = 0$ if and only if $M_{\mathfrak{m}} = 0$ for all maximal ideals $\mathfrak{m} \subseteq R$.

Proof. We have already discussed the forwards direction in Example 2.77. In the other direction, suppose that the R-module M has $M_{\mathfrak{m}} = 0$ for every maximal ideal $\mathfrak{m} \subseteq R$.

Well, pick up any $m \in M$. Then $\operatorname{Ann} m$ is an R-ideal. Using the proof of Proposition 2.74, we see that each maximal ideal $\mathfrak{m}$ has $\operatorname{Ann} m \not\subseteq \mathfrak{m}$, so $\operatorname{Ann} m$ is not contained in any maximal ideal! Thus, we must have

$$\operatorname{Ann} m = R,$$

so $1 \in \operatorname{Ann} m$, so $m = 1m = 0$. So all elements of M are zero, so $M = 0$. ■

Remark 2.85. In fact, the above implies $M = 0$ if and only if $\operatorname{Supp} M = \varnothing$. Indeed, we note that $\operatorname{Supp} M = \varnothing$ will directly imply that $M_{\mathfrak{m}} = 0$ for each maximal ideal $\mathfrak{m}$, from which $M = 0$ follows by the above argument.

In the other direction, if $\operatorname{Supp} M \neq \varnothing$, then there is a prime $\mathfrak{p} \in \operatorname{Supp} M$. Thus, by Proposition 2.74, there is some m so that

$$\operatorname{Ann} m \subseteq \mathfrak{p}.$$

Placing $\mathfrak{p}$ inside a maximal ideal $\mathfrak{m}$, we see $\operatorname{Ann} m \subseteq \mathfrak{m}$, so $M_{\mathfrak{m}} \neq 0$ as well. So indeed, $M \neq 0$.

Corollary 2.86. Fix $\varphi : M \to N$ an R-module homomorphism and $\mathfrak{m} \subseteq R$ a maximal ideal. Then we are promised a localized map $\varphi_{\mathfrak{m}} : M_{\mathfrak{m}} \to N_{\mathfrak{m}}$. Then $\varphi_{\mathfrak{m}}$ is injective/surjective/isomorphic for all maximal ideals $\mathfrak{m}$ if and only if φ is as well.

Proof. The main point is to repeatedly use Corollary 2.54. Note φ is injective if and only if $\ker\varphi = 0$ if and only if $\ker\varphi_{\mathfrak{m}} = (\ker\varphi)_{\mathfrak{m}} = 0$ for all maximal ideals $\mathfrak{m} \subseteq R$ if and only if $\varphi_{\mathfrak{m}}$ is injective for all $\mathfrak{m}$.

Repeating the same argument with coker gives the analogous result for surjectivity. Combining the results for injectivity and surjectivity gives the result for being an isomorphism. This finishes. ■

Remark 2.87 (Nir)**.** Here is an example application. Fix C finitely presented in a short exact sequence

$$0 \to A \to B \stackrel{\pi}{\to} C \to 0. \qquad (*)$$

By Lemma 4.53, this sequence splits if and only if $\operatorname{Hom}_R(C,B) \stackrel{\pi\circ-}{\to} \operatorname{Hom}_R(C,C)$ is surjective if and only if, for each maximal $\mathfrak{p}$, the map $\operatorname{Hom}_R(C,B)_{\mathfrak{p}} \stackrel{\pi\circ-}{\to} \operatorname{Hom}_R(C,C)_{\mathfrak{p}}$ is surjective by Corollary 2.86. Tracking Remark 2.69 through shows this is equivalent to

$$\operatorname{Hom}_{R_{\mathfrak{p}}}(C_{\mathfrak{p}},B_{\mathfrak{p}}) \stackrel{\pi_{\mathfrak{p}}\circ-}{\to} \operatorname{Hom}_{R_{\mathfrak{p}}}(C_{\mathfrak{p}},C_{\mathfrak{p}})$$

being surjective, which is equivalent to $(*)$ splitting locally for each maximal $\mathfrak{p}$ (again, by Lemma 4.53).

We continue our fact-collection.

Proposition 2.88. Fix R a ring and R-modules M and N. Then

$$\operatorname{Supp}(M \otimes_R N) \subseteq \operatorname{Supp} M \cap \operatorname{Supp} N.$$

Proof. We take $\mathfrak{p} \notin \operatorname{Supp} M \cup \operatorname{Supp} N$ and show that $\mathfrak{p} \notin \operatorname{Supp}(M \otimes_R N)$. Without loss of generality, we can actually take $\mathfrak{p} \notin \operatorname{Supp} M$.

Well, we are given that $M_\mathfrak{p} = N_\mathfrak{p} = 0$, so for each $m \in M$, there exists $u \notin \mathfrak{p}$ such that $um = 0$ (using Proposition 2.74). But then each $m \otimes n$ has

$$u \cdot (m \otimes n) = (um) \otimes n = 0,$$

each $m \otimes n$ has some $u_{m\otimes n} \notin \mathfrak{p}$ such that $u(m \otimes n) = 0$. Extending linearly, any element $\sum_{k=1}^n m_k \otimes n_k$ in $M \otimes_R N$ will have

$$u := \prod_{k=1}^n u_{m_k \otimes n_k}$$

with $u \notin \mathfrak{p}$ (because $\mathfrak{p}$ is prime) while

$$u \cdot \sum_{k=1}^n m_k \otimes n_k = \sum_{k=1}^n (um_k) \otimes n_k = 0.$$

So we have indeed checked by Proposition 2.74 that $\mathfrak{p} \notin \operatorname{Supp}(M \otimes_R N)$. ■

Remark 2.89. In fact, in fact, if M and N are finitely generated, then $\operatorname{Supp}(M \otimes_R N) = \operatorname{Supp} M \cap \operatorname{Supp} N$. We do not prove this now because it will require a little more technology; we prove it in Corollary 3.43.

Example 2.90. Consider the $\mathbb{Z}$-modules $\mathbb{Q}$ and $\mathbb{Z}/2\mathbb{Z}$. Note $\mathbb{Q} \otimes_\mathbb{Z} \mathbb{Z}/2\mathbb{Z} = 0$, so

$$\operatorname{Supp}(\mathbb{Q} \otimes_\mathbb{Z} \mathbb{Z}/2\mathbb{Z}) = \varnothing.$$

However, $\mathbb{Q}$ is an integral domain, so $\operatorname{Ann} 1 = (0)$, implying by Proposition 2.74 that $\operatorname{Supp} \mathbb{Q} = \operatorname{Spec} R$. On the other hand, $\operatorname{Ann} \mathbb{Z}/2\mathbb{Z} = (2)$, so Proposition 2.75 gives $\operatorname{Supp} \mathbb{Z}/2\mathbb{Z} = \{(2)\}$. Thus,

$$\operatorname{Supp}(\mathbb{Q} \otimes_\mathbb{Z} \mathbb{Z}/2\mathbb{Z}) = \varnothing \subsetneq \{(2)\} = \operatorname{Supp} \mathbb{Q} \cap \operatorname{Supp} \mathbb{Z}/2\mathbb{Z}.$$

2.2.8 Tensoring Algebras

For the next construction, we note that if S and T are R-algebras, then $S \otimes_R T$ is an R-algebra, where our multiplication is defined by

$$(s_1 \otimes t_1)(s_2 \otimes t_2) = (s_1 s_2) \otimes (t_1 t_2).$$

One can run through the checks that this will be an R-algebra, but because I am actively avoiding proving that anything is a ring, we will not do this here.

We mention this to talk about the tensor product of coordinate rings. Here's a first example.

Exercise 2.91. If we have two free k-algebras $k[x_1, \ldots, x_n]$ and $k[y_1, \ldots, y_m]$, then we claim that

$$k[x_1, \ldots, x_m] \otimes_k k[y_1, \ldots, y_n]$$

is freely generated by the elements of the form $x_\bullet \otimes 1$ and $1 \otimes y_\bullet$; i.e., this is tensor product is a polynomial ring over k with $m + n$ letters.

Proof. Note that any polynomial $f \in k[x_1, \ldots, x_m]$ has a unique representation as

$$f(x_1, \ldots, x_m) = \sum_{d_1, \ldots, d_m = 0}^{\infty} a_{d_1, \ldots, d_m} \left(x_1^{d_1} \cdots x_m^{d_m} \right),$$

where all but finitely many of the a coefficients vanish. In other words, this is really saying that the terms $x_1^{d_1} \cdots x_m^{d_m}$ form a k-basis of $k[x_1, \ldots, x_m]$; similarly, the terms $y_1^{e_1} \cdots y_n^{e_n}$ form a k-basis of $k[y_1, \ldots, y_n]$.

Now, by Example 2.42, it follows that the terms of the form

$$x_1^{d_1} \cdots x_m^{d_m} \otimes y_1^{e_1} \cdots y_n^{e_n}$$

will form a k-basis of $k[x_1, \ldots, x_m] \otimes_k k[y_1, \ldots, y_n]$.

We are now ready to attack the statement directly. Indeed, note that the terms of the form $x_\bullet \otimes 1$ and $1 \otimes y_\bullet$ will indeed generate $k[x_1, \ldots, x_m] \otimes_k k[y_1, \ldots, y_m]$ because we can write

$$x_1^{d_1} \cdots x_m^{d_m} \otimes y_1^{e_1} \cdots y_n^{e_n} = \left(\prod_{i=1}^{m} (x_i \otimes 1)^{d_i} \right) \left(\prod_{j=1}^{n} (1 \otimes y_j)^{e_j} \right),$$

meaning that we can generate any basis element and hence any element by linear combination.

It remains to show that the generation is free. Well, suppose that we can find some algebraic equation

$$\sum_{\substack{d_1, \ldots, d_m \in \mathbb{N} \\ e_1, \ldots, e_n \in \mathbb{N}}} a_{d_1, \ldots, d_m, e_1, \ldots, e_n} \left(\prod_{i=1}^{m} (x_i \otimes 1)^{d_i} \right) \left(\prod_{j=1}^{n} (1 \otimes y_j)^{e_j} \right) = 0,$$

where all but finitely many of the a coefficients vanish. We claim that all the a coefficients must vanish. Indeed, we can expand out the monomials as

$$\sum_{\substack{d_1, \ldots, d_m \in \mathbb{N} \\ e_1, \ldots, e_n \in \mathbb{N}}} a_{d_1, \ldots, d_m, e_1, \ldots, e_n} \left(x_1^{d_1} \cdots x_m^{d_m} \otimes y_1^{e_1} \cdots y_n^{e_n} \right) = 0.$$

However, this means that a k-linear combination of $x_1^{d_1} \cdots x_m^{d_m} \otimes y_1^{e_1} \cdots y_n^{e_n}$ elements is vanishing, so all coefficients must be 0 because we already established that these elements form a basis. ■

Remark 2.92. Geometrically, we can write this as $A\left(\mathbb{A}^n(k)\right) \otimes_k A\left(\mathbb{A}^m(k)\right) \cong A\left(\mathbb{A}^n(k) \times \mathbb{A}^m(k)\right)$, which makes more immediate sense.

As suggested by the remark, in fact the following more general statement is true.

Proposition 2.93. Fix affine algebraic sets X and Y. Then $A(X \times Y) \cong A(X) \otimes_k A(Y)$ canonically as k-algebras.

Proof. A lot of this problem is finding exactly what statement we want to prove. Let $X = Z(I)$ for an ideal $I \subseteq k[x_1, \ldots, x_m]$ and $Y = Z(J)$ for an ideal $J \subseteq k[y_1, \ldots, y_m]$.

We now describe $X \times Y$. We see that $(x, y) \in \mathbb{A}^m(k) \times \mathbb{A}^n(k)$ if and only if $x \in X$ and $y \in Y$ if and only if $f(x) = 0$ for each $f \in I$ and $g(y) = 0$ for each $g \in J$. Embedding the f and g into $k[x_1, \ldots, x_m, y_1, \ldots, y_n] = A\left(\mathbb{A}^m(k) \times \mathbb{A}^n(k)\right)$ in the natural way, we see that $f(x) = f(x, y)$ so that $f(x) = 0$ is equivalent to $f(x, y) = 0$, and $g(x, y) = g(y)$ so that $g(y) = 0$ is equivalent to $g(x, y) = 0$.

Thus, $(x, y) \in X \times Y$ if and only if $f(x, y) = g(x, y) = 0$ for each $f \in I$ and $g \in J$, implying we see that

$$X \times Y = Z(I \cup J).$$

Note that the ideal generated by $I \cup J$ is $(I \cup J) = I + J$. Thus, the claim that $A(X \times Y) \cong A(X) \otimes_k A(Y)$ canonically is the same as saying

$$\frac{k[x_1, \ldots, x_m, y_1, \ldots, y_n]}{I+J} \cong \frac{k[x_1, \ldots, x_m]}{I} \otimes_k \frac{k[y_1, \ldots, y_n]}{J},$$

canonically.

We have now transformed the desired result into an algebra problem. To exhibit the required isomorphism, we provide maps in both directions.

- Note that we can construct a k-bilinear map

$$\psi : \frac{k[x_1, \ldots, x_m]}{I} \times \frac{k[y_1, \ldots, y_n]}{J} \to \frac{k[x_1, \ldots, x_m, y_1, \ldots, y_n]}{I+J}$$

  by $\psi : ([f],[g]) \mapsto [fg]$. We show that ψ is well-defined and k-bilinear separately.

  - Well-defined: if $[f]_I = [f']_I$ and $[g]_J = [g']_J$, then $f - f' \in I$ and $g - g' \in J$. Then

$$(f-f')g, f'(g-g') \in I + J \subseteq k[x_1, \ldots, x_m, y_1, \ldots, y_n],$$

    so $fg - f'g' \in I + J$, so $[fg] = [f'g']$ in $A(X \times Y)$.
  - Bilinear: given $c, c' \in k$ and $[f], [f'] \in A(X)$ and $[g] \in A(Y)$, we find

$$\psi(c[f] + c'[f'], [g]) = \psi([cf + c'f'], [g]) = [(cf + c'f')g] = c[fg] + c'[f'g] = c\psi(f, g) + c'\psi(f', g).$$

    Similarly, given $c, c' \in k$ and $[f] \in A(X)$ and $[g], [g'] \in A(Y)$, we find

$$\psi([f], c[g]+c'[g']) = \psi([f], [cg+c'g']) = [f(cg+c'g')] = c[fg]+c'[fg'] = c\psi([f],[g])+c'\psi([f],[g']).$$

  So ψ is a k-bilinear map and therefore will induce a k-module morphism

$$\overline{\psi} : \frac{k[x_1, \ldots, x_m]}{I} \otimes_k \frac{k[y_1, \ldots, y_n]}{J} \to \frac{k[x_1, \ldots, x_m, y_1, \ldots, y_n]}{I+J}$$

  by $f \otimes g \mapsto fg$.

- We cheat by appealing to Exercise 2.91, which provides a canonical k-algebra isomorphism

$$k[x_1, \ldots, x_m, y_1, \ldots, y_n] \cong k[x_1, \ldots, x_m] \otimes_k k[y_1, \ldots, y_n]$$

  by $x_\bullet \mapsto x_\bullet \otimes 1$ and $y_\bullet \mapsto 1 \otimes y_\bullet$. Now, modding out by I and J in the left and right coordinates, we get a k-algebra morphism

$$\varphi : k[x_1, \ldots, x_m, y_1, \ldots, y_n] \to \frac{k[x_1, \ldots, x_m]}{I} \otimes_k \frac{k[y_1, \ldots, y_n]}{J}.$$

  Further, note that each $f(x, y) \in I$ will go to $f(x) \otimes 1 = 0 \otimes 1$ (using the fact that φ is a k-algebra morphism), so $f \in \ker \varphi$. Similarly, each $g \in J$ has $g \in \ker \varphi$, so $I \cup J \subseteq \ker \varphi$, so $I + J \subseteq \ker \varphi$, so we get an induced k-algebra morphism

$$\overline{\varphi} : \frac{k[x_1, \ldots, x_m, y_1, \ldots, y_n]}{I+J} \to \frac{k[x_1, \ldots, x_m]}{I} \otimes_k \frac{k[y_1, \ldots, y_n]}{J}.$$

Now, we claim that $\overline{\varphi}$ is our desired canonical k-algebra isomorphism. By construction, we know $\overline{\varphi}$ is a k-algebra homomorphism, and because $\overline{\varphi}$ is induced by the projection of an isomorphism, we know $\overline{\varphi}$ is surjective.

Thus, it remains to show that $\overline{\varphi}$ is injective. It suffices to provide $\overline{\varphi}$ with a right inverse, which we claim is $\overline{\psi}$. Namely, we show $\overline{\psi} \circ \overline{\varphi} = \mathrm{id}$. Indeed, we see that, for any $x_\bullet$ and $y_\bullet$,

$$(\overline{\psi} \circ \overline{\varphi})([x_\bullet]) = \overline{\psi}([x_\bullet] \otimes [1]) = [x_\bullet] \qquad \text{and} \qquad (\overline{\psi} \circ \overline{\varphi})([y_\bullet]) = \overline{\psi}([1] \otimes [y_\bullet]) = [y_\bullet],$$

so it follows that $\overline{\psi} \circ \overline{\varphi}$ induces the identity on all of $A(X \times Y)$. This finishes. ■

Remark 2.94 (Nir). I am under the impression that some trickery is required to show that (the more natural map) $\overline{\psi}$ is bijective. At a high level, we can view the above proof as requiring the creation of $\overline{\varphi}$ to prove the bijectivity and $\overline{\psi}$, where the "hard work" of this proof was in the appeal to Exercise 2.91 to show that $\overline{\varphi}$ is well-defined.

Remark 2.95. One can generalize this construction to fiber products.

Next class we will finish up localization by discussing modules of finite length.

2.3 February 1

Hopefully we finish localizing today.

2.3.1 A Little On Tensor Products

Let's start with some review exercises.

Proposition 2.96. Fix R a ring and M an R-module and $I \subseteq R$ an R-ideal. This gives the R-module R/I, and we claim that we have a canonical isomorphism

$$(R/I) \otimes_R M \cong M/IM$$

by $[r]_I \otimes m \mapsto [rm]_{IM}$.

Proof. We will use a few facts about the tensor product here. To start off, we use the short exact sequence

$$0 \to I \to R \to R/I \to 0$$

and then tensor by $\otimes_R M$. This gives the right-exact sequence

$$I \otimes_R M \to R \otimes_R M \to (R/I) \otimes_R M \to 0.$$

We know that $R \otimes_R M \cong M$ (canonically) by $r \otimes m \mapsto rm$, and then tracking the image of $I \otimes_R M$ through the isomorphism $R \otimes_R M \cong M$, we see that

$$I \otimes_R M = \{r \otimes m : r \in R \text{ and } m \in M\} \cong \{rm : r \in I \text{ and } m \in M\} = IM.$$

So we are promised the following commutative diagram with (right) exact rows, where the dashed arrow is induced by the rest of the diagram.

$$\begin{tikzcd} I \otimes_R M \arrow[r] \arrow[d] & R \otimes_R M \arrow[r] \arrow[d] & (R/I) \otimes_R M \arrow[r] \arrow[d, dashed] & 0 \\ IM \arrow[r] & M \arrow[r] & M/IM \arrow[r] & 0 \end{tikzcd}$$

To be explicit, the induced arrow is created by pulling back $(R/I) \otimes_R M$ to $R \otimes_R M$, then pushing forward through to M and then M/IM. Explicitly, we take

$$[r]_I \otimes m \mapsfrom r \otimes m \mapsto rm \mapsto [rm]_{IM}.$$

Being well-defined is by the commutativity and exactness of the diagram: if $r \equiv s \pmod{I}$, then $r \otimes m$ and $s \otimes m$, but $(r-s) \otimes m$ is in the kernel of $R \otimes_R M \to (R/I) \otimes_R M$, so $(r-s)m$ is in the kernel of $M \to M/IM$, so $[rm]_{IM} = [sm]_{IM}$.

The fact that the left two vertical morphisms are isomorphisms forces the rightmost induced morphism to be an isomorphism. Formally, we should replace $I \otimes_R M$ and IM with their images in $R \otimes_R M$ and M to ensure that we have short exact sequences, and then we can finish by applying the snake lemma. ∎

Remark 2.97 (Nir)**.** As usual, this isomorphism is functorial in M in the following sense: if we have $\varphi : M \to N$, then the following diagram commutes.

$$\begin{tikzcd}
(R/I)\otimes_R M \arrow[r, "\varphi"] \arrow[d, "\cong"'] & (R/I)\otimes_R N \arrow[d, "\cong"] \\
M/IM \arrow[r, "\varphi"] & N/IN
\end{tikzcd}$$

Here, the φ arrows are all induced. To see the commutativity, we track $[r]_I \otimes m \mapsto [r]_I \otimes \varphi(n) \mapsto [r\varphi(n)]_{IM}$ along the top, and similarly $[r]_I \otimes m \mapsto [r]_I \otimes \varphi(m) \mapsto [r\varphi(m)]_{IM}$ along the bottom.

Corollary 2.98. Fix R a ring and $I, J \subseteq R$ ideals. Then $(R/I)\otimes_R (R/J) \cong R/(I+J)$.

Proof. From the above we can compute

$$(R/I)\otimes_R (R/J) \cong \frac{R/J}{I(R/J)} = \frac{R/J}{(I+J)/J} \cong \frac{R}{I+J}.$$

Here, $I(R/J) = (I+J)/J$ is set-theoretic: $I(R/J)$ is $\{[x]_J : x \in I\}$, but in fact $[x]_J = [x+y]_J$ for any $y \in J$, so we can write this as $\{[x]_J : x \in I+J\}$. Additionally, $R/(I+J) \cong (R/J)/((I+J)/J)$ is by tracking the kernel of the (surjective) composite $R \twoheadrightarrow R/J \twoheadrightarrow (R/J)/((I+J)/J)$. ■

The above result could be used for fun and profit on the homework.

Remark 2.99. Professor Serganova does not care too much about noncommutative rings in this class.

We also have the following "change of constants" results.

Proposition 2.100. Fix S an R-algebra. Then, given an R-module A as well as S-modules B and C, we have

$$(A \otimes_R B)\otimes_S C \cong A \otimes_R (B \otimes_S C).$$

Proof. The isomorphism is by $(a\otimes b)\otimes c \mapsto a \otimes (b \otimes c)$. Doing this proof rigorously would induce a lot of pain, so we won't bother. ■

Proposition 2.101. Fix S an R-algebra. Then, given R-modules M and N, we have

$$S \otimes_R (M \otimes_R N) \cong (S\otimes_R M)\otimes_S (S \otimes_R N),$$

where $S \otimes_R M$ is given an S-module structure by multiplying the left coordinate.

Proof. The trick is to use associativity in clever ways. Indeed,

$$\begin{aligned}
(S\otimes_R M)\otimes_S (S\otimes_R N) &\cong (M \otimes_R S)\otimes_S (S \otimes_R N) \\
&\overset{*}{\cong} (M \otimes_R (S \otimes_S (S \otimes_R N))) \\
&\overset{*}{\cong} (M \otimes_R ((S \otimes_S S)\otimes_R N)) \\
&\cong (M \otimes_R (S \otimes_R N)),
\end{aligned}$$

which becomes $S \otimes_R (M \otimes_R N)$ after more association. Note we have used Proposition 2.100 (carefully!) on the isomorphisms denoted $\overset{*}{\cong}$. ■

Remark 2.102 (Nir)**.** Tracking through the isomorphism, we see that $(s \otimes m) \otimes (t \otimes n)$ gets sent to $(m \otimes s) \otimes (t \otimes m)$ gets sent to $m \otimes (s \otimes (t \otimes n))$ gets sent to $m \otimes ((s \otimes t) \otimes n)$ gets sent to $m \otimes (st \otimes n)$ gets sent to $st \otimes (m \otimes n)$.

Corollary 2.103. Fix R a ring and $U \subseteq R$ a multiplicatively closed subset. Then, given R-modules M and N, we have

$$(M \otimes_R N)\left[U^{-1}\right] \cong M\left[U^{-1}\right] \otimes_{R[U^{-1}]} N\left[U^{-1}\right].$$

Proof. After noting that $M\left[U^{-1}\right] \cong M \otimes_R R\left[U^{-1}\right]$, we see that we are trying to show

$$(M \otimes_R N) \otimes_R R\left[U^{-1}\right] \cong (M \otimes_R R\left[U^{-1}\right]) \otimes_R \left[U^{-1}\right](N \otimes_R R\left[U^{-1}\right]),$$

which is exactly Proposition 2.101. ■

Remark 2.104 (Nir)**.** Tracking through the isomorphism, we see that $\frac{1}{u}m \otimes \frac{1}{v} \otimes n$ gets sent to $(m \otimes \frac{1}{u}) \otimes (n \otimes \frac{1}{v})$ gets sent to $\frac{1}{uv} \otimes (m \otimes n)$ gets sent to $\frac{1}{uv}(m \otimes n)$.

Remark 2.105 (Nir)**.** Thus, we see that Corollary 2.103 is functorial in M and N. That is, if we have morphisms $\varphi_M : M \to M'$ and $\varphi_N : N \to N'$, the following diagram commutes.

$$\begin{tikzcd}
M\left[U^{-1}\right] \otimes_{R[U^{-1}]} N\left[U^{-1}\right] \arrow[r] \arrow[d] & M'\left[U^{-1}\right] \otimes_{R[U^{-1}]} N'\left[U^{-1}\right] \arrow[d] \\
(M \otimes_R N)\left[U^{-1}\right] \arrow[r] & (M' \otimes_R N')\left[U^{-1}\right]
\end{tikzcd}$$

The vertical arrows are isomorphisms, and the horizontal arrows are induced. To see this commutes, along the top we take $\frac{1}{u}m \otimes \frac{1}{v}n$ to $\frac{1}{u}\varphi_M m \otimes \frac{1}{v}\varphi_N n$ to $\frac{1}{uv}(\varphi_M m \otimes \varphi_N n)$. Then along the bottom we take $\frac{1}{u}m \otimes \frac{1}{v}n$ to $\frac{1}{uv}(m \otimes n)$ to $\frac{1}{uv}(\varphi_M m \otimes \varphi_N n)$, which is the same.

2.3.2 Artinian Rings

We have the following definition, dual to the ascending chain condition for Noetherian modules.

Definition 2.106 (Artinian module)**.** An R-module M is *Artinian* if and only if any descending chain of R-submodules

$$M \supseteq M_1 \supseteq M_2 \supseteq \cdots$$

will stabilize.

Definition 2.107. The ring R is *Artinian* if and only if R is an Artinian as an R-module.

In other words, after recalling that R-submodules of R are ideals, we see that being an Artinian ring is the same as having the descending chain on ideals.

Example 2.108. Fix k a field and $p(x) \in k[x] \setminus \{0\}$. Then $k[x]/p(x)$ is a finite-dimensional k-vector space (in fact, of dimension $\deg p$), which means that it is both Noetherian and Artinian because a chain of k-subspaces can be measured to stabilize by dimension.

Example 2.109. More generally, any finite-dimensional k-algebra is an Artinian ring.

Example 2.110. The ring $\mathbb{Z}/n\mathbb{Z}$ is finite and hence Artinian (and Noetherian).

Observe that all of our examples of Artinian rings are in fact Noetherian. In fact, we will show that all Artinian rings are Noetherian; in the process, we will be able to describe all Artinian rings.

Here is a technical result which we will want to use later; it is dual to the Noetherian case in Proposition 1.50.

Proposition 2.111. Fix a short exact sequence

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

of R-modules. Then B is Artinian if and only if A and C are Artinian.

Proof. We omit this proof; one can essentially copy the proof of the Noetherian case in Proposition 1.50. ■

2.3.3 Composition Series

The main character in our story on Artinian rings will be the "module of finite length."

Definition 2.112 (Composition series)**.** Fix an R-module M. Then a *composition series* (or *Jordan–Hölder series*) is a chain of distinct R-submodules

$$M := M_0 \supsetneq M_1 \supsetneq \cdots \supsetneq M_N := (0)$$

such that each quotient M_i/M_{i+1} is a nonzero simple R-module. The M_i/M_{i+1} are the *composition factors.*

Composition series give rise to the notion of length.

Definition 2.113 (Length)**.** An R-module M with a composition series is said to have *length* n if and only if the shortest composition series (of which there might be many) have n factors.

Definition 2.114 (Finite length)**.** An R-module M is *of finite length* if and only if M has a composition series.

Note that we can already see the Artinian condition playing with being of finite length.

Lemma 2.115. If an R-module M is both Artinian and Noetherian, then M is of finite length.

Proof. If $M = (0)$, we can use the composition series made of only M. Otherwise, because M is Noetherian, the set of all proper ideals will have a maximal element, which we call M_1.

If $M_1 = (0)$, then we have a finite composition series made of $M \supseteq M_0$. Otherwise, observe that M_1 will then be both Artinian and Noetherian (as a submodule of M), so we can repeat the process to get a maximal submodule $M_2 \subsetneq M_1$.

We can continue this process inductively, which gives us the descending chain

$$M \supsetneq M_1 \supsetneq M_2 \supsetneq \cdots,$$

where the quotients are simple modules. But this process must stop eventually because M is Artinian, and the only way to stop is when $M_n = (0)$ for some n, so indeed, this is a composition series. So M is of finite length. ■

Non-Example 2.116. This process does not work when M is not Artinian. For example,

$$\mathbb{Z} \supsetneq 2\mathbb{Z} \supsetneq 4\mathbb{Z} \supsetneq 8\mathbb{Z} \supsetneq \cdots$$

creates an infinite descending chain.

In fact, we can build composition series in short exact sequences, just like how the Noetherian and Artinian conditions build in short exact sequences.

Proposition 2.117. Fix a short exact sequence

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

of R-modules. Then B is of finite length if and only if A and C are of finite length. In fact, the length of B upper-bounds the lengths of A and B, and the length of B is at most the sum of the lengths of A and C.

Proof. We use the embedding $A \hookrightarrow B$ to view A as an R-submodule of B, and we use the projection $B \twoheadrightarrow C$ to view $C \cong B/A$ as a quotient. We now take the directions independently.

- Suppose that B is of finite length; namely, we get a composition series

$$B =: B_0 \supsetneq B_1 \supsetneq \cdots \supsetneq B_{n-1} \supsetneq B_0 := (0).$$

  We have two parts.

  - We show that A has finite length. Indeed, set $A_k := B_k \cap A$ so that we get the descending chain

$$A = A_0 \supseteq A_1 \supseteq \cdots \supseteq A_{n-1} \supseteq A_n = (0).$$

    Now, we can compute the quotients as[3]

$$\frac{A \cap B_k}{A \cap B_{k+1}} \cong \frac{(A \cap B_k) + B_{k+1}}{B_{k+1}},$$

    which we can see is a submodule of the simple module B_k/B_{k+1}. Thus, the quotients A_k/A_{k+1} are either 0 or simple, so after removing the A_k which have $A_k = A_{k+1}$, we will have a composition series of length at most n.
  - We show that C has finite length. Indeed, set $C_k := (B_k + A)/A$ so that we get the descending chain

$$C = C_0 \supseteq C_1 \supseteq \cdots \supseteq C_{n-1} \supseteq C_n = (0).$$

    We can compute the quotients as[4]

$$\frac{(B_k + A)/A}{(B_{k+1} + A)/A} \cong \frac{B_k + A}{B_{k+1} + A}.$$

    But now we note that the map $B_k \hookrightarrow B_k + A \twoheadrightarrow (B_k + A)/(B_{k+1} + A)$ is surjective and has kernel containing B_{k+1}, so there is a surjective map

$$\frac{B_{k+1}}{B_k} \twoheadrightarrow \frac{C_{k+1}}{C_k}.$$

    In particular, this kernel is a submodule of a simple module, so the quotient C_{k+1}/C_k is either B_{k+1}/B_k (and therefore simple) or (0). So, removing the C_k such that $C_k = C_{k+1}$ will remove the (0)s from the composition series will give C a composition series of length at most n.

[3] The kernel of the composition $A \cap B_k \hookrightarrow (A \cap B_k) + B_{k+1} \twoheadrightarrow ((A \cap B_k) + B_{k+1})/B_{k+1}$ is $A \cap B_{k+1}$. The map is surjective because any element of $((A \cap B_k) + B_{k+1})/B_{k+1}$ will have a representative in $A \cap B_k$.

[4] The kernel of the composite of surjective maps $B_k + A \twoheadrightarrow (B_k + A)/A \twoheadrightarrow \frac{(B_k+A)/A}{(B_{k+1}+A)/A}$ is $B_{k+1} + A$.

We remark that the above arguments showed that the length of B upper-bounds the lengths of A and C by constructing a composition series with length at most the length B.

- Suppose that A and C both have finite length. In particular, we can conjure a composition series

$$C =: C_0 \supsetneq C_1 \supsetneq \cdots \supsetneq C_{n-1} \supseteq C_n := (0),$$

and the idea is to pull this back along $\pi : B \twoheadrightarrow C$, setting $B_k := \pi^{-1}(C_k)$. In particular, we will get a descending chain (in fact strictly descending because π is surjective) of submodules

$$B = B_0 \supsetneq B_1 \supsetneq \cdots \supsetneq B_{n-1} \supseteq B_n = A, \tag{$*$}$$

where $B_n = \pi^{-1}((0)) = A$ by exactness. Furthermore, we see that π restricts to a surjection $B_k \to C_k$, and upon modding out the image by C_{k+1}, we see that exactly B_{k+1} will be in the kernel, implying that the quotient

$$\frac{B_k}{B_{k+1}} \cong \frac{C_k}{C_{k+1}}$$

will be simple. So indeed, $(*)$ starts a composition series for B with so far n composition factors.

However, we can then append $(*)$ with the composition series of A, thus providing a composition series for B with length equal to the sum of the lengths of A and C. It follows from the definition that the length of B is at most the sum of the lengths of A and C. ■

Remark 2.118 (Nir)**.** We will show below that the length of a module of finite length is unique among composition series. In this case, the second part of the argument shows that equality holds: the length of B is equal to the sums of the lengths of A and C.

Corollary 2.119. Fix a module M and a chain of submodules

$$M := M_0 \supseteq M_1 \supseteq \cdots \supseteq M_N := (0).$$

If each quotient M_i/M_{i+1} is of finite length, then M is of finite length.

Proof. We induct on N. When $N = 1$, we have $M = M_0/M_1$, so there is nothing to say. Otherwise, by the induction, we may assume that M_1 is of finite length because of the chain of submodules

$$M_1 \supseteq \cdots \supseteq M_N := \{0\}$$

with M_i/M_{i+1} always simple. But now we see we have the short exact sequence

$$0 \to M_1 \to M \to M_0/M_1 \to 0,$$

so because M_1 and M_0/M_1 both have finite length, $M = M_0$ will have finite length. ■

2.3.4 The Jordan–Hölder Theorem

We will now check that the length of a submodule is well-defined. Here is a follow-up result from the argument of Proposition 2.117; we will use it as a technical lemma in the proof.

Lemma 2.120. Fix $A \subsetneq B$ a proper containment of R-modules, and suppose that B has finite length so that A also has finite length. Then the length of A is strictly less than the length of B.

Proof. We will show that, if the lengths of A and B are in fact equal, then $A = B$. As in the argument for Proposition 2.117, fix a composition series

$$B =: B_0 \supsetneq B_1 \supsetneq \cdots \supsetneq B_{n-1} \supsetneq B_0 \coloneqq (0),$$

where n is the length of B. This induces a descending chain

$$A = A_0 \supseteq A_1 \supseteq \cdots \supseteq A_{n-1} \supseteq A_n = (0), \tag{$*$}$$

where $A_k \coloneqq A \cap B_k$. This chain for A would be a composition series, but some composition factors might vanish, and we obtained a composition series for A by removing the equal terms from the series.

However, if the length of A were equal to the length of B, then in the process of removing redundancies from $(*)$ must not do anything at all, for any removed redundancy would imply that the length of A is strictly less than the length of B.

It follows that we have

$$\frac{A_k}{A_{k+1}} = \frac{A \cap B_k}{A \cap B_{k+1}} \cong \frac{(A \cap B_k) + B_{k+1}}{B_{k+1}}$$

is equal to B_k/B_{k+1} for each k. In particular, $(A \cap B_k) + B_{k+1} = B_k$ for each k.

Now, we claim that A contains B_k by inducting downwards on k; this will finish because it will show A contains $B = B_0$ and hence equals B. Now, the statement is true for $k = n$ because $A_n = B_n = (0)$. Then for the inductive step, we know $A \supseteq B_{k+1}$, so it follows

$$B_k = (A \cap B_k) + B_{k+1} \subseteq A$$

as well, finishing. ■

Here is the main result on composition series.

Theorem 2.121 (Jordan–Hölder)**.** Fix M an R-module which has a composition series. Then all composition series of M have the same length. Namely, any strictly descending chain of submodules of M can be refined into a composition series of length equal to the length of M.

Proof. We follow the proof in Eisenbud. Fix M of length n. The key claim is as follows.

Lemma 2.122. Fix M an R-module of length n. If we have a strictly descending chain

$$M = M_0 \supsetneq M_1 \supsetneq M_2 \supsetneq \cdots \supsetneq M_k,$$

then $k \le n$.

Proof. We induct on n. When $n = 0$, the definition of a composition series forces $M = 0$, so our strictly descending chain must consist of only 0, so $k = 0$.

For the inductive step, we note that Lemma 2.120 forces the length of M_1 to be strictly less than the length of M, so the length of M_1 is at most $n-1$. So the inductive hypothesis tells us that the chain

$$M_1 \supsetneq M_2 \supsetneq \cdots \supsetneq M_k$$

forces $k - 1 \ge n - 1$, so $k \ne n$ follows. ■

It follows from Lemma 2.122 that all composition series have length at most n, but because n is the length of the shortest composition series, we see that all composition series must have length exactly n.

As for the second claim, suppose that we have a strictly descending chain

$$M = M_0 \supsetneq M_1 \supsetneq M_2 \supsetneq \cdots \supsetneq M_k.$$

If this is not a composition series, we claim that we can make it longer. Indeed, if some term $M_\ell/M_{\ell+1}$ is not simple, then we can find a proper nonzero submodule $N' \subseteq M_\ell/M_{\ell+1}$, which we can pull back along $M_\ell \twoheadrightarrow M_\ell/M_{\ell+1}$ to a submodule N strictly contained between M_ℓ and $M_{\ell+1}$. In particular, $N' \neq 0$ forces $N \neq M_{\ell+1}$, and $N' \neq M_\ell/M_{\ell+1}$ forces $N \neq M_\ell$.

Thus, we have the strictly descending chain

$$M = M_0 \supsetneq M_1 \supsetneq \cdots \supsetneq M_\ell \supsetneq N \supsetneq M_{\ell+1} \supsetneq \cdots \supsetneq M_k$$

of length $k+1$. We can continue this process as long as we don't have a composition series, but because all composition series have length n, this means that we can only add terms so long as we have length less than n. Namely, we have showed that the all strictly descending chains can be refined to a composition series of length n. ■

2.3.5 Modules of Finite Length

The Jordan–Hölder theorem gives us the following quick result about modules of finite length, which is arguably a classification of modules of finite length. (We will shortly be able to give better descriptions of modules of finite length.)

Corollary 2.123. Fix M an R-module. Then M is of finite length if and only if M is both Artinian and Noetherian.

Proof. The backwards direction is Lemma 2.115.

For the forwards direction, suppose M has a composition series with n composition factors. We show that M is Noetherian and Artinian separately. The point is that Lemma 2.122 basically says that we cannot have arbitrarily long strictly descending or ascending chains.

- We show that M is Noetherian. For this, fix an ascending chain of submodules

  $$N_0 \subseteq N_2 \subseteq N_3 \subseteq \cdots .$$

  Suppose for the sake of contradiction that this ascending chain never stabilizes. Removing equal terms from the chain, we may assume that all the submodules are distinct. But then we can create the descending chain

  $$M \supseteq N_{n+1} \supsetneq N_n \supsetneq N_{n-1} \supsetneq \cdots \supsetneq N_1 \supsetneq N_0$$

  of length $n+1$. This violates Lemma 2.122, which is our contradiction.

- We show that M is Artinian. For this, fix a descending chain of submodules

  $$N_0 \supseteq N_2 \supseteq N_3 \supseteq \cdots .$$

  Suppose for the sake of contradiction that this descending chain never stabilizes. Removing equal terms from the chain, we may assume that all the submodules are distinct. But then we can create the descending chain

  $$M \supseteq N_0 \supsetneq N_1 \supsetneq N_2 \supsetneq \cdots \supsetneq N_n \supsetneq N_{n+1}$$

  of length $n+1$. This violates Lemma 2.122, which is our contradiction. ■

Quickly, note that the support of M is particularly nice when M has a composition series, which essentially comes from various facts we've already proven.

Lemma 2.124. Fix M an R-module with a finite composition series

$$M := M_0 \supsetneq M_1 \supsetneq \cdots \supsetneq M_n := \{0\}.$$

If the composition factors are $R/\mathfrak{p}_k \cong M_{k-1}/M_k$ for $k \in \{1, \ldots, n\}$, then $\operatorname{Supp} M = \{\mathfrak{p}_1, \ldots, \mathfrak{p}_n\}$.

Proof. We induct on the length n of M, using Proposition 2.82 for the induction. If $n = 0$, then the composition series has no composition factors, so $M = 0$ and so $\operatorname{Supp} M = \varnothing$ by Example 2.77, which matches.

For the inductive step, we take $n > 0$ and note that

$$M_1 \supsetneq \cdots \supsetneq M_n = \{0\}$$

provides a composition series for M_1 of length $n-1$, where our composition factors are $R/\mathfrak{p}_k \cong M_{k-1}/M_k$ for $k \in \{2, \ldots, n\}$. So the inductive hypothesis promises

$$\operatorname{Supp} M_1 = \{\mathfrak{p}_2, \ldots, \mathfrak{p}_n\}.$$

Now we use Proposition 2.82. Namely, we have the short exact sequences

$$0 \to M_1 \to M_0 \to M_0/M_1 \to 0$$

which tells us that

$$\operatorname{Supp} M = \operatorname{Supp} M_0 = \operatorname{Supp}(M_0/M_1) \cup \operatorname{Supp} M_1$$

by Proposition 2.82. But $\operatorname{Supp}(M_0/M_1) = \operatorname{Supp} R/\mathfrak{p}_1 = \{\mathfrak{p}_1\}$ by Exercise 2.80. It follows that

$$\operatorname{Supp} M = \{\mathfrak{p}_1, \mathfrak{p}_2, \ldots, \mathfrak{p}_n\},$$

which is what we wanted. ■

And here is a nice result which we get from this.

Theorem 2.125. Fix M an R-module of finite length. Then the following are true.

(a) We can glue the localization maps $M \to M_\mathfrak{p}$ together to form an R-module isomorphism

$$M \cong \bigoplus_{\mathfrak{p} \in \operatorname{Supp} M} M_\mathfrak{p}.$$

(b) The multiplicity of a simple module $R/\mathfrak{m}$ as a composition factor is the length of $M_\mathfrak{p}$ as an $R_\mathfrak{p}$-module.

Proof. We will be very brief. The details are in Eisenbud. Last time we showed that if a morphism $\varphi : M \to N$ induces isomorphisms $\varphi_\mathfrak{m} : M_\mathfrak{m} \to N_\mathfrak{m}$ for each maximal ideal $\mathfrak{m} \subseteq R$, then φ is an isomorphism. Thus, it suffices to show the canonical map

$$\varphi : M \to \bigoplus_{\mathfrak{p} \in \operatorname{Supp} M} M_\mathfrak{p}$$

induces isomorphisms under localization. Namely, localizing by some maximal ideal $\mathfrak{m}$, we get a map

$$\varphi_\mathfrak{m} : M_\mathfrak{m} \to \bigoplus_{\mathfrak{p} \in \operatorname{Supp} M} (M_\mathfrak{p})_\mathfrak{m}.$$

The main point, now, is to compute that

$$(R/\mathfrak{p})_\mathfrak{q} \cong \begin{cases} 0 & \mathfrak{p} \neq \mathfrak{q}, \\ R_\mathfrak{p}/\mathfrak{p}R_\mathfrak{p} & \mathfrak{p} = \mathfrak{q}. \end{cases}$$

For (b), the point is to localize a composition series to get the result, again using the above computation. ■

2.3.6 Artinian Grab-Bag

We are now able to give the following classification.

> **Theorem 2.126.** Fix R a ring. Then R is Artinian if and only if R is Noetherian and all its primes are maximal.

We split the proof into two parts.

Proof of the backwards direction in Theorem 2.126. Suppose R is neither Artinian nor Noetherian. It will suffice to show that not all prime ideals of R are maximal.

Being neither Artinian nor Noetherian conspire to give us an ideal J maximal with respect to the property that R/J is not Artinian: because R is not Artinian, the collection

$$\mathcal{P} := \{\text{ideal } J \subseteq R : R/J \text{ is not Artinian}\}$$

is nonempty (for $(0) \in \mathcal{P}$), and because R is Noetherian, there will be a maximal element, which we call $\mathfrak{p}$. Observe that $\mathfrak{p}$ is not maximal, for then $R/\mathfrak{p}$ would be a field and hence be Artinian.

With this in mind, we claim that $\mathfrak{p}$ must be prime. This will finish because $\mathfrak{p}$ will be a prime which is not maximal. Well, suppose that $a \notin \mathfrak{p}$. Consider the short exact sequence of R-modules

$$0 \to \frac{\mathfrak{p} + (a)}{\mathfrak{p}} \to \frac{R}{\mathfrak{p}} \to \frac{R}{\mathfrak{p} + (a)} \to 0.$$

We are going to profit from studying this short exact sequence by using Proposition 2.111. In particular, $R/\mathfrak{p}$ is not Artinian, so we cannot have both R-modules on its left and right be Artinian.

Well, $\mathfrak{p} \subsetneq \mathfrak{p} + (a)$, so by maximality, $R/(\mathfrak{p} + (a))$ will have to be Artinian. So instead $(\mathfrak{p} + (a))/\mathfrak{p}$ cannot be Artinian. But now we observe that we have the following isomorphism of R-modules.

> **Lemma 2.127.** Fix R a ring and $I \subseteq R$ an ideal and $a \in R$. Then we define $(I : a) := \{r \in R : ar \in I\}$, and we claim that $(I : a)$ is an ideal and
>
> $$\frac{R}{(I : a)} \cong \frac{I + (a)}{I}.$$

Proof. Note that there is an R-module map $\varphi : R \to (a) + I$ by

$$\varphi : x \mapsto ax.$$

Indeed, $\varphi(r_1x_1 + r_2x_2) = ar_1x_1 + ar_2x_2 = r_1\varphi(x_1) + r_2\varphi(x_2)$. Now, modding out the image by $I \subseteq (a) + I$, we get a map

$$\widetilde{\varphi} : R \to \frac{(a) + I}{I}.$$

We note that this map is surjective because any coset $[x]_I$ with $x \in (a) + I$ can have $x = ar + p$ where $r \in R$ and $p \in I$, meaning that $\widetilde{\varphi}(r) = [ar]_I = [x]_I$. Further, we can compute the kernel of $\widetilde{\varphi}$ as

$$\{r \in R : ar \in I\} = (I : a).$$

Thus, $(I : a) = \ker \widetilde{\varphi}$ is an ideal, and $\widetilde{\varphi}$ induces an isomorphism $R/(I : a) \to (I + (a))/I$, finishing. ■

Now, because $(\mathfrak{p} + (a))/\mathfrak{p}$ is not Artinian, we see $R/(\mathfrak{p} : a)$ cannot be Artinian. But certainly $\mathfrak{p} \subseteq (\mathfrak{p} : a)$ because each $x \in \mathfrak{p}$ has $ax \in \mathfrak{p}$, so we must have

$$\mathfrak{p} = (\mathfrak{p} : a)$$

by the maximality of $\mathfrak{p}$. We now finish the proof. Suppose now that $ab \in \mathfrak{p}$, and we claim that $b \in \mathfrak{p}$. Well, $ab \in \mathfrak{p}$ implies that $b \in (\mathfrak{p} : a) = \mathfrak{p}$. So we are done. ■

Proof of the forwards direction of Theorem 2.126. For the other direction, we note that we can show all primes are maximal without tears.

Lemma 2.128. Fix R an Artinian ring. Then any prime ideal $\mathfrak{p} \subseteq R$ is maximal.

Proof. We follow the argument given here. Well, given $\mathfrak{p}$ a prime so that $R/\mathfrak{p}$ is an integral domain, we show that $R/\mathfrak{p}$ is actually a field. Well, we can pick up $[x]_\mathfrak{p} \neq 0$ represented by some $x \notin \mathfrak{p}$, and we show that $[x]_\mathfrak{p}$ is a unit. Note that we have the descending chain

$$(x) \supseteq \left(x^2\right) \supseteq \left(x^3\right) \supseteq \cdots,$$

which must eventually stabilize, so there is some $n \in \mathbb{N}$ such that $(x^n) = \left(x^{n+1}\right)$, so there is $r \in R$ with $x^n = rx^{n+1}$. In particular,

$$x^n(1 - xr) = 0.$$

Working in $R/\mathfrak{p}$, we see that $[x]_\mathfrak{p} \neq 0$, so the fact that $R/\mathfrak{p}$ is an integral domain implies that

$$[x]_\mathfrak{p} \cdot [r]_\mathfrak{p} = 1,$$

so indeed, $[x]_\mathfrak{p}$ is a unit. ■

So it remains to show that R is Artinian implies that R is Noetherian. We introduce the following definition.

Definition 2.129 (Jacobson radical)**.** Fix R a ring. Then we define the *Jacobson radical* $J \subseteq R$ to be

$$J := \bigcap_{\mathfrak{m}} \mathfrak{m},$$

where $\mathfrak{m}$ ranges over all maximal ideals of R.

Note that the Jacobson radical is an ideal because ideals are closed under intersection. Alternatively, we can view J as the kernel of the map

$$R \to \prod_{\mathfrak{m}} R/\mathfrak{m},$$

for any ring R, where the product is over maximal ideals $\mathfrak{m} \subseteq R$.

In fact, in the case where R is Artinian, the above map will be surjective. By the Chinese remainder theorem, it suffices to show that there are only finitely many maximal ideals of R.

Lemma 2.130. Fix R an Artinian ring. Then R has only finitely many maximal ideals.

Proof. We follow the argument from here because I think it is pretty close to what I understand Professor Serganova saying in class.

The point here is that infinitely many maximal ideals will induce an infinite composition series. Indeed, suppose that we have some infinite collection $\{\mathfrak{m}_k\}_{k=1}^\infty$ of maximal ideals, and we claim that the chain

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

is an infinite composition series; this will verify that R is not Artinian.

But now, this chain is infinite, and to see that it is a composition series, we have to check that

$$\frac{\mathfrak{m}_1 \cap \cdots \cap \mathfrak{m}_k}{\mathfrak{m}_1 \cap \cdots \cap \mathfrak{m}_k \cap \mathfrak{m}_{k+1}}$$

is simple for each $k \geq 1$. Indeed, note that we have the following commutative diagram with exact rows, where the vertical morphisms are isomorphisms given by the Chinese remainder theorem.

$$\begin{tikzcd}
0 \arrow[r] & \dfrac{\mathfrak{m}_1 \cap \cdots \cap \mathfrak{m}_n}{\mathfrak{m}_1 \cap \cdots \cap \mathfrak{m}_n \cap \mathfrak{m}_{n+1}} \arrow[r] & \dfrac{R}{\mathfrak{m}_1 \cap \cdots \cap \mathfrak{m}_n \cap \mathfrak{m}_{n+1}} \arrow[r] \arrow[d] & \dfrac{R}{\mathfrak{m}_1 \cap \cdots \cap \mathfrak{m}_n} \arrow[r] \arrow[d] & 0 \\
0 \arrow[r] & R/\mathfrak{m}_{n+1} \arrow[r] & \displaystyle\bigoplus_{k=1}^{n+1} R/\mathfrak{m}_k \arrow[r] & \displaystyle\bigoplus_{k=1}^{n} R/\mathfrak{m}_k \arrow[r] & 0
\end{tikzcd}$$

In particular, the square commutes because $[r]_{\mathfrak{m}_1 \cap \cdots \mathfrak{m}_n \cap \mathfrak{m}_{n+1}}$ in the top-left will go to $([r]_{\mathfrak{m}_1}, \ldots, [r]_{\mathfrak{m}_n})$ in the bottom-right, no matter which we path we choose. Thus, there is an induced isomorphism

$$\frac{\mathfrak{m}_1 \cap \cdots \cap \mathfrak{m}_n}{\mathfrak{m}_1 \cap \cdots \cap \mathfrak{m}_n \cap \mathfrak{m}_{n+1}} \cong \frac{R}{\mathfrak{m}_{n+1}},$$

so indeed this R-module is simple, say by Remark 2.81. ■

Remark 2.131. Intuitively, there can only be finitely many maximal ideals $\mathfrak{m}$ because each $R/\mathfrak{m}$ will induce a composition factor, of which there are only finitely many because R is Artinian. In the above proof, we have actually shown how to induce such a composition series using each of these composition factors.

Remark 2.132 (Nir). In fact, an Artinian ring will have only finitely many prime ideals, which we can see directly because all primes are maximal.

We now proceed with the proof of Theorem 2.126. The main idea is to try to make Lemma 2.130 sharp by using the descending chain of submodules

$$R \supsetneq \mathfrak{m}_1 \supsetneq \mathfrak{m}_1 \cap \mathfrak{m}_2 \supsetneq \cdots \supsetneq \bigcap_{k=1}^{r} \mathfrak{m}_k,$$

where $\{\mathfrak{m}_k\}_{k=1}^r$ are our maximal ideals. However, it turns out that this descending chain may and can simply bottom out at the Jacobson radical J, which might be nonzero, and so we will not get an actual composition series. But at least we can (again) hope that J is "small enough" so that continue this sequence somehow.

Remark 2.133 (Serganova). Here is alternate motivation for the below claim: the payoff to Lemma 2.130 is that the Chinese remainder theorem gives us right-exactness of the short exact sequence

$$0 \to J \to R \to \prod_{\mathfrak{m}} R/\mathfrak{m} \to 0.$$

In particular,

$$R/J \cong \prod_{\mathfrak{m}} R/\mathfrak{m}$$

is a product of finitely many simple modules $R/\mathfrak{m}$, so R/J will be of finite length. (Note R/J has only finitely many ideals because each $R/\mathfrak{m}$ has only two ideals.) We would like to turn the fact that R/J is of finite length into the fact that R is of finite length, but we will need a smallness condition on J to make this work.

The key claim is as follows.

Lemma 2.134. Fix R an Artinian ring. Then the Jacobson radical J is nilpotent.

Proof. Observe that we have a descending chain

$$J \supseteq J^2 \supseteq J^3 \supseteq \cdots,$$

which stabilizes because R is Artinian. So suppose that $J^N = J^{N+1} = I$ for some $N \geq 1$, and we hope $I = (0)$. By the stabilization, we see $I^2 = J^{2N} = J^N = I$.

Now, if $I \neq (0)$, then we can find a minimal ideal $K \subseteq I$ such that $IK \neq (0)$ and $K \neq (0)$. (Note that $I = K$ would work—$I^2 = I \neq (0)$—but is perhaps not minimal; we need the Artinian condition to get the minimal such ideal.) We start with some fact-collection on K. Note that $I(IK) = I^2K = IK \neq (0)$ and $IK \neq (0)$ while $IK \subseteq K$, so K's minimality forces

$$IK = K.$$

Furthermore, because $K \neq (0)$, there exists $a \in K \setminus \{(0)\}$ such that $aI \neq (0)$. So $(a)I \neq (0)$ while $(a) \neq 0$, so $(a) \subseteq K$ combined with K's minimality (again) forces

$$K = (a).$$

Combining the above two facts, we are granted $b \in I$ such that $ba = a$.

But here is the key trick: we can write $ba = a$ as

$$a(1 - b) = 0.$$

However, $b \in I$ implies $b \in J$ implies $1 - b \notin J$, so $(1 - b)$ is not in any maximal ideal. So it follows $(1 - b) = R$, so $1 - b \in R^\times$! Upon cancelling, we see $K = (a) = 0$, which is our contradiction. ■

We now return to the proof. We claim that R is of finite length, which will imply that R is Noetherian. Instead of using intersections of maximal ideals as in Lemma 2.130, our salvage will use products of maximal ideals, which grant us enough flexibility.

Indeed, the main obstruction is verifying that some finite product of maximal ideals will actually vanish. But if, say, $J^N = (0)$ where $J \subseteq R$ is our Jacobson radical, then

$$(\mathfrak{m}_1 \cdots \mathfrak{m}_r)^N \subseteq \left(\bigcap_{k=1}^n \mathfrak{m}_k \right)^N = J^N = (0).$$

So some finite product of maximal ideals will vanish; for the sake of not mixing up our letters, let $\{\mathfrak{p}\}_{k=1}^n$ be a sequence of (not necessarily distinct) maximal ideals so that $\mathfrak{p}_1 \cdots \mathfrak{p}_n = (0)$. Then we work with the chain

$$R \supseteq \mathfrak{p}_1 \supseteq \mathfrak{p}_1\mathfrak{p}_2 \supseteq \cdots \supseteq \mathfrak{p}_1\mathfrak{p}_2 \cdots \mathfrak{p}_{n-1} \supseteq \mathfrak{p}_1\mathfrak{p}_2 \cdots \mathfrak{p}_n = (0).$$

By Corollary 2.119, it suffices to check that each quotient

$$M_k := \frac{\mathfrak{p}_1 \cdots \mathfrak{p}_k}{\mathfrak{p}_1 \cdots \mathfrak{p}_{k+1}}$$

is of finite length, for each $k \geq 0$. (When $k = 0$, the empty product gives R.) Now, M_k is an R-module, but note that the $\mathfrak{p}_{k+1}$-action kills an element, so in fact the ring morphism $R \to \operatorname{End}(M_k)$ descends to a ring morphism $R/\mathfrak{p}_{k+1} \to \operatorname{End}(M_k)$.

This is to say that M_k is an $R/\mathfrak{p}_{k+1}$-vector space. To show that M_k is of finite length, we need to know that M_k is finite-dimensional. Well, if M_k were not finite-dimensional, then an infinite basis would provide an infinitely descending chain of $R/\mathfrak{p}_{k+1}$-submodules

$$\frac{\mathfrak{p}_1 \cdots \mathfrak{p}_k}{\mathfrak{p}_1 \cdots \mathfrak{p}_{k+1}} \supsetneq \frac{N_1}{\mathfrak{p}_1 \cdots \mathfrak{p}_{k+1}} \supsetneq \frac{N_1}{\mathfrak{p}_1 \cdots \mathfrak{p}_{k+1}} \supsetneq \cdots.$$

Taking the pre-images of $R \to R/\mathfrak{p}_1 \cdots \mathfrak{p}_{k+1}$, this lifts to an infinite descending chain

$$\mathfrak{p}_1 \cdots \mathfrak{p}_k \supsetneq N_1 + \mathfrak{p}_1 \cdots \mathfrak{p}_{k+1} \supsetneq N_2 + \mathfrak{p}_1 \cdots \mathfrak{p}_{k+1} \supsetneq \cdots,$$

which violates the condition that R is Artinian.[5] This finishes. ■

Remark 2.135 (Miles). Here is an alternate finish after Lemma 2.134. The point is to extend the unfinished composition series

$$R \supseteq \mathfrak{m}_1 \supseteq \mathfrak{m}_1 \cap \mathfrak{m}_2 \supseteq \cdots \supseteq J$$

by $J \supseteq J^2 \supseteq \cdots \supseteq J^N = (0)$. Namely, it remains to check that J^k/J^{k+1} has finite length. Well, we use Proposition 2.96 and Remark 2.133 to write

$$\frac{J^k}{J^{k+1}} = \frac{(J^k)}{J\,(J^k)} \cong J^k \otimes_R \frac{R}{J} \cong J^k \otimes_R \bigoplus_{\mathfrak{m}} R/\mathfrak{m} \cong \bigoplus_{\mathfrak{m}} \left(J^k \otimes_R R/\mathfrak{m}\right).$$

So to finish, we need to show $J^k \otimes_R R/\mathfrak{m}$ has finite length, for which it suffices to show $\mathfrak{m} \otimes_R R/\mathfrak{m}$ has finite length. But by Proposition 2.96, $\mathfrak{m} \otimes_R R/\mathfrak{m} \cong \mathfrak{m}/\mathfrak{m}^2$, which is a finite-dimensional $R/\mathfrak{m}$-vector space (when R is Artinian!) as discussed at the end of the above proof.

2.3.7 Geometry of Artinian Rings

While we're here, we provide some more nice facts.

Proposition 2.136. Any Artinian ring is a product of local Artinian rings.

Proof. This essentially comes down to modules of finite length being products of localizations over their support. ■

We can even give a geometric view to what we are doing.

Proposition 2.137. Fix $I \subseteq k[x_1, \ldots, x_n]$. Then the following are equivalent.

(a) The ring $R := k[x_1, \ldots, x_n]/I$ is Artinian.

(b) The set $Z(I) \subseteq \mathbb{A}^n(k)$ is finite.

(c) The ring R is a finite-dimensional k-algebra.

Proof. We follow Eisenbud. We take our implications in sequence.

- We show (a) implies (b). Suppose that the ring $R := k[x_1, \ldots, x_n]/I$ is Artinian. Then R has finitely many maximal ideals by Lemma 2.130, which are in bijection to points in $Z(I)$, so $Z(I)$ is finite.
- We show (b) implies (c). Suppose that $Z(I)$ is finite. Then $R = k[x_1, \ldots, x_n]/I$ is in bijection with k-valued (polynomial) functions on $Z(I)$, but as $Z(I)$ is finite, we can build any function as a polynomial function by (say) Lagrange interpolation.

  Rigorously, two polynomials $f, g \in k[x_1, \ldots, x_n]$ has $[f]_I = [g]_I$ if and only if $[f - g]_I = [0]_I$ if and only if $f - g \in I$ if and only if $f - g$ vanishes on $Z(I)$ if and only if f and g agree on $Z(I)$. So $[f]_I$ can indeed be viewed as a function on $Z(I)$.

  Thus, R is in bijection with k-valued functions on finitely many points, but this space is simply $k^{Z(I)}$, which is a finite-dimensional vector space. Adding in the ring structure to R makes R into a finite-dimensional k-algebra.

[5] Technically we ought to check that these submodules are distinct. This is because the projection map $\varphi : R \to R/\mathfrak{p}_1 \cdots \mathfrak{p}_{k+1}$ is surjective, so the pre-image of distinct sets will remain distinct.

- We show (c) implies (a). Indeed, any strictly descending chain of submodules of a finite-dimensional k-vector space must terminate, so R is Artinian as a k-vector space. Any R-submodule of R will also be a k-vector space, so we see that any strictly descending chain of R-submodules of R must terminate as well. Thus, R is Artinian. ■

2.3.8 The Radical, Returned

And we end our discussion with the following miscellaneous result.

Proposition 2.138. Fix an ideal $I \subseteq R$. Then

$$\operatorname{rad} I = \bigcap_{I \subseteq \mathfrak{p}} \mathfrak{p},$$

where $\mathfrak{p}$ ranges over all prime ideals containing I.

Proof. The main point is the following lemma.

Lemma 2.139. Fix R a ring and $I \subseteq R$ an ideal and $U \subseteq R$ a multiplicatively closed subset such that $I \cap U = \varnothing$. Suppose $\mathfrak{p}$ is maximal in the set of ideals satisfying $\mathfrak{p} \cap U = \varnothing$ and $I \subseteq \mathfrak{p}$. Then $\mathfrak{p}$ is prime.

Before proving the lemma, we note that, under the hypotheses of the problem, such a maximal ideal $\mathfrak{p}$ will exist, which we can conjure by Zorn's lemma from the set of all ideals satisfying $\mathfrak{p} \cap U = \varnothing$ and $I \subseteq \mathfrak{p}$.[6]

Proof. Suppose that $a, b \notin \mathfrak{p}$, and it suffices to show that $ab \notin \mathfrak{p}$. Well, $(a) + \mathfrak{p}$ and $(b) + \mathfrak{p}$ are both strictly larger than $\mathfrak{p}$ while containing $I \subseteq \mathfrak{p}$, so they must intersect U. Suppose $u \in ((a)+\mathfrak{p}) \cap U$ and $v \in ((b)+\mathfrak{p}) \cap U$. Then

$$uv \in ((a) + \mathfrak{p})((b) + \mathfrak{p}) = (ab) + (a)\mathfrak{p} + (b)\mathfrak{p} + \mathfrak{p}^2 \subseteq (ab) + \mathfrak{p}.$$

Thus, $(ab)+\mathfrak{p}$ intersects U at $uv \in U$, so it follows $\mathfrak{p} \neq (ab)+\mathfrak{p}$ because $\mathfrak{p} \cap U = \varnothing$. Thus, $ab \notin \mathfrak{p}$, finishing. ■

We now attack the proposition directly. In one direction, suppose that $a \in \operatorname{rad} I$ so that $a^n \in I$ for some $n \in \mathbb{N}$. Then for any prime $\mathfrak{p}$ containing I, we have $a^n \in \mathfrak{p}$, so $a \in \mathfrak{p}$ by primality of $\mathfrak{p}$. It follows

$$\operatorname{rad} I \subseteq \bigcap_{I \subseteq \mathfrak{p}} \mathfrak{p}.$$

The other inclusion requires the lemma. Suppose that $a \notin \operatorname{rad} I$, and we will find a prime $\mathfrak{p} \supseteq I$ such that $a \notin \mathfrak{p}$. Indeed, we pick up an ideal $\mathfrak{p}$ containing I which is maximal avoiding the set

$$\langle a \rangle := \{a^n : n \in \mathbb{N}\}.$$

In particular, such an ideal $\mathfrak{p}$ by the discussion preceding the lemma, and it is prime by the lemma. But $a \notin \mathfrak{p}$ while $I \subseteq \mathfrak{p}$, so it follows that

$$a \notin \bigcap_{I \subseteq \mathfrak{p}} \mathfrak{p},$$

finishing. ■

Corollary 2.140. Fix R a ring. Then $r \in R$ is nilpotent if and only if $r \in \mathfrak{p}$ for each prime ideal $\mathfrak{p} \subseteq R$.

Proof. The set of nilpotent elements in R is

$$\operatorname{rad}(0) = \{r \in R : r^n = 0 \text{ for some } n \in \mathbb{N}\}.$$

By Proposition 2.138, this will be the intersection of all prime ideals of R. In other words, an element $r \in R$ is nilpotent if and only if $r \in \mathfrak{p}$ for all primes $\mathfrak{p}$, which is what we wanted. ■

[6] This set is nonempty because $I \cap U = \varnothing$ and $I \subseteq I$. All ascending chains have an upper bound by taking the union along the chain.

2.4 February 3

Today we are talking associated primes.

2.4.1 Associated Primes

Fix M an R-module. Then given $m \in M$, recall that we can look at

$$\operatorname{Ann} m = \{r \in R : rm = 0\}.$$

Observe that $m \neq 0$ promises $\operatorname{Ann} m \neq R$ because $1_R m \neq 0$. In particular, these ideals are proper most of the time.

It will turn out to be productive to give require some structure out of these annihilators.

Definition 2.141 (Associated primes). Fix M an R-module. Then a prime ideal $\mathfrak{p} \in \operatorname{Spec} R$ is *associated to* M if and only if $\mathfrak{p} = \operatorname{Ann} m$ for some $m \in M$. We denote $\operatorname{Ass} M \subseteq \operatorname{Spec} R$ to be the set of all associated primes to M.

As usual, let's see some examples.

Example 2.142. We have that $\operatorname{Ass}(0) = \varnothing$ because the annihilator of any element in (0) is R (because all elements are 0), which is not a prime ideal.

Exercise 2.143. Let n be a nonzero integer. Fix $M := \mathbb{Z}/n\mathbb{Z}$ as a $\mathbb{Z}$-module. Then $\operatorname{Ass} M = \{(p) :$ prime $p \mid n\}$.

Proof. Let (p) be a prime. Then (p) is associated to M if and only if there exists some $m \in M$ such that

$$\operatorname{Ann} m = (p).$$

If $p \mid n$, then we note that $\operatorname{Ann} \left[\frac{n}{p}\right]_n = (p)$ because $n \mid \frac{n}{p} \cdot k$ if and only if $p \mid k$. Thus, $\{(p) : \text{prime } p \mid n\} \subseteq \operatorname{Ass} M$.

Conversely, if $\operatorname{Ann} m =: (p)$ is prime, then we see that we have a $\mathbb{Z}$-module map $\varphi : \mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ by $r \mapsto rm$, which has kernel $\operatorname{Ann} m = (p)$. Namely, we have an injection

$$\mathbb{Z}/p\mathbb{Z} \hookrightarrow \mathbb{Z}/n\mathbb{Z},$$

so $p \mid n$ by Lagrange's theorem on groups. ■

We can generalize the trick at the end of the proof to give the following characterization of associated primes; this characterization will be easier to use for more element-free proofs.

Lemma 2.144. Fix M an R-module. Then a prime $\mathfrak{p} \in \operatorname{Spec} R$ is associated to M if and only if there is an injective R-module homomorphism $R/\mathfrak{p} \hookrightarrow M$. In fact, if $\mathfrak{p} = \operatorname{Ass} m$, then the injection provides an isomorphism $R/\mathfrak{p} \to Rm$.

Proof. We take the directions separately.

- Suppose that $\mathfrak{p}$ is associated to M. Then there exists $m \in M$ such that $\mathfrak{p} = \operatorname{Ann} m$, so we consider the map $\varphi : R \to M$ by

$$\varphi : r \mapsto rm$$

If $r_1, r_2 \in R$ and $x_1, x_2 \in R$, then $\varphi(r_1x_1 + r_2x_2) = r_1x_1m + r_2x_2m = r_1\varphi(x_1) + r_2\varphi(x_2)$, so φ is indeed an R-linear map. Then, by definition of $\operatorname{Ann} m$ we see that $\mathfrak{p} = \operatorname{Ann} m = \ker\varphi$, so there is an induced injection

$$\overline{\varphi} : R/\mathfrak{p} \hookrightarrow M,$$

which is what we wanted.

To finish, we note that φ is surjective onto Rm, so $\varphi : R/\mathfrak{p} \to Rm$ is an isomorphism.

- Suppose that there is an embedding $\varphi : R/\mathfrak{p} \hookrightarrow M$. Then define $m := \varphi([1]_\mathfrak{p})$. Now, $rm = 0$ if and only if $r\varphi([1]_\mathfrak{p}) = \varphi([r]_\mathfrak{p})$ is equal to $0 = \varphi([0]_\mathfrak{p})$, so $rm = 0$ is equivalent to $r \in \mathfrak{p}$. Thus, $\operatorname{Ann} m = \mathfrak{p}$, as desired.

  Lastly, we note φ is again surjective onto Rm, so $\varphi : R/\mathfrak{p} \to Rm$ is an isomorphism. ■

Remark 2.145 (Nir). The embedding

$$\frac{\mathbb{Q}[x]}{(x-2)} \cong \mathbb{Q} \cong \frac{\mathbb{Q}[x]}{(x)}$$

does not mean that $(x-2)$ is an associated prime of $\mathbb{Q}[x]/(x)$ because the above embedding is of $\mathbb{Q}$-modules, not $\mathbb{Q}[x]$-modules. Explicitly, $[x]_{(x-2)}$ goes to 2 goes to $[2]_{(x)}$, but $x \cdot [1]_{(x-2)}$ goes to $x \cdot 1$ goes to $x \cdot [1]_{(x)} = [0]_{(x)}$.

We close our introduction with another example.

Example 2.146. Fix $\mathfrak{p} \subseteq R$ a prime ideal and fix $M := R/\mathfrak{p}$. Certainly $\mathfrak{p} \in \operatorname{Ass} M$ because $\operatorname{Ann}[1]_\mathfrak{p} = \mathfrak{p}$. (Alternatively, use Lemma 2.144 and note $R/\mathfrak{p} \hookrightarrow R/\mathfrak{p} = M$.) Conversely, fix some $b \in R \setminus \mathfrak{p}$, and we want to know what primes can arise as

$$\operatorname{Ann}([b]_\mathfrak{p}) = \{a \in R : ab \in \mathfrak{p}\}.$$

But with $b \notin \mathfrak{p}$, the primality of $\mathfrak{p}$ means that $ab \in \mathfrak{p}$ implies $a \in \mathfrak{p}$. (And conversely, $a \in \mathfrak{p}$ implies $ab \in \mathfrak{p}$.) So $\operatorname{Ann}([b]_\mathfrak{p}) = \mathfrak{p}$ for any $b \notin \mathfrak{p}$, so $\operatorname{Ass} M = \{\mathfrak{p}\}$.

So indeed, any prime of R can arise as an associated prime.

2.4.2 Associated Primes in Localization

In the spirit of the above example, we have the following proposition.

Proposition 2.147. Fix M an R-module. Suppose $\mathfrak{p} \subseteq R$ is an ideal maximal in

$$\mathcal{P} := \{\operatorname{Ann} m : m \in M \setminus \{0\}\}.$$

Then we claim $\mathfrak{p}$ is prime.

Proof. Now take $ab \in \mathfrak{p}$ and $a \notin \mathfrak{p}$, and we show that $b \in \mathfrak{p}$. Well, $ab \in \mathfrak{p}$ implies that $a(bm) = (ab)m = 0$, so $a \in \operatorname{Ann} bm$. But certainly any $x \in \mathfrak{p}$ will have

$$x(bm) = b(xm) = 0,$$

so $x \in \operatorname{Ann} bm$, so $\mathfrak{p} \subseteq \operatorname{Ann} bm$. However, we now see that $\operatorname{Ann} bm$ is an annihilator strictly containing $\mathfrak{p}$ (because $a \in \operatorname{Ann} bm \setminus \mathfrak{p}$). This looks like a contradiction, but it is not: instead we merely must have $bm = 0$, which means $b \in \mathfrak{p}$. ■

We have the following corollary.

Corollary 2.148. Fix R a Noetherian ring and M a nonzero R-module. Then $\operatorname{Ass} M$ is nonempty.

Proof. As in Proposition 2.147, set

$$\mathcal{P} := \{\operatorname{Ann} m : m \in M \setminus \{0\}\}.$$

Because R is Noetherian, $\mathcal{P}$ will contain a maximal element, which will be a prime $\mathfrak{p} = \operatorname{Ann} m$ for some $m \in M$. So $\mathfrak{p} \in \operatorname{Ass} M$, meaning $\operatorname{Ass} M \neq \varnothing$. ■

Remark 2.149 (Nir)**.** It is possible to have a nonzero module with no associated primes; we follow the example given in sx2931719. Consider $R := C(\mathbb{R}, \mathbb{R})$ the ring of continuous functions $\mathbb{R} \to \mathbb{R}$ as a module over itself. Fix any $f \in R \setminus \{0\}$, and we show $\operatorname{Ann} f$ is not prime.

Because $f \neq 0$, find $a \in \mathbb{R}$ such that $f(a) \neq 0$, and by continuity some $b > a$ close to a also has $f(b) \neq 0$. (Here we use continuity of f.) Then set $m := \frac{a+b}{2}$ and

$$g(x) = \begin{cases} (x-m)^2 & x \leq m, \\ 0 & x \geq m, \end{cases} \qquad \text{and} \qquad h(x) = \begin{cases} 0 & x \leq m, \\ (x-m)^2 & x \geq m. \end{cases}$$

Then $g, h \in C(\mathbb{R}, \mathbb{R})$ and $gh = 0 \in \operatorname{Ann} f$. However, $(gf)(a) \neq 0$ an $(hf)(b) \neq 0$, so $g, h \notin \operatorname{Ann} f$.

Remark 2.150. For the sake of comparison, let's compare $\operatorname{Supp} M$ with $\operatorname{Ass} M$. For example, when R is a domain, then $\operatorname{Ass}_R R = \{(0)\}$ by the integral domain condition. However, the support $\operatorname{Supp} R = \operatorname{Spec} R$, so the associated primes appear smaller.

More generally, for R any ring, if $\mathfrak{p} \in \operatorname{Ass} M$, then set $\mathfrak{p} = \operatorname{Ann} m$. Thus, in $M_\mathfrak{p}$, we have $\frac{m}{1} \neq \frac{0}{1}$, for this would imply there is $u \in R \setminus \mathfrak{p}$ such that $um = 0$, which cannot be because $\operatorname{Ann} m \subseteq \mathfrak{p}$. It follows $M_\mathfrak{p} \neq 0$, so $\mathfrak{p} \in \operatorname{Supp} M$. We conclude $\operatorname{Ass} M \subseteq \operatorname{Supp} M$.

Indeed, we will find that the associated primes will be smaller than $\operatorname{Supp} M$.

Localization was able to tell us about maps by looking locally everywhere: an element was 0 if and only if zero on all localizations. However, it turns out that we can limit what we have to focus on.

Proposition 2.151. Fix R Noetherian and M an R-module. Then, given $m \in M$, we have $m = 0$ if and only if $\frac{m}{1} = 0$ in $M_\mathfrak{p}$ for each $\mathfrak{p} \in \operatorname{Ass} M$.

Proof. The forwards direction here is easy: if $m = 0$, then $\frac{m}{1} = \frac{0}{1} = 0$ in $M_\mathfrak{p}$ for any prime $\mathfrak{p}$ and therefore for any prime $\mathfrak{p} \in \operatorname{Ass} M$.

In the other direction, suppose $m \neq 0$, and we need to find an associated prime $\mathfrak{p} \in \operatorname{Ass} M$ for which $\frac{m}{1} \neq 0$ in $M_\mathfrak{p}$. But we note that $\frac{m}{1} = \frac{0}{1}$ in $M_\mathfrak{p}$ if and only if there exists $u \in M \setminus \mathfrak{p}$ such that $um = 0$ if and only if $(M \setminus \mathfrak{p}) \cap \operatorname{Ann} m \neq \varnothing$ if and only if

$$\operatorname{Ann} m \not\subseteq \mathfrak{p}.$$

So our goal is to construct an associated prime $\mathfrak{p}$ such that $\operatorname{Ann} m \subseteq \mathfrak{p}$.

The main idea is to use Proposition 2.147 to give us our prime. We set

$$\mathcal{P}_m := \{\operatorname{Ann} m' : \operatorname{Ann} m' \supseteq \operatorname{Ann} m \text{ and } m' \neq 0\}.$$

Note that $\mathcal{P}_m$ is nonempty because $\operatorname{Ann} m \in \mathcal{P}_m$, so $\mathcal{P}_m$ will have a maximal element named $\mathfrak{p}$. (Here we are using the condition that R is Noetherian.) We now note that $\mathfrak{p}$ is also maximal in

$$\mathcal{P} := \{\operatorname{Ann} m' : m' \neq 0\}.$$

Indeed, if $\mathfrak{p} \subseteq \operatorname{Ann} m'$, then $\operatorname{Ann} m \subseteq \operatorname{Ann} m'$, so $\operatorname{Ann} m' \in \mathcal{P}_m$, so $\mathfrak{p} = \operatorname{Ann} m'$ by maximality of $\mathfrak{p}$. It follows from Proposition 2.147 that $\mathfrak{p}$ is indeed prime, so it is an associated prime containing $\operatorname{Ann} m$. ■

Here are some corollaries.

Corollary 2.152. Fix R Noetherian and M an R-module. Then a submodule $N \subseteq M$ has $N = 0$ if and only if $N_\mathfrak{p} = 0$ for each $\mathfrak{p} \in \operatorname{Ass} M$.

Proof. Again, in the forwards direction, note that $N = 0$ implies $N_\mathfrak{p} = 0$ for each prime $\mathfrak{p}$.

In the reverse direction, suppose that $N_\mathfrak{p} = 0$ for each $\mathfrak{p} \in \operatorname{Ass} M$. Then any $m \in N$ has $\frac{m}{1} = 0$ in $N_\mathfrak{p}$ for each $\mathfrak{p} \in \operatorname{Ass} M$, but this means that there exists $u \in R \setminus \mathfrak{p}$ such that $um = 0$, which also holds in $M_\mathfrak{p}$. This is to say that $\frac{m}{1} = 0$ in $M_\mathfrak{p}$ for each $\mathfrak{p} \in \operatorname{Ass} M$, so $m = 0$ by Proposition 2.151. ■

Corollary 2.153. Fix R Noetherian and M, N as R-modules. Then a map $\varphi : M \to N$ is injective if and only if $\varphi : M_\mathfrak{p} \to N_\mathfrak{p}$ is injective for each $\mathfrak{p} \in \operatorname{Ass} M$.

Proof. By Corollary 2.152, $\ker\varphi \subseteq M$ vanishes if and only if $(\ker\varphi)_\mathfrak{p} = 0$ for each $\mathfrak{p} \in \operatorname{Ass} M$. But $(\ker\varphi)_\mathfrak{p} = \ker\varphi_\mathfrak{p}$ by Corollary 2.54, so $\ker\varphi = 0$ if and only if $\ker\varphi_\mathfrak{p}$ for each $\mathfrak{p} \in \operatorname{Ass} M$, which is what we wanted. ■

2.4.3 Associated Primes in Short Exact Sequences

We note that associated primes also behave in short exact sequences, somewhat.

Lemma 2.154. Suppose

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

is a short exact sequence of R-modules. Then $\operatorname{Ass} A \subseteq \operatorname{Ass} B \subseteq \operatorname{Ass} A \cup \operatorname{Ass} C$.

Proof. Denote our morphisms by

$$0 \to A \xrightarrow{\iota} B \xrightarrow{\pi} C \to 0.$$

We have that $\operatorname{Ass} A \subseteq \operatorname{Ass} B$ because any annihilator in A will end up being any annihilator in B as well. We note that any $a \in A$ has

$$\operatorname{Ann}\iota(a) = \{r \in R : r\iota(a) = 0\} = \{r \in R : \iota(ra) = 0\} \stackrel{*}{=} \{r \in R : ra = 0\} = \operatorname{Ann} a,$$

where in $\stackrel{*}{=}$ we have used the injectivity of ι. So any associated prime $\mathfrak{p} = \operatorname{Ann} a$ of A will also be an associated prime $\mathfrak{p} = \operatorname{Ann}\iota(a)$ of B.

Remark 2.155 (Nir). Alternatively, any associated prime $\mathfrak{p} \in \operatorname{Ass} A$ induces an R-embedding $R/\mathfrak{p} \hookrightarrow A$ (by Lemma 2.144). Post-composing with ι gives an R-embedding $R/\mathfrak{p} \hookrightarrow B$, so Lemma 2.144 gives $\mathfrak{p} \in \operatorname{Ass} B$.

It remains to show $\operatorname{Ass} B \subseteq \operatorname{Ass} A \cup \operatorname{Ass} C$. Well, suppose $\mathfrak{p} \in \operatorname{Ass} B \setminus \operatorname{Ass} A$, and we show that $\mathfrak{p} \in \operatorname{Ass} C$. Namely, we can find $b \in B$ such that

$$\operatorname{Ann} b = \mathfrak{p}.$$

To make some of our language easier, we note that this $b \in B$ induces $f : R/\mathfrak{p} \hookrightarrow B$ by $f : [r]_\mathfrak{p} \mapsto rb$ (as in Lemma 2.144); note $\operatorname{im} f = Rb$. It will be enough to show that $\pi f : R/\mathfrak{p} \to C$ is injective to show that $\mathfrak{p} \in \operatorname{Ass} C$ by Lemma 2.144.

We compute

$$\ker(\pi f) = \{[r]_\mathfrak{p} \in R/\mathfrak{p} : \pi f([r]_\mathfrak{p}) = 0\} = \{[r]_\mathfrak{p} \in R/\mathfrak{p} : rb \in \ker\pi = \operatorname{im}\iota\}.$$

In particular, because $f : R/\mathfrak{p} \to Rb$ is an isomorphism, $\ker(\pi f)$ will vanish if and only if each $rb \in Rb$ with $rb \in \operatorname{im}\iota$ has $rb = 0$. That is, we want to show that

$$Rb \cap \operatorname{im}\iota \stackrel{?}{=} \{0\}.$$

Indeed, each $rb \in Rb \setminus \{0\}$ (so that $r \notin \mathfrak{p}$) has $s \in \operatorname{Ann} rb$ if and only if $sr \in \mathfrak{p}$ if and only if $s \in \mathfrak{p}$, so any nontrivial intersection above would induce an annihilator $\mathfrak{p} \in \operatorname{Ass} A$, which we assumed is not the case. ■

Corollary 2.156. Suppose $B = A \oplus C$ as R-modules. Then $\operatorname{Ass} B = \operatorname{Ass} A \cup \operatorname{Ass} C$.

Proof. Note the split short exact sequences

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

and

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

give that $\operatorname{Ass} A, \operatorname{Ass} C \subseteq \operatorname{Ass} B$ by Lemma 2.154. In particular, $\operatorname{Ass} A \cup \operatorname{Ass} C \subseteq \operatorname{Ass} B$, but Lemma 2.154 implies $\operatorname{Ass} B \subseteq \operatorname{Ass} A \cup \operatorname{Ass} C$ already, so equality follows. ■

Here's a quick example of our theory at work, actually able to classify associated primes.

Example 2.157. We work with $\mathbb{Z}$-modules. Indeed, fix any finitely generated abelian group

$$M \cong \bigoplus_{k=1}^{n} \mathbb{Z}/p_k^{\alpha_k}\mathbb{Z},$$

where the p_k are primes (possible equal to 0) and α_k positive integers. Then By Corollary 2.156, we have that

$$\operatorname{Ass} M = \bigcup_{k=1}^{n} \operatorname{Ass} \mathbb{Z}/p_k^{\alpha_k}\mathbb{Z}.$$

So it remains to compute $\operatorname{Ass} \mathbb{Z}/p^\alpha\mathbb{Z}$ where p is a prime (possibly equal to 0) and α is a positive integer. But we note $\operatorname{Ass} \mathbb{Z}/0\mathbb{Z} = \operatorname{Ass} \mathbb{Z} = \{(0)\}$ because $\mathbb{Z}$ is an integral domain. And for nonzero primes, Exercise 2.143 tells us that $\operatorname{Ass} \mathbb{Z}/p^\alpha\mathbb{Z} = \{(p)\}$, so we find $\operatorname{Ass} M = \{(p_k)\}_{k=1}^n$.

2.4.4 Finding All Associated Primes

Let's try as hard as we can to find all associated primes. To start, we show there are finitely many. Here is our main lemma in the proof that there are finitely many associated primes.

Lemma 2.158. Fix M a finitely generated module over a Noetherian ring R. Then M has a finite filtration

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

such that each quotient $M_{k+1}/M_k \cong R/\mathfrak{p}_k$ for some prime ideals $\{\mathfrak{p}_k\}_{k=0}^{n-1}$.

Proof. If $M = 0$, then our filtration is just "$M_0 = M$."

If $M \neq 0$, then because R is Noetherian, $\operatorname{Ass} M$ is nonempty. So find some $\mathfrak{p}_0 = \operatorname{Ann} m_0$ for $m_0 \in M/M_0 = M$, and (using Lemma 2.144) set $M_1 := Rm_1 \cong R/\mathfrak{p}_1$. If $M/M_1 = (0)$, then we get the filtration series

$$M_0 \subseteq M_1.$$

More generally, suppose that, for some $\ell \in \mathbb{N}$, we have built a strictly ascending chain

$$M_0 \subseteq M_1 \subseteq \cdots \subseteq M_\ell$$

such that $M_{k+1}/M_k \cong R/\mathfrak{p}_k$ for each $0 \le k < \ell$. If $M/M_\ell = 0$, then this filtration satisfies the conclusion.

Otherwise, R is Noetherian, so $\operatorname{Ass} M/M_\ell$ is nonempty, so find $\mathfrak{p}_\ell \in \operatorname{Ass} M/M_\ell$. Then (by Lemma 2.144), we get to say $\mathfrak{p}_\ell = \operatorname{Ann}[m]_{M_\ell}$ so that $R/\mathfrak{p}_\ell \cong R[m]_{M_\ell}$. So define $M_{\ell+1} := M_\ell + Rm$. Then

$$\frac{M_{\ell+1}}{M_\ell} = \frac{M_\ell + Rm}{M_\ell} \cong R[m]_{M_\ell},$$

where the last isomorphism is by $[x+rm]_{M_\ell} = [rm]_{M_\ell} \mapsto r[m]_{M_\ell}$. But then $M_{\ell+1}/M_\ell \cong R/\mathfrak{p}_\ell$, so we get to continue our filtration.

However, this filtration-creating process gives us an ascending chain of R-submodules

$$M_0 \subseteq M_1 \subseteq \cdots,$$

which must eventually terminate because M is Noetherian—M is finitely generated over the Noetherian ring R. But the only way for our process to terminate is when we find some M_n such that $M/M_n = (0)$, or equivalently $M = M_n$, so the filtration is completed. ■

And here is our result.

Theorem 2.159. Fix M a finitely generated module over a Noetherian ring R. Then $\operatorname{Ass} M$ is finite.

Proof. By Lemma 2.158, we are promised a filtration

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

such that each quotient $M_{k+1}/M_k \cong R/\mathfrak{p}_k$ for some primes $\{\mathfrak{p}_k\}_{k=0}^{n-1}$. In particular, we get the short exact sequences

$$0 \to M_k \to M_{k+1} \to M_{k+1}/M_k \to 0,$$

which tell us that $\operatorname{Ass} M_{k+1} \subseteq \operatorname{Ass} M_k \cup \operatorname{Ass} M_{k+1}/M_k$ by Lemma 2.154. But $\operatorname{Ass} M_{k+1}/M_k = \operatorname{Ass} R/\mathfrak{p}_k = \{\mathfrak{p}_k\}$ by Example 2.146. So, inductively, we get that

$$\operatorname{Ass} M_k \subseteq \bigcup_{\ell=0}^{k-1} \{\mathfrak{p}_\ell\},$$

where the induction starts with $\operatorname{Ass} M_0 = \operatorname{Ass}(0) = \varnothing$. Now, setting $k = n$ recovers the result. ■

Remark 2.160 (Nir)**.** The above theorem is "effective" in the sense that, if we could compute the filtration Lemma 2.158, we would have an effective upper bound on $\operatorname{Ass} M$. However, making the filtration required using the non-effective Proposition 2.147.

Let's also discuss some other ways we can access associated primes; just like support, associated primes commute with localization.

Proposition 2.161. Fix M a finitely generated module over a Noetherian ring R. Further, fix $U \subseteq R$ a multiplicatively closed subset. Then we have that

$$\operatorname{Ass}_{R[U^{-1}]} M\left[U^{-1}\right] = \{\mathfrak{p}\left[U^{-1}\right] : \mathfrak{p} \in \operatorname{Ass} M, \mathfrak{p} \cap U = \varnothing\}.$$

Proof. Recall from Theorem 2.29 that

$$\operatorname{Spec} R\left[U^{-1}\right] = \{\mathfrak{p}\left[U^{-1}\right] : \mathfrak{p} \in \operatorname{Spec} R \text{ and } \mathfrak{p} \cap U = \varnothing\},$$

so these are all the primes we have to consider.

In one direction, suppose that $\mathfrak{p} \in \operatorname{Ass} M$ and $\mathfrak{p} \cap U = \varnothing$ so that $\mathfrak{p}\left[U^{-1}\right] \in \operatorname{Spec} R\left[U^{-1}\right]$. Because $\mathfrak{p} \in \operatorname{Ass} M$, Lemma 2.144 gives us an embedding

$$R/\mathfrak{p} \hookrightarrow M.$$

But localization preserves injections, so this induces an injection

$$R\left[U^{-1}\right]/\mathfrak{p}\left[U^{-1}\right] \hookrightarrow M\left[U^{-1}\right],$$

from which Lemma 2.144 promises $\mathfrak{p}\left[U^{-1}\right] \in \operatorname{Ass} M\left[U^{-1}\right]$.

The other direction is harder. Suppose that $\mathfrak{p}\left[U^{-1}\right] \in \operatorname{Ass}_{R[U^{-1}]} M\left[U^{-1}\right]$, so we are promised some injection

$$R\left[U^{-1}\right]/\mathfrak{p}\left[U^{-1}\right] \hookrightarrow M\left[U^{-1}\right].$$

We need to turn this into an injection $R/\mathfrak{p} \hookrightarrow M$. As a first step, we note that, because $R\left[U^{-1}\right]$, we can let φ be the composite

$$(R/\mathfrak{p}) \otimes_R R\left[U^{-1}\right] \cong \frac{R \otimes_R R\left[U^{-1}\right]}{\mathfrak{p} \otimes_R R\left[U^{-1}\right]} \cong \frac{R\left[U^{-1}\right]}{\mathfrak{p}\left[U^{-1}\right]} \hookrightarrow M\left[U^{-1}\right] \cong M \otimes_R R\left[U^{-1}\right].$$

The key trick is to apply Lemma 2.61, which gives a functorial morphism

$$\alpha : \operatorname{Hom}_R(R/\mathfrak{p}, M) \otimes_R R\left[U^{-1}\right] \cong \operatorname{Hom}_{R[U^{-1}]}\left((R/\mathfrak{p}) \otimes_R R\left[U^{-1}\right], M \otimes_R R\left[U^{-1}\right]\right).$$

But now we see M is finitely generated, so there is some projection $R^n \twoheadrightarrow M$. With R Noetherian, all submodules of R^n will be finitely generated, so the kernel of $R^n \twoheadrightarrow M$ is finitely generated, so M is in fact finitely presented.

Thus, Proposition 2.68 promises our α is an isomorphism. Namely, we have some morphism $\psi : R/\mathfrak{p} \to M$ such that $\alpha(s/u \otimes \psi) = \varphi$ in the sense that (tracking Lemma 2.61 through)

$$\alpha(\psi \otimes s/u)([r]_\mathfrak{p} \otimes s'/u') = \psi([r]_\mathfrak{p}) \otimes (ss')/(uu') = \varphi([r]_\mathfrak{p} \otimes s'/u').$$

We now check that ψ is an injection, which will finish by Lemma 2.144.

Indeed, if $\psi([r]_\mathfrak{p}) = 0$, then $\psi([r]_\mathfrak{p}) \otimes 1/1 = \varphi([r]_\mathfrak{p} \otimes 1/1) = 0$, so the injectivity of φ implies $[r]_\mathfrak{p} \otimes 1/1 = 0$. Viewing this in $(R/\mathfrak{p})\left[U^{-1}\right]$, we see we're saying

$$\frac{[r]_\mathfrak{p}}{1} = \frac{[0]_\mathfrak{p}}{1},$$

which implies there is some $u \in U$ such that $u[r]_\mathfrak{p} = u[0]_\mathfrak{p} = [0]_\mathfrak{p}$ so that $ur \in \mathfrak{p}$. But $U \cap \mathfrak{p} = \varnothing$, so $u \notin \mathfrak{p}$, so this requires $r \in \mathfrak{p}$, so $[r]_\mathfrak{p} = [0]_\mathfrak{p}$. Thus, $\ker\psi$ is trivial, and ψ is indeed injective. ■

Amusingly, we can also look at associated primes by their union.

Proposition 2.162. Fix M a module over a Noetherian ring R. Then

$$\bigcup_{\mathfrak{p} \in \operatorname{Ass} M} \mathfrak{p} = \bigcup_{m \in M \setminus \{0\}} \operatorname{Ann} m.$$

Proof. Note that each $\mathfrak{p} \in \operatorname{Ass} m$ is an annihilator of a nonzero element $m \in M \setminus \{0\}$, so we get

$$\bigcup_{\mathfrak{p} \in \operatorname{Ass} M} \mathfrak{p} \subseteq \bigcup_{m \in M \setminus \{0\}} \operatorname{Ann} m.$$

For the other direction, pick up any $\operatorname{Ann} m$ for $m \neq 0$. By Proposition 2.151, there exists $\mathfrak{p} \in \operatorname{Ass} M$ such that $\frac{m}{1} \neq \frac{0}{1}$, so there exists no $u \in R \setminus \mathfrak{p}$ such that $um = 0$. In other words, $(R \setminus \mathfrak{p}) \cap \operatorname{Ann} m = \varnothing$, so

$$\operatorname{Ann} m \subseteq \mathfrak{p}.$$

Looping all over $\operatorname{Ann} m$ gives the needed inclusion. ■

Remark 2.163 (Serganova)**.** One could also proceed more directly, without using Proposition 2.151, by choosing $\mathfrak{p}$ to be maximal among annihilators containing $\operatorname{Ann} m$ as in the proof of Proposition 2.151.

Corollary 2.164. Fix M a finitely generated module over a Noetherian ring R, and fix any ideal $J \subseteq R$. Then one of the following is true.

(i) We have $J \subseteq \operatorname{Ann} m$ for some $m \in M$

(ii) There exists $a \in J$ such that $am = 0$ implies $m = 0$ for each $m \in M$.

Proof. The idea is to use Proposition 2.162. Suppose (ii) is false so that every $a \in J$ annihilates some nonzero element of M. Then

$$J \subseteq \bigcup_{m \in M \setminus \{0\}} \operatorname{Ann} m = \bigcup_{\mathfrak{p} \in \operatorname{Ass} M} \mathfrak{p}.$$

We claim that $J \subseteq \mathfrak{p}$ for some $\mathfrak{p} \in \operatorname{Ass} M$, which will show J satisfies (i). For concreteness, label

$$\{\mathfrak{p}_1, \ldots, \mathfrak{p}_n\}$$

as the primes of $\operatorname{Ass} M$ maximal among the other primes of $\operatorname{Ass} M$; this labeling is finite because of Theorem 2.159. Note that only working with these maximal primes will not hurt us because each $\mathfrak{p} \in \operatorname{Ass} M$ lives inside some prime maximal in $\operatorname{Ass} M$ so that

$$J \subseteq \bigcup_{\mathfrak{p} \in \operatorname{Ass} M} \mathfrak{p} \subseteq \bigcup_{k=1}^{n} \mathfrak{p}_k.$$

The reason that we are using these maximal primes is to be promised some $x_{k,\ell} \in \mathfrak{p}_\ell \setminus \mathfrak{p}_k$ for $k \neq \ell$.

Now, suppose that $J \not\subseteq \mathfrak{p}_k$ for each $\mathfrak{p}_k$, and we will show J is not a subset of the union of the $\mathfrak{p}_k$s. For this, we appeal to the following lemma.

Lemma 2.165 (Prime avoidance)**.** Fix a ring R and ideals $I_1, \ldots, I_n$ of R, at most two of which are not prime. If an ideal H has $J \not\subseteq \mathfrak{I}_k$ for each I_k, then J contains an element not in any of the I_k.

Proof. We induct on n. If $n = 0$, then $0 \in J$ will do. If $n = 1$, then we just say that $J \setminus I_1$ is nonempty, finishing.

Now take $n \geq 2$. By the induction, we are promised elements

$$x_\ell \in J \Bigg\backslash \bigcup_{k \neq \ell} I_k.$$

For psychological reasons, suppose for the sake of contradiction that J is in fact contained in the union of the I_k. Then we must have $x_\ell \in I_\ell$ for each ℓ. We now have two cases to finish our inductive step.

- If $n = 2$, then
$$x_1 + x_2 \equiv x_2 \not\equiv 0 \pmod{I_1} \qquad \text{and} \qquad x_1 + x_2 \equiv x_1 \not\equiv 0 \pmod{I_2},$$
so $x_1 + x_2 \in J \setminus (I_1 + I_2)$, finishing the proof. (Technically, this is our contradiction.)
- If $n > 2$, then at least one of the I_k is prime, so we may rearrange the I_k so that I_1 is prime. But then $y \coloneqq x_1 + x_2 x_3 \cdot \ldots \cdot x_n$ has
$$y \equiv x_2 x_3 \cdot \ldots \cdot x_n \not\equiv 0 \pmod{I_1} \qquad \text{and} \qquad y \equiv x_1 \pmod{I_k} \text{ for } k > 1.$$
In particular, $x_2 x_3 \cdot \ldots \cdot x_n \notin I_1$ because each of the x_k is not in I_1 and I_1 is prime. Thus, y will now provide our contradiction.

The above cases finish the proof. ■

The above lemma immediately finishes the proof. ■

Lastly, we provide another way to generated associated primes, to close out our discussion.

Proposition 2.166. Fix M a finitely generated module over a Noetherian ring R. If $\mathfrak{p}$ is a minimal prime ideal containing $\operatorname{Ann} M$, then $\mathfrak{p} \in \operatorname{Ass} M$.

Proof. The main idea is to localize at $\mathfrak{p}$ so that $\operatorname{Ass} M_\mathfrak{p}$ should be $\{\mathfrak{p}R_\mathfrak{p}\}$. Because M is finitely generated, Proposition 2.75 tells us that $\mathfrak{p} \supseteq \operatorname{Ann} M$ implies $M_\mathfrak{p} \neq 0$. In particular, Corollary 2.148 tells us that

$$\operatorname{Ass}_{R_\mathfrak{p}} M_\mathfrak{p} \neq \varnothing.$$

However, Proposition 2.161 tells us that

$$\operatorname{Ass}_{R_\mathfrak{p}} M_\mathfrak{p} = \{\mathfrak{q}R_\mathfrak{p} : \mathfrak{q} \in \operatorname{Ass} M, \mathfrak{q} \cap (R \setminus \mathfrak{p}) = \varnothing\},$$

which must be nonempty. So we are given some associated prime $\mathfrak{q} \in \operatorname{Ass} M$ with $\mathfrak{q} \cap (R \setminus \mathfrak{p}) = \varnothing$. But $\mathfrak{q} \in \operatorname{Ass} M$ implies that $\mathfrak{q} \supseteq \operatorname{Ann} M$ ($\mathfrak{q}$ is an annihilator) while $\mathfrak{q} \cap (R \setminus \mathfrak{p}) = \varnothing$ implies that $\mathfrak{q} \subseteq \mathfrak{p}$. So minimality of $\mathfrak{p}$ (!) tells us $\mathfrak{p} = \mathfrak{q} \in \operatorname{Ass} M$, finishing. ■

Quote 2.167. I hope you see how powerful this idea is, of localization.

2.4.5 Motivating Primary Decomposition

Let's give some motivational remarks for the primary decomposition. As an example, we consider $\mathbb{Z}$, where it happens that

$$(m) \cap (n) = (mn) = (m)(n).$$

This is a very nice property to have, with respect to proving unique prime factorization and such. Namely, to state unique prime factorization, we call an ideal "primary" if it is the power of some prime ideal. Then we see existence of prime factorization is saying that any ideal (n) is the intersection of finitely many "primary" ideals.

We will try to generalize this. Here is our definition of "primary."

Definition 2.168 (Primary)**.** Fix $\mathfrak{p} \in \operatorname{Spec} R$ a prime ideal and R-modules $N \subseteq M$. Then N is a $\mathfrak{p}$-*primary* submodule of M if and only if

$$\operatorname{Ass} M/N = \{\mathfrak{p}\}.$$

Example 2.169. For a prime $p \in \mathbb{Z}$, the ideals (p^k) are p-primary in $\mathbb{Z}$ by Exercise 2.143.

Example 2.170. Any prime ideal $\mathfrak{p}$ is $\mathfrak{p}$-primary in R because $\operatorname{Ass}(R/\mathfrak{p}) = \{\mathfrak{p}\}$ by Example 2.146.

Let's prove one nice lemma to finish off today.

Lemma 2.171. Fix M a module over a Noetherian ring R. Fix $N_1, \ldots, N_m$ a finite collection of $\mathfrak{p}$-primary submodules of an R-module M. Then

$$\bigcap_{k=1}^n N_k$$

is also $\mathfrak{p}$-primary.

Proof. By induction, it suffices to show the result for $m = 2$ so that we want to show $N_1 \cap N_2$ is $\mathfrak{p}$-primary. Now, we have the right-exact sequence

$$0 \to N_1 \cap N_2 \to M \to \frac{M}{N_1} \oplus \frac{M}{N_2},$$

which tells us that we have an embedding $\frac{M}{N_1 \cap N_2} \hookrightarrow \frac{M}{N_1} \oplus \frac{M}{N_2}$. But then Lemma 2.154 gives

$$\operatorname{Ass} \frac{M}{N_1 \cap N_2} \subseteq \operatorname{Ass} M/N_1 \cup \operatorname{Ass} M/N_2 = \{\mathfrak{p}\},$$

so we are done. In particular, $\operatorname{Ass} \frac{M}{N_1 \cap N_2} \neq \varnothing$ by Corollary 2.148 because R is Noetherian and $N_1 \cap N_2 \subseteq N_1 \subsetneq M$. ■

And we close by stating the theorem.

Theorem 2.172 (Primary Decomposition)**.** Fix a finitely generated module M over a Noetherian ring R. Then any submodule $M' \subseteq M$ is an intersection of finitely many primary submodules of M.

2.5 February 8

Today we discuss primary decomposition.

2.5.1 Minimal Primes

Let's talk a little about minimal prime ideals. In particular, suppose that we have a strictly descending chain of prime ideals

$$\mathfrak{p}_1 \supsetneq \mathfrak{p}_2 \supsetneq \cdots.$$

Because prime ideals are closed under intersection in the chain, Zorn's lemma now promises us a minimal prime ideal.

More generally, we have the following definition.

Definition 2.173 (Minimal prime)**.** Fix R a ring and $I \subseteq R$ an ideal. Then a prime $\mathfrak{p} \subseteq R$ is a *minimal prime ideal over* I if $\mathfrak{p}$ is a minimal element of the set of prime ideals containing I.

The above Zorn's lemma argument shows that these minimal primes actually exist.

Proposition 2.174. Fix R a ring and $I \subsetneq R$ a proper ideal. Then there is a minimal prime $\mathfrak{p}$ over I.

Proof. We will be a little more careful than the above discussion. Let $\mathcal{P}$ be the set of primes containing I, and we partial-order $\mathcal{P}$ by inclusion. Note that I, being a proper ideal, is contained in some maximal ideal $\mathfrak{m}$, so $\mathfrak{m} \in \mathcal{P}$. Thus, $\mathcal{P}$ is nonempty.

To apply Zorn's lemma to get out a minimal element, we need to show that any descending chain in $\mathcal{P}$ is bounded below. Well, suppose that we have a chain

$$\mathfrak{p}_1 \supseteq \mathfrak{p}_2 \supseteq \mathfrak{p}_3 \supseteq \cdots$$

of prime ideals containing I. Then we set

$$\mathfrak{p} := \bigcap_{k=1}^{\infty} \mathfrak{p}_k.$$

We claim that $\mathfrak{p} \in S$, which will finish by Zorn's lemma. Because $I \subseteq \mathfrak{p}_k$ for each $\mathfrak{p}_k$, we have $I \subseteq \mathfrak{p}$. Because each $\mathfrak{p}_k$ is an ideal, the intersection $\mathfrak{p}$ will be an ideal.

Lastly, to see that $\mathfrak{p}$ is prime, suppose that $xy \in \mathfrak{p}$ so that we need to show $x \in \mathfrak{p}$ or $y \in \mathfrak{p}$. If $x \in \mathfrak{p}_k$ for each $\mathfrak{p}_k$, then $x \in \mathfrak{p}$, and we are done. Otherwise, there exists $\mathfrak{p}_N$ such that $x \notin \mathfrak{p}_N$, but then for any $n \geq N$, we have $\mathfrak{p}_n \subseteq \mathfrak{p}_N$, so $x \notin \mathfrak{p}_n$ as well. But because $xy \in \mathfrak{p}_n$, we see that

$$y \in \mathfrak{p}_n$$

for each $n \geq N$. Because $\mathfrak{p}_N \subseteq \mathfrak{p}_m$ for each $m \leq N$, we see that in fact $y \in \mathfrak{p}_k$ for each k. Thus, $y \in \mathfrak{p}$. ■

In the Noetherian case, our minimal primes are somewhat controlled.

Proposition 2.175. Fix R a Noetherian ring and $I \subseteq R$ an ideal. Then there are only finitely many minimal prime ideals over I.

Proof 1. Note $I = R$ has no minimal prime ideals over R, so we only consider proper ideals. Suppose for the sake of contradiction we have a proper ideal J for which there are infinitely many minimal prime ideals over J. Then, because R is Noetherian, we may find a maximal such ideal, and we name it I.

Note that if I is prime, then I is the unique minimal prime over I, for any minimal prime over I which is contained in I must equal I. Thus, I cannot be prime, so there exist $a, b \in R$ such that $a, b \notin I$ while $ab \in I$. Now we look at

$$I + (a) \qquad \text{and} \qquad I + (b).$$

In particular, I is a strict subset of both $I + (a)$ and $I + (b)$, so maximality of I forces $I + (a)$ and $I + (b)$ to have only finitely many minimal prime ideals over them. Let $\mathcal{P}_a$ and $\mathcal{P}_b$ be the finite sets of minimal primes over $I + (a)$ and $I + (b)$, respectively.

To finish, we claim that the set of minimal primes over I is a subset $\mathcal{P}_a \cup \mathcal{P}_b$, which will be enough because it will show that there are only finitely many minimal primes over I, a contradiction. Indeed, suppose $\mathfrak{p}$ is a minimal prime over I. Then $ab \in \mathfrak{p}$, so $a \in \mathfrak{p}$ or $b \in \mathfrak{p}$; without loss of generality, we take

$$I + (a) \subseteq \mathfrak{p}.$$

So we claim that $\mathfrak{p} \in \mathcal{P}_a$. Indeed, if a prime $\mathfrak{q}$ is contained in $\mathfrak{p}$ while containing $I + (a)$, then $\mathfrak{q}$ is a prime contained in $\mathfrak{p}$ while containing I, so minimality of $\mathfrak{p}$ implies $\mathfrak{p} = \mathfrak{q}$. This finishes. ■

Proof 2. We can use the machinery of associated primes we have been building. Note that R/I is a finitely generated R-module, and $x \in \operatorname{Ann} R/I$ if and only if $x \cdot [r]_I = [0]_I$ for all $r \in R$ if and only if $xr \in I$ for all $r \in R$ if and only if $x \in I$ (by taking $r = 1$). Thus,

$$\operatorname{Ann} R/I = I.$$

Now, any prime minimal over I will be a minimal prime containing $\operatorname{Ann} R/I$, which by Proposition 2.166 will be a prime associated to R/I. Thus, the set of minimal primes over I is a subset of

$$\operatorname{Ass} R/I,$$

which is finite by Theorem 2.159. ■

2.5.2 Primary Decomposition for Geometers

We note that Proposition 2.175 has the following corollary.

Corollary 2.176. Fix R a Noetherian ring and $I \subseteq R$ an ideal. Then $\operatorname{rad} I$ is the intersection of finitely many prime ideals.

Proof. By Proposition 2.138, we write

$$\operatorname{rad} I = \bigcap_{I \subseteq \mathfrak{p}} \mathfrak{p}.$$

Letting $\mathcal{P}$ be the set of minimal primes over I, we see that each $\mathfrak{p}$ over I has some $\mathfrak{P}_\mathfrak{p} \in \mathcal{P}$ such that $\mathfrak{P}_\mathfrak{p} \subseteq \mathfrak{p}$ (for otherwise $\mathfrak{p}$ ought to be minimal). Thus,

$$\bigcap_{\mathfrak{p} \in \mathcal{P}} \mathfrak{p} \subseteq \bigcap_{I \subseteq \mathfrak{p}} \mathfrak{p} \subseteq \bigcap_{I \subseteq \mathfrak{p}} \mathfrak{P}_\mathfrak{p} \subseteq \bigcap_{\mathfrak{p} \in \mathcal{P}} \mathfrak{p},$$

so equalities follow. Thus, $\operatorname{rad} I$ is equal to the intersection of the primes in $\mathcal{P}$, of which there are finitely many by Proposition 2.175. ■

We close with a geometric interpretation of Corollary 2.176. We have the following definition.

Definition 2.177 (Irreducible)**.** Fix $X \subseteq \mathbb{A}^n(k)$ an affine algebraic set. Then X is *irreducible* if and only if $I(X) \subseteq k[x_1, \ldots, x_n]$ is prime; i.e., $A(X)$ is an integral domain. We might call X a *variety* in this case.

As an application, consider any algebraic set $X \subseteq \mathbb{A}^n(k)$. Then we know that $I(X)$ is radical, so Corollary 2.176 is saying that we can decompose

$$I(X) = \bigcap_{\mathfrak{p} \in \mathcal{P}} \mathfrak{p},$$

where $\mathcal{P}$ is the finite collection of minimal primes over $I(X)$. Taking zero-sets everywhere, we see that[7] $Z(I \cap J) = Z(I) \cup Z(J)$, so

$$X = Z(I(X)) = Z\left(\bigcap_{\mathfrak{p} \in \mathcal{P}} \mathfrak{p}\right) = \bigcup_{\mathfrak{p} \in \mathcal{P}} Z(\mathfrak{p}).$$

Now, $I(Z(\mathfrak{p})) = \operatorname{rad} \mathfrak{p}$ by the Nullstellensatz, and $\operatorname{rad} \mathfrak{p} = \mathfrak{p}$ be primality, so the point of the above is that we have written an arbitrary algebraic set X as a union of finitely many irreducible algebraic sets $Z(\mathfrak{p})$.

Corollary 2.178. Fix $X \subseteq \mathbb{A}^n(k)$ an algebraic set. Then X can be written as the union of finitely many irreducible algebraic sets.

Proof. This follows from the above discussion. ■

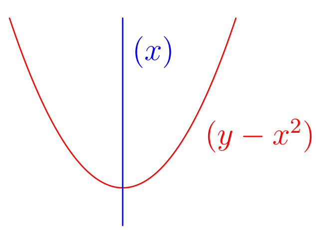
And now let's see a physical example.

Exercise 2.179. Fix $I := \left(yx - x^3\right) \subseteq k[x_1, x_2]$, and we decompose $Z(I) \subseteq \mathbb{A}^2(k)$ into irreducibles.

Proof. Well, $yx - x^3 = 0$ if and only if $x = 0$ or $y - x^2 = 0$, so

$$I = (x) \cap \left(y - x^2\right).$$

So here is the image of $Z(I)$.



Now we note (x) and $\left(y - x^2\right)$ are prime ideals because they are irreducible. ■

[7] If $x \in Z(I \cap J)$ while $x \notin Z(J)$, then there is $g \in J$ such that $g(x) \neq 0$; but $x \in Z(I \cap J)$ means that each $f \in I$ has $(fg)(x) = 0$, forcing $f(x) = 0$. Conversely, if $x \in Z(I)$ (without loss of generality), x will also vanish on $I \cap J$.

2.5.3 Primary Grab-Bag

In Corollary 2.176, we saw that when I was a radical ideal, we could write it as a finite intersection of prime ideals. Primary decomposition provides us with a general theory to do something similar for arbitrary modules. Let's start building towards that.

We pick up the following definitions.

Definition 2.168 (Primary)**.** Fix $\mathfrak{p} \in \operatorname{Spec} R$ a prime ideal and R-modules $N \subseteq M$. Then N is a $\mathfrak{p}$-*primary* submodule of M if and only if

$$\operatorname{Ass} M/N = \{\mathfrak{p}\}.$$

Definition 2.180 (Coprimary)**.** Fix M a finitely generated module over R a Noetherian ring. Then M is $\mathfrak{p}$-*coprimary* if and only if $\operatorname{Ass} M = \{\mathfrak{p}\}$.

In other words, $N \subseteq M$ is $\mathfrak{p}$-primary if and only if M/N is $\mathfrak{p}$-coprimary. Similarly, M is $\mathfrak{p}$-coprimary if and only if $(0) \subseteq M$ is $\mathfrak{p}$-primary.

We would like some more concrete conditions for being $\mathfrak{p}$-primary.

Proposition 2.181. Fix M a finitely generated module over R a Noetherian ring. Then the following are equivalent.

(a) M is $\mathfrak{p}$-coprimary.

(b) $\mathfrak{p}$ is the unique minimal prime over $\operatorname{Ann} M$, and $\mathfrak{p}$ contains $\operatorname{Ann} m$ for each $m \in M$.

(c) $\mathfrak{p}^n \subseteq \operatorname{Ann} M$ for some positive integer n, and $\mathfrak{p}$ contains $\operatorname{Ann} m$ for each $m \in M$.

Proof. We take our implications one at a time.

- We show that (a) implies (b). Note that we are given that $\operatorname{Ass} M = \{\mathfrak{p}\}$.

  We first show that $\mathfrak{p}$ is the unique minimal prime over $\operatorname{Ann} M$. Note that $M \neq (0)$ because $\operatorname{Ass} M \neq \varnothing$, so $\operatorname{Ann} M \neq R$; thus, there is at least one minimal prime over $\operatorname{Ann} M$. But we know that any prime minimal containing $\operatorname{Ann} M$ will be associated (by Proposition 2.166) and therefore must equal $\mathfrak{p}$. In particular, $\mathfrak{p}$ is indeed the unique minimal prime over $\operatorname{Ann} M$.

  To finish, we recall from Proposition 2.162 that

  $$\bigcup_{m \in M \setminus \{0\}} \operatorname{Ann} m = \bigcup_{\mathfrak{q} \in \operatorname{Ass} M} \mathfrak{q}.$$

  However, $\operatorname{Ass} M = \{\mathfrak{p}\}$, so the right-hand side is just $\mathfrak{p}$. Thus, each $m \in M \setminus \{0\}$ has $\operatorname{Ann} m \subseteq \mathfrak{p}$, as needed.

- We have to show that $\mathfrak{p}^n \subseteq \operatorname{Ann} M$ for some positive integer n. By Proposition 2.138, we see that

  $$\operatorname{rad} \operatorname{Ann} M = \bigcap_{\operatorname{Ann} M \subseteq \mathfrak{q}} \mathfrak{q},$$

  where the intersection is over all primes $\mathfrak{q}$ containing $\operatorname{Ann} M$. But $\mathfrak{p}$ is the minimal such prime, so

  $$\mathfrak{p} = \bigcap_{\operatorname{Ann} M \subseteq \mathfrak{q}} \mathfrak{p} \subseteq \bigcap_{\operatorname{Ann} M \subseteq \mathfrak{q}} \mathfrak{q} \subseteq \mathfrak{p},$$

  so equalities hold. Thus, $\mathfrak{p} = \operatorname{rad} \operatorname{Ann} M$. We now finish by appealing to the following lemma.

Lemma 2.182. Fix R a Noetherian ring and I and J ideals such that $I \subseteq \operatorname{rad} J$. Then there exists a positive integer $n \in \mathbb{N}$ such that $I^n \subseteq J$.

Proof. Because R is Noetherian, the ideal I is finitely generated, so we set

$$I := (x_1, \ldots, x_m).$$

Additionally, because $I \subseteq \operatorname{rad} J$, we are promised positive integers $a_1, \ldots, a_m$ such that $x_k^{a_k} \in J$ for each x_k. So we set $n := a_1 + \cdots + a_m$.

We claim that $I^n \subseteq J$. Indeed, I^n will be generated by elements of the form $y_1 \cdots y_n \in I^n$ such that each $y_k \in I$, so it suffices to show that such a generic element $y_1 \cdots y_n$ lives in J. We can write

$$y_k = \sum_{\ell=1}^{m} r_{k,\ell} x_\ell$$

so that when we expand

$$y_1 \cdots y_n = \prod_{k=1}^{n} \sum_{\ell=1}^{m} r_{k,\ell} x_\ell,$$

each monomial $x_1^{d_1} \cdots x_m^{d_m}$ must have some d_k at least a_k because $d_1 + \cdots + d_m = n = a_1 + \cdots + a_m$. In particular, each monomial lives in J, so the full generating element $y_1 \cdots y_m$ lives in J. ■

Remark 2.183 (Nir). The Noetherian condition is necessary. Consider $R := k[x_1, x_2, x_3, \ldots]$ with $I = (x_1, x_2, x_3, \ldots)$ and $J = \left(x_1, x_2^2, x_3^3, \ldots\right)$. Then any element of I will only use finitely many monomials, so we can reduce to the Noetherian case to show that a sufficiently large power will be contained in R, giving $I \subseteq \operatorname{rad} J$. However, for each positive integer n, we see $x_{n+1}^n \in I^n \setminus J$, so $I^n \not\subseteq J$.

- Lastly, we show that (c) implies (a). The point is to read the arguments above backwards. Because $\mathfrak{p}$ contains $\operatorname{Ann} m$ for each $m \neq 0$, we see that $\mathfrak{p}$ will contain each associated prime because associated primes are themselves annihilators.

  So suppose $\mathfrak{q}$ is some associated prime; because we already know that associated primes exist, it will suffice to show that $\mathfrak{q} = \mathfrak{p}$. We know

  $$\mathfrak{p}^n \subseteq \operatorname{Ann} M \subseteq \mathfrak{q} \subseteq \mathfrak{p},$$

  from which $\mathfrak{q} = \mathfrak{p}$ will follow. Indeed, if $x \in \mathfrak{p}$, we see that $x^n \in \mathfrak{p}^n \subseteq \mathfrak{q}$, so $x \in \mathfrak{q}$ by primality. So $\mathfrak{q} \subseteq \mathfrak{p}$, finishing. ■

Corollary 2.184. Fix R a Noetherian ring. An ideal $I \subseteq R$ is $\mathfrak{p}$-primary if and only if $\mathfrak{p}^n \subseteq I$ for some positive integer n and, for all $a \notin I$, we have $ab \in I$ implies $b \in \mathfrak{p}$.

Proof. This follows directly from (c) of the proposition. Namely, I is $\mathfrak{p}$-primary if and only if R/I is $\mathfrak{p}$-coprimary if and only if $\mathfrak{p}^n \subseteq I$ for some positive integer n and $\mathfrak{p}$ contains all $\operatorname{Ann}[a]_I$ for each $[a]_I \in R/I \setminus \{[0]_I\}$. This latter condition is the same as saying, if $a \notin I$, then $ab \in I$ (which is equivalent to $b \in \operatorname{Ann}[a]_I$) implies $b \in \mathfrak{p}$. ■

Example 2.185. Fix R an integral domain and $(p) \subseteq R$ is a nonzero prime ideal. Then, for any positive integer n, we claim $(p)^n$ is (p)-primary: note $(p)^n \subseteq (p)^n$ and, for $a \notin (p^n)$ and $ab \in (p^N)$, we claim $b \notin (p)$ by primality.

Explicitly, there is a largest nonnegative integer ν such that $a \in (p^\nu)$, so $a/p^\nu \notin (p)$. Because $a \notin (p^n)$, we see $\nu < n$. But then $p^n \mid ab$ implies that $p \mid p^{n-\nu} \mid ab$, but $p \nmid a$, so $p \mid b$.

2.5.4 Primary Decomposition

And here is our main result.

Theorem 2.186 (Primary decomposition, I)**.** Fix M a finitely generated module over a Noetherian ring R. Then every submodule $N \subseteq M$ is the intersection of finitely many primary submodules. Such an intersection is called a *primary decomposition*.

Proof. The key to this result is to instead talk about irreducible decomposition.

Definition 2.187 (Irreducible)**.** Fix M a module over a ring R. Then a submodule $N \subseteq M$ is *irreducible* if and only if $N = N_1 \cap N_2$ for submodules $N_1, N_2 \subseteq M$ implies $N = N_1$ or $N = N_2$.

Example 2.188. The module M is an irreducible submodule of M. Indeed, if $N_1, N_2 \subseteq M$ have $M = N_1 \cap N_2$, then in fact $N_1 = N_2 = M$ is forced.

It will turn out that irreducible implies primary, but we do not know this yet.

Here is the key claim.

Lemma 2.189. Fix M a finitely generated module over a Noetherian ring R. Then every submodule $N \subseteq M$ is the intersection of finitely many irreducible submodules. (The empty intersection is considered M here.)

Proof. Suppose for the sake of contradiction that the statement is false so that there is a submodule which is not the intersection of finitely many irreducible submodules. Because M is a Noetherian module, we can find a maximal such submodule N.

Note that N cannot be irreducible, so we can write $N = A \cap B$ for $N \subsetneq A, B$. But by the maximality of N, we can write

$$A = \bigcap_{k=1}^{n} A_k \qquad \text{and} \qquad B = \bigcap_{\ell=1}^{m} B_k,$$

where the A_k and B_k are irreducible modules. But now

$$N = A \cap B = \left(\bigcap_{k=1}^{n} A_k\right) \cap \left(\bigcap_{\ell=1}^{m} B_k\right),$$

so N is also the intersection of finitely many irreducible modules, which is a contradiction. ■

Remark 2.190 (Nir)**.** This essentially follows the proof of existence of prime factorizations in $\mathbb{Z}$: to show that any positive integer n greater than 1 has a prime factorization, we suppose a minimal counterexample (which corresponds to the maximal submodule).

But the smallest counterexample cannot be prime and is thus a product of primes (which corresponds to the intersection of submodules) and derive from the factors having prime factorizations.

And now we can finish up.

Lemma 2.191. Fix M a finitely generated module over a Noetherian ring R and $N \subsetneq M$ a proper submodule. If N is irreducible, then N is primary.

Proof. We know that $\operatorname{Ass} M/N$ is nonempty because $M \neq N$, so we need to show that there is exactly one prime.

We proceed by contraposition. So suppose $\mathfrak{p}, \mathfrak{q} \in \operatorname{Ass} M/N$ which are distinct, and we show that N is not irreducible. By Lemma 2.144, we get embeddings

$$\iota_{\mathfrak{p}} : R/\mathfrak{p} \hookrightarrow M/N \qquad \text{and} \qquad \iota_{\mathfrak{q}} : R/\mathfrak{q} \hookrightarrow M/N.$$

In particular, let $[m_{\mathfrak{p}}]_N := \iota_{\mathfrak{p}}([1]_{\mathfrak{p}})$ and $[m_{\mathfrak{q}}]_N := \iota_{\mathfrak{q}}([1]_{\mathfrak{1}})$. Note that an element $\iota_{\mathfrak{p}}([r]_{\mathfrak{p}}) \in \operatorname{im} \iota_{\mathfrak{p}}$ is nonzero if and only if $r \notin \mathfrak{p}$ because $\iota_{\mathfrak{p}}$ is an embedding. In fact, for any nonzero $\iota_{\mathfrak{p}}([r]_{\mathfrak{p}})$, the annihilator consists of $s \in R$ such that

$$s \cdot r[m_{\mathfrak{p}}] = sr\iota_{\mathfrak{p}}([1]_{\mathfrak{p}}) = \iota_{\mathfrak{p}}([sr]_{\mathfrak{p}})$$

vanishes, but then $r \notin \mathfrak{p}$ makes this equivalent to $s \in \mathfrak{p}$.

So the annihilator of any nonzero element in $\operatorname{im} \iota_{\mathfrak{p}}$ is $\mathfrak{p}$. Similarly, the annihilator of any nonzero element in $\operatorname{im} \iota_{\mathfrak{q}}$ is $\mathfrak{q}$. Thus, nonzero elements of $\operatorname{im} \iota_{\mathfrak{p}}$ and $\operatorname{im} \iota_{\mathfrak{q}}$ cannot coincide, so

$$(\operatorname{im} \iota_{\mathfrak{p}}) \cap (\operatorname{im} \iota_{\mathfrak{q}}) = 0.$$

So we can write

$$N = (\operatorname{im} \iota_{\mathfrak{p}} + N) \cap (\operatorname{im} \iota_{\mathfrak{q}} + N)$$

to break that N is irreducible. Indeed, the $\operatorname{im} \iota_\bullet + N$ strictly contains N because the $\iota_\bullet$ embedded into M/N from a module with more than one element. And $m \in (\operatorname{im} \iota_{\mathfrak{p}} + N) \cap (\operatorname{im} \iota_{\mathfrak{q}} + N)$ implies that $[m]_N \in (\operatorname{im} \iota_{\mathfrak{p}}) \cap (\operatorname{im} \iota_{\mathfrak{q}})$, forcing $m \in N$ as above. ■

Remark 2.192. Not all primary modules are irreducible; we follow sx3039361. Namely, set $R := k[x, y]$ and $I := (x^2, xy, y^2) = (x, y)^2$.

- We see I is (x, y)-primary. Any constant c will have $\operatorname{Ann}[c]_I = I$, which is not prime. But any linear $f := ax + by$ will have $\operatorname{Ann}[f]_I = (x, y)$. Because R/I only has constants and linear polynomials, $\operatorname{Ass} R/I = \{(x, y)\}$.
- We see I is not irreducible because

$$I = \left(x^2, y\right) \cap \left(x, y^2\right).$$

That $x^2, xy, y^2 \in \left(x^2, y\right) \cap \left(x, y^2\right)$ is clear. In the other direction, if we take $f \in \left(x^2, y\right) \cap \left(x, y^2\right)$ and remove all monomials divisible by x^2 or y^2, the remaining polynomial must live in $(x) \cap (y) = (xy)$.

The above two lemmas essentially finish the theorem. Given our submodule $N \subseteq M$, we give it an irreducible "decomposition"

$$N = \bigcap_{k=1}^{n} N_k.$$

Note that if any $N_k = M$, then we may safely remove the term because all terms of the intersection are subsets of M. So we can write an irreducible decomposition for N where all terms are proper irreducible submodules, which we then know are primary submodules. ■

Let's try to make primary decomposition a little more canonical.

Theorem 2.193 (Primary decomposition, II)**.** Fix M a finitely generated module over a Noetherian ring R. Then write some submodule $N\subseteq M$ as

$$N=\bigcap_{i=1}^n N_i$$

such that N_i is $\mathfrak{p}_i$-primary. Then the following are true.

(a) We have $\operatorname{Ass} M/N\subseteq\{\mathfrak{p}_1,\ldots,\mathfrak{p}_n\}$.

(b) If we cannot remove some N_i from the decomposition, then $\mathfrak{p}_i\in\operatorname{Ass} M/N$. In particular, if we cannot remove any N_i from the decomposition, then equality in (a) holds.

(c) If n is as small as possible, then each $\mathfrak{p}_i$ is unique.

Proof. We show these one at a time.

(a) Note that we can glue together $M\twoheadrightarrow M/N_i$ into a map

$$M\to\bigoplus_{i=1}^n M/N_i$$

with kernel $\bigcap_i N_i=N$, so we have an induced embedding $M/N\hookrightarrow\bigoplus_{i=1}^n M/N_i$. Then applying Lemma 2.154 and Corollary 2.156, we see

$$\operatorname{Ass} M/N\subseteq\operatorname{Ass}\left(\bigoplus_{i=1}^n M/N_i\right)=\bigcup_{i=1}^n\operatorname{Ass} M/N_i=\{\mathfrak{p}_1,\ldots,\mathfrak{p}_n\},$$

where the last equality is by definition of the N_i.

(b) We are given that, for each j, we have

$$K_j:=\bigcap_{\substack{i=1\\ i\neq j}}^n N_i$$

is not equal to N, but $N_j\cap K_j=N$. Thus, we can construct an embedding

$$\frac{K_j}{N}=\frac{K_j}{K_j\cap N_j}\cong\frac{N_j+K_j}{N_j}\subseteq\frac{M}{N_j}$$

to embed a nonzero submodule of M/N into M/N_j. In particular, Lemma 2.154 tells us (because of the above embedding) that $\operatorname{Ass} K_j/N\subseteq\operatorname{Ass} M/N_i=\{\mathfrak{p}_j\}$ forces $\operatorname{Ass} K_j/N=\{\mathfrak{p}_j\}$ because K_j/N is nonzero.

But then applying Lemma 2.154 again, we see $\{\mathfrak{p}_j\}=\operatorname{Ass} K_j/N\subseteq\operatorname{Ass} M/N$, so we do indeed have $\mathfrak{p}_j\in\operatorname{Ass} M/N$.

(c) This is easiest done by contraposition: if we have $\mathfrak{p}:=\mathfrak{p}_i=\mathfrak{p}_j$ for $i\neq j$, then we show that we can find a smaller primary decomposition. Indeed, by Lemma 2.171, we see that $N_i\cap N_j$ will also be $\mathfrak{p}$-primary, so we can write

$$N=\bigcap_{k=1}^n N_k=(N_i\cap N_j)\cap\bigcap_{\substack{k=1\\ k\neq i,j}}^n N_k$$

is a primary decomposition of N now using $n-1$ primary submodules. ■

Remark 2.194 (Nir)**.** With Theorem 2.193, we bound the size of a minimal primary decomposition: any minimal primary decomposition $N = \bigcap_{i=1}^n N_i$ will have none of the N_i removable, which means that $\operatorname{Ass} M/N = \{\mathfrak{p}_1, \ldots, \mathfrak{p}_n\}$ by Theorem 2.193 part (b). In particular,

$$\# \operatorname{Ass} M/N \le n.$$

In fact, it is not too hard to be convinced that this is achievable, essentially using the argument from Theorem 2.193 part (c): start with any primary decomposition and remove any removable terms until $\operatorname{Ass} M/N = \{\mathfrak{p}_1, \ldots, \mathfrak{p}_n\}$ as in Theorem 2.193 part (b). Then, intersecting all the N_i which share a $\mathfrak{p}_i$, we get a decomposition where all the $\mathfrak{p}_i$ are unique, meaning $\# \operatorname{Ass} M/N = n$, which must be minimal.

Primary decomposition also behaves with localization.

Theorem 2.195 (Primary decomposition, III)**.** Fix M a finitely generated module over a Noetherian ring R. Then write some submodule $N \subseteq M$ as

$$N = \bigcap_{i=1}^n N_i$$

such that N_i is $\mathfrak{p}_i$-primary. If $U \subseteq R$ is some multiplicatively closed subset, then

$$N\left[U^{-1}\right] = \bigcap_{\substack{i=1 \\ \mathfrak{p}_i \cap U = \varnothing}}^n N_i\left[U^{-1}\right],$$

where $N_i\left[U^{-1}\right]$ is $\mathfrak{p}_i\left[U^{-1}\right]$-primary.

Proof. By Corollary 2.55, we see that

$$N\left[U^{-1}\right] = \bigcap_{i=1}^n N_i\left[U^{-1}\right].$$

Not all the $N_i\left[U^{-1}\right]$ will in fact be primary submodules, but we can test which will be associated by using Proposition 2.161 to note

$$\operatorname{Ass} M\left[U^{-1}\right]/N_i\left[U^{-1}\right] = \left\{\mathfrak{p}\left[U^{-1}\right] : \mathfrak{p} \in \operatorname{Ass} M/N_i, \mathfrak{p} \cap U = \varnothing\right\}.$$

(We have implicitly used the fact that localization commutes with quotients.) In particular, $\operatorname{Ass} M/N_i = \{\mathfrak{p}_i\}$ implies that we only have one prime to check.

- If $\mathfrak{p}_i \cap U = \varnothing$, then $\mathfrak{p}_i\left[U^{-1}\right]$ is in fact a prime, so $\operatorname{Ass} M_i\left[U^{-1}\right]/N_i\left[U^{-1}\right] = \{\mathfrak{p}_i\left[U^{-1}\right]\}$. Thus, $N_i\left[U^{-1}\right]$ is in fact $\mathfrak{p}_i\left[U^{-1}\right]$-primary.

- Otherwise, if $\mathfrak{p}_i \cap U \neq \varnothing$, then we see that $\operatorname{Ass} M\left[U^{-1}\right]/N_i\left[U^{-1}\right]$ is empty, so the quotient is 0, so $N_i\left[U^{-1}\right] = M\left[U^{-1}\right]$. In particular, we can remove $N_i\left[U^{-1}\right]$ from the intersection.

So we see that

$$N\left[U^{-1}\right] = \bigcap_{\substack{i=1 \\ \mathfrak{p}_i \cap U = \varnothing}}^n N_i\left[U^{-1}\right],$$

and we have in fact verified that each $N_i\left[U^{-1}\right]$ is $\mathfrak{p}_i\left[U^{-1}\right]$-primary, so this provides a primary decomposition. ■

2.5.5 Factorization via Primary Decomposition

Let's do some examples.

Example 2.196. For any nonzero integer $n \in \mathbb{Z} \setminus \{0\}$, we can write

$$(n) = \prod_{p \text{ prime}} (p^{\alpha_p}),$$

for some exponents α_p. This does indeed provide a primary decomposition; notably, $(p^{\alpha_p}) = (p)^{\alpha_p}$ is (p)-primary by Example 2.185.

Remark 2.197 (Nir)**.** It is actually legal to set $n = 0 \in \mathbb{Z}$, but it is not interesting: (0) is a prime ideal, so it provides its own primary decomposition.

We can generalize the above example.

Proposition 2.198. Fix R a Noetherian domain. If $r \in R$ can be written as

$$r = u \prod_{k=1}^{n} p_k^{\alpha_k}$$

where $u \in R^\times$ and (p_k) are distinct nonzero prime ideals and $\alpha_k > 0$ are positive integers. Then

$$(r) = \bigcap_{k=1}^{n} (p_k^{\alpha_k})$$

is a minimal primary decomposition for (r).

Proof. We note that the ideal (p_k) is prime, so $(p_k)^{\alpha_k} = (p_k^{\alpha_k})$ is (p_k)-primary by Example 2.185. So to check that we have a minimality primary decomposition, we have to check that the intersection is in fact (r), and we have to check minimality.

- We check the intersection. We show the equality $\stackrel{?}{=}$ in the chain

$$(r) = \left(\prod_{k=1}^{n} p_k^{\alpha_k}\right) = \prod_{k=1}^{n} (p_k^{\alpha_k}) \stackrel{?}{=} \bigcap_{k=1}^{n} (p_k^{\alpha_k})$$

by induction on n. For $n = 0$, both sides are empty, so both sides are R. For the inductive step, we set $(s) := \prod_{k=1}^{n} (p_k^{\alpha_k}) = \bigcap_{k=1}^{n} (p_k)^{\alpha_k}$, and we have to show that

$$\left(sp_{n+1}^{\alpha_{n+1}}\right) = (s) \cap \left(p_{n+1}^{\alpha_{n+1}}\right).$$

Of course, we get $\left(sp_{n+1}^{\alpha_{n+1}}\right) \subseteq (s) \cap \left(p_{n+1}^{\alpha_{n+1}}\right)$ because $sp_{n+1}^{\alpha_{n+1}} \in (s), \left(p_{n+1}^{\alpha_{n+1}}\right)$. In the other direction, suppose that $x \in (s) \cap \left(p_{n+1}^{\alpha_{n+1}}\right)$, and we want to show that $x \in \left(sp_{n+1}^{\alpha_{n+1}}\right)$.

Quickly, note that $s \notin (p_{n+1})$ because $s \in (p_{n+1})$ would imply that one of the primes dividing into s, say $p_\bullet$, would live in (p_{n+1}). But then $p_\bullet = p_{n+1}q$ for some $q \in R$, meaning $p_\bullet \mid p_{n+1}$ or $p_\bullet \mid q$.

  - If $p_\bullet \mid p_{n+1}$, then $q \in R^\times$, so $(p_\bullet) = (p_{n+1})$, violating the distinctness of these primes.
  - Otherwise, if $p_\bullet \mid q$, then $p_{n+1} \in R^\times$, violating primality.

So all cases have given contradiction. Note that the above arguments implicitly used the fact that $p_\bullet \neq 0$ to divide it out.

Now, returning to the proof, write $x = sy$, and we show inductively that, for $k \in [0, \alpha_{n+1}]$,

$$y \in \left(p_{n+1}^k\right),$$

which will verify that indeed $x = sy \in \left(sp_{n+1}^{\alpha_{n+1}}\right)$. Well, for $k = 0$, there is nothing to say. But if $y \in \left(p_{n+1}^k\right)$ for $k < \alpha_{n+1}$, then we note that

$$sy/p_{n+1}^k \in \left(p_{n+1}^{\alpha_{n+1}-k}\right) \subseteq (p_{n+1}),$$

but (p_{n+1}) is prime while $s \notin (p_{n+1})$, so we must instead have $y/p_{n+1}^k \in (p_{n+1})$, which finishes the induction.

- It remains to check that the primary decomposition is minimal. By Remark 2.194, we see that the smallest possible number of terms n must be at least $\# \operatorname{Ass} R/(r)$, so to show that our primary decomposition is minimal, it suffices to show that $n \le \# \operatorname{Ass} R/(r)$.

  Well, because the prime ideals (p_k) are all distinct, we have left to show that (p_k) is in fact associated to $R/(r)$. For this, we claim that
  $$\operatorname{Ann}[r/p_k]_{(r)} = \{(p_k)\}.$$
  Indeed, $x \cdot [r/p_k]_{(r)} = [0]_{(r)}$ if and only if $r \mid x \cdot r/p_k$ if and only if we can find $q \in R$ such that $r = xrq/p_k$ if and only if $p_k = xq$ if and only if $p_k \mid x$ if and only if $x \in (p_k)$. ■

Of course, the main power to primary decomposition is Theorem 2.186 in the existence of the primary decomposition, so we would like to leverage this power to talk more directly about factorizations.

Proposition 2.199. Fix R a Noetherian domain. Then R is a unique factorization domain if and only if every minimal prime ideal over a principal ideal is principal.

Proof of the forwards direction in Proposition 2.199. We begin with the forward direction. The main technical lemma is as follows.

Lemma 2.200. Fix R a ring and ideals $\{I_k\}_{k=1}^n$ and a prime ideal $\mathfrak{p}$. Then if

$$\bigcap_{k=1}^n I_k \subseteq \mathfrak{p},$$

then $I_k \subseteq \mathfrak{p}$ for some I_k.

Proof. We show this by contraposition: suppose that $I_k \not\subseteq \mathfrak{p}$ for each I_k, and we show that $\bigcap_k I_k \not\subseteq \mathfrak{p}$. Well, $I_k \not\subseteq \mathfrak{p}$ promises us some $x_k \in I_k \setminus \mathfrak{p}$. But then we set

$$x := x_1 \cdots x_n.$$

Because each of the factors x_k are not in $\mathfrak{p}$, the entire product x is also not in $\mathfrak{p}$. But $x \in (x_k) \subseteq I_k$ for each I_k, so

$$x \in \left(\bigcap_{k=1}^n I_k\right) \Big\backslash\, \mathfrak{p},$$

which finishes. ■

Remark 2.201 (Nir)**.** This result cannot be extended to allow n to be infinite. For example, in $\mathbb{Z}$,

$$\bigcap_{\substack{p\text{ prime}\\ p>2}} (p) = (0) \subseteq (2),$$

but none of the prime ideals (p) for $p > 2$ are contained in (2).

Now suppose that R is a unique factorization domain, and we pick up some minimal prime ideal $\mathfrak{p}$ over a principal ideal $(r) \subseteq R$. Very quickly, we note that if $r = 0$, then (0) is prime (R is a domain), so $\mathfrak{p} = (0)$ is the unique minimal prime over (0).

Otherwise, r is nonzero. Because R is a unique factorization domain, we may write

$$r = u\prod_{k=1}^{n} p_k^{\alpha_k}$$

where $u \in R^\times$ and the (p_k) are distinct nonzero prime ideals and the $\alpha_k > 0$ are positive integers. Then we see that, by Proposition 2.198, we get

$$\bigcap_{k=1}^{n} (p_k^{\alpha_k}) = (r) \subseteq \mathfrak{p}.$$

In particular, by Lemma 2.200, we have some $(p_\bullet^{\alpha_\bullet}) \subseteq \mathfrak{p}$, so $p_\bullet^{\alpha_\bullet} \in \mathfrak{p}$, so $p_\bullet \in \mathfrak{p}$ by primality, so

$$(p_\bullet) \subseteq \mathfrak{p}.$$

But $r \in (p_\bullet)$, so $(p_\bullet)$ is a prime over (r). Thus, minimality of $\mathfrak{p}$ forces $\mathfrak{p} = (p_\bullet)$, finishing. ■

Proof of the backwards direction in Proposition 2.199. By Remark 1.30, it suffices to show that R satisfies the ascending chain condition on principal ideals and has all irreducible elements prime. Well, R is Noetherian, so it satisfies the ascending chain condition on all ideals, so any ascending chain of principal ideals will also have to stabilize.

So to finish, suppose we have some irreducible element $\pi \in R$, and we want to show that (π) is a prime ideal. Note $(\pi) \neq R$ because π is not a unit. Now, because R is Noetherian, Proposition 2.174 promises us some minimal prime $\mathfrak{p}$ over (π).

But by hypothesis on R, we see $\mathfrak{p}$ is principal, so $\mathfrak{p} = (p)$ for some $p \in R$. In particular, $\pi \in (p)$ implies that

$$\pi = pu$$

for some $u \in R$. Because π is irreducible, either $p \in R^\times$ or $u \ni R^\times$, but $(p) = \mathfrak{p} \subsetneq R$, so $p \notin R^\times$. Namely, $u \in R^\times$, so

$$(\pi) = (p) = \mathfrak{p}$$

is indeed a prime ideal. ■

Remark 2.202 (Nir)**.** As an example of the condition in Proposition 2.199 being sharp, we note that, in $R := \mathbb{Z}[\sqrt{-5}]$, we have

$$(2) \subsetneq \left(2, 1+\sqrt{-5}\right).$$

To be explicit, 2, which is irreducible but not prime, has minimal prime over (2) as $\left(2, 1+\sqrt{-5}\right)$, which is not principal. We will not justify these claims, but they follow from norm arguments.

2.5.6 A Little on Uniqueness

We remark that primary decomposition is not unique, in general, however. Here is a particularly egregious example.

Exercise 2.203. Fix $R := k[x,y]/\left(x^2, xy\right)$ a Noetherian ring. Then we claim, for any positive integer $n \geq 2$,

$$(0) = (x) \cap (y^n)$$

is a minimal primary decomposition of (0).

Proof. We have many things to check here. We quickly note that $k[x,y]$ has k-basis $\{x^i y^j\}_{i,j\in\mathbb{N}}$, so R is spanned by

$$\{1, x, y, y^2, y^3, \ldots\}$$

because the other monomials vanish. In fact, this is a basis: if

$$ax+$$

- We check that $(0) = (x) \cap (y^n)$. Indeed, suppose $f \in k[x,y]$ such that $f \in (x) \cap (y^n)$, and we claim that $f \in \left(x^2, xy\right)$. In fact, we will show that $f \in (x) \cap (y) \subseteq (x) \cap (y^n)$ implies that $f \in (xy) \subseteq \left(x^2, xy\right)$.

  Well, we note that $k[x,y]/(x) \cong k[y]$ (by $x \mapsto 0$) and $k[x,y]/(y) \cong k[y]$ (by $y \mapsto 0$), which are both integral domains, so (x) and (y) are both prime, and they are distinct because $x \notin (y)$. So Proposition 2.198 tells us that

  $$(xy) = (x) \cap (y),$$

  so $f \in (x) \cap (y)$ implies $f \in (xy)$.

- We check that (x) is (x)-primary. Well, we note that $x \mapsto 0$ induces a surjective ring morphism

  $$\varphi : k[x,y] \to k[y]$$

  with kernel (x).[8] But $x^2, xy \in (x)$, so we get an induced surjective map

  $$R \to k[y]$$

  which still has kernel (x). So $R/(x) \cong k[y]$, so (x) is prime and in particular (x)-primary.

- We check that (y^n) is (x,y)-primary. For this, we search for possible associated primes of $R/\left(y^n\right)$.

  Suppose we have $m \in R/\left(y^n\right)$ with $\mathfrak{p} = \operatorname{Ann} m \in \operatorname{Ass} R/\left(y^n\right)$. Well, we see that

  $$x^2 \cdot m = y^n \cdot m = 0,$$

  so $x^2, y^n \in \mathfrak{p}$, so primality forces $x, y \in \mathfrak{p}$, so $(x,y) \subseteq \mathfrak{p}$. But (x,y) is a maximal ideal: $x, y \mapsto 0$ induces a map $R \to k$ with kernel (x,y). Thus, we must have $\mathfrak{p} = (x,y)$ as our only possible associated prime.

  It remains to show that (x,y) is actually achievable as an annihilator. Well, consider $m := y^{n-1}$. Indeed, $x \cdot y^{n-1} = xy \cdot y^{n-2} = 0$ (here we use $n \geq 2$) and $y \cdot y^{n-1} = y^n = 0$, so

  $$(x,y) \subseteq \operatorname{Ann} m.$$

  But $y^{n-1} \neq 0$ in $R/\left(y^n\right)$: this would mean we could write $y^{n-1} = ax^2 + bxy + cy^n$ for $a, b, c \in k[x,y]$, which is impossible by degree arguments. Thus, maximality of (x,y) forces $(x,y) = \operatorname{Ann} m$.

- We check that $(0) = (x) \cap (y^n)$ is a minimal primary decomposition. Well, $x \neq 0$ and $y^n \neq 0$ implies that $(0) \neq (x)$ and $(0) \neq (y^n)$, so no module in this primary decomposition is removable.

  Thus, by Theorem 2.193, we see $\operatorname{Ass} R = \{(x,y), (x)\}$, and Remark 2.194 tells us that a minimal primary decomposition will have at least $\# \operatorname{Ass} R = 2$ terms. So indeed, we have a primary decomposition with 2 terms, and it must be minimal. ■

The point is that the above example provides "lots" of different minimal primary decomposition.

[8] Namely, $\varphi(f) = 0$ if and only if all monomials in f are divisible by x if and only if $f \in (x)$.

2.5.7 A Little on Graded Rings

We will want to consider primary decomposition for graded rings because later in life we will want to talk about projective space.

Proposition 2.204. Fix $R = R_0 \oplus R_1 \oplus \cdots$ a graded ring and M a graded module over R. Suppose that we have $m \in M$ and $\mathfrak{p} := \operatorname{Ann} m$ an associated prime ideal. Then $\mathfrak{p}$ is a graded ideal of R.

In other words, associated primes of a graded module are graded.

Proof. This is an exercise in proof by brute force. We have to show that

$$\mathfrak{p} = \bigoplus_{i=1}^{\infty} (R_i \cap \mathfrak{p}).$$

So we write, for some $f \in \mathfrak{p}$, that

$$f = \sum_{i=1}^{s} f_i,$$

where $f_i \in R_{d_i}$, and $d_1 < \cdots < d_n$. We are showing that $f_i \in \mathfrak{p}$ for each f_i. For this, we induct on s: if $s = 1$, then there is nothing to show. For the inductive step, we now remark that it will be enough to show that $f_1 \in \mathfrak{p}$ because then $f - f_1$ will have fewer terms, triggering the inductive hypothesis.

Well, using any m with $\mathfrak{p} = \operatorname{Ann} m$, we may write

$$m = \sum_{j=1}^{t} m_j,$$

where $m_j \in R_{e_j}$ and $e_1 < \cdots < e_t$. We are interested in isolating $f_1 m$, and to make our lives easier we will do yet another induction on t. Note that a full expansion of $fm = 0$ gives

$$0 = \sum_{i=1}^{s} \sum_{j=1}^{t} f_i m_j.$$

However, by the grading, we note that $f_i m_j \in M_{d_i + e_j}$, so the term of lowest degree will occur when $d_i + e_j$ is minimized, which is $d_1 + e_1$. In particular, the term of lowest degree is when $i = j = 1$ and is therefore (uniquely!) $f_1 m_1$, so we see $f_1 m_1 = 0$. In particular, we get to write

$$f_1 m = \sum_{j=2}^{t} f_1 m_j.$$

So if we were in the base case of $t = 1$, we would now be able to conclude $f_1 m = 0$ so that $f_1 \in \mathfrak{p}$.

Otherwise, for the inductive step, we remark that any $x \in \mathfrak{p}$ will have $x \cdot f_1 m = f_1(xm) = 0$, so $\mathfrak{p} \subseteq \operatorname{Ann} f_1 m$. We finish by considering the following two cases.

- If $\mathfrak{p} = \operatorname{Ann} f_1 m$, then we note that we can replace m with $\sum_{j=2}^{t} m_j$, which has one fewer term, so we get to apply the inductive hypothesis to conclude $f_1 \in \mathfrak{p}$.
- Otherwise, $\mathfrak{p} \subsetneq \operatorname{Ann} f_1 m$, which means that there is some $g \in \operatorname{Ann} f_1 m \setminus \mathfrak{p}$. But then $g f_1 m = 0$, so $g f_1 \in \operatorname{Ann} m = \mathfrak{p}$, so $g \notin \mathfrak{p}$ forces $f_1 \in \mathfrak{p}$. ■

Theme 3
Monic Polynomials

One is the loneliest number that you'll ever do

—Harry Nilsson

3.1 February 10

Here we go.

3.1.1 Unique Factorization Domains

We start with the following result; it is due to Gauss.

Theorem 3.1. Fix R a unique factorization domain. Then $R[x]$ is a unique factorization domain.

Proof. The main character in our story is as follows.

Definition 3.2 (Content)**.** Fix R a ring and $f(x) = a_0x^0 + \cdots + a_nx^n \in R[x]$. Then we define the *content* of f to be the ideal

$$\operatorname{cont}(f) := (a_0, \ldots, a_n) \subseteq R.$$

Remark 3.3 (Nir)**.** Readers might be more familiar with the case of a principal ideal domain, in which the content is chosen to be a generator of the above ideal. For example, one can write the proof that $\mathbb{Z}[x]$ is a unique factorization domain avoiding ideals as much as possible by setting the content to be the greatest common denominator of the coefficients.

Remark 3.4 (Nir). This definition always looked unnatural until I realized that it does in fact preserve some structure of $R[x]$. For example, for $r \in R$ and $f(x) = a_0x^0 + \cdots + a_nx^n \in R[x]$, we see $(rf)(x) = ra_0x^0 + \cdots + ra_nx^n$ so that

$$\operatorname{cont}(rf) = (ra_0, \ldots, ra_n) = r(a_0, \ldots, a_n) = r\operatorname{cont}(f).$$

Additionally, we can show $\operatorname{cont}(f(x+r)) = \operatorname{cont}(f(x))$. By symmetry, it suffices for $\operatorname{cont}(f(x+r)) \subseteq \operatorname{cont}(f(x))$, for which we note

$$f(x+r) = \sum_{k=0}^{n} a_k(x+r)^k = \sum_{k=0}^{n}\left(\sum_{\ell=0}^{k} a_k\binom{k}{\ell}x^\ell r^k\right) = \sum_{\ell=0}^{n}\left(\sum_{k=\ell}^{n}\binom{k}{\ell}r^k a_k\right)x^\ell$$

has all coefficients in $\operatorname{cont}(f)$.

Here is the main claim.

Lemma 3.5 (Gauss). Fix R a ring and $f, g \in R[x]$. Then $\operatorname{cont}(fg) \subseteq \operatorname{cont}(f)\operatorname{cont}(g) \subseteq \operatorname{rad}\operatorname{cont}(fg)$.

Proof. We show the inclusions independently.

- That $\operatorname{cont}(fg) \subseteq \operatorname{cont}(f)\operatorname{cont}(g)$ is easier. We write

$$f(x) = \sum_{k=0}^{\infty} a_kx^k \qquad \text{and} \qquad g(x) = \sum_{\ell=0}^{\infty} b_\ell x^\ell,$$

  where all but finitely many of the a_k and b_ℓ vanish. Then

$$(fg)(x) = \sum_{n=0}^{\infty}\left(\sum_{k+\ell=n} a_kb_\ell\right)x^n.$$

  Now, by definition, each a_k and b_ℓ will have $a_k \in \operatorname{cont}(f)$ and $b_\ell \in \operatorname{cont}(g)$ so that $a_kb_\ell \in \operatorname{cont}(f)\operatorname{cont}(g)$. In particular all coefficients of fg live in $\operatorname{cont}(f)$ and $\operatorname{cont}(g)$, so $\operatorname{cont}(fg) \subseteq \operatorname{cont}(f)\operatorname{cont}(g)$.

- The other inclusion $\operatorname{cont}(f)\operatorname{cont}(g) \subseteq \operatorname{rad}\operatorname{cont}(fg)$ is harder. Note that, by Proposition 2.138,

$$\operatorname{rad}\operatorname{cont}(fg) = \bigcap_{\operatorname{cont}(fg)\subseteq\mathfrak{p}} \mathfrak{p}.$$

  Thus, to show that $\operatorname{cont}(f)\operatorname{cont}(g) \subseteq \operatorname{rad}\operatorname{cont}(fg)$, we will show that $\operatorname{cont}(f)\operatorname{cont}(g) \subseteq \mathfrak{p}$ for each prime $\mathfrak{p}$ containing $\operatorname{cont}(fg)$.

  The key trick is to work in $R/\mathfrak{p}$. Let $\overline{p}$ denote the image of some $p \in R[x]$ along $R[x] \to (R/\mathfrak{p})[x]$. (Importantly, the map $R[x] \to (R/\mathfrak{p})[x]$ merely mods coefficients.) Because $\operatorname{cont}(fg) \subseteq \mathfrak{p}$, all the coefficients of fg live in $\mathfrak{p}$, so

$$\overline{f}\cdot\overline{g} = \overline{fg} = 0$$

  in $(R/\mathfrak{p})[x]$. But now we see that $R/\mathfrak{p}$ is an integral domain, so $(R/\mathfrak{p})[x]$ is also an integral domain!

  So without loss of generality, we take $\overline{f} = 0$ in $(R/\mathfrak{p})[x]$, so all the coefficients of f live in $\mathfrak{p}$, so $\operatorname{cont}(f) \subseteq \mathfrak{p}$, so $\operatorname{cont}(f)\operatorname{cont}(g) \subseteq \mathfrak{p}$. This finishes. ■

Remark 3.6 (Nir). The above proof actually gave us something which looks a little stronger: for each $\mathfrak{p}$ containing $\operatorname{cont}(fg)$, we have $\operatorname{cont}(f) \subseteq \mathfrak{p}$ or $\operatorname{cont}(g) \subseteq \mathfrak{p}$.

Remark 3.7 (Nir). Here is one way to view Gauss's lemma: if $\mathfrak{p}$ is a prime ideal in R, then $\mathfrak{p}R[x]$ remains prime in $R[x]$. Namely, if $fg \in \mathfrak{p}R[x]$, then $\operatorname{cont}(fg) \subseteq \mathfrak{p}$, so Remark 3.6 forces $\operatorname{cont}(f) \subseteq \mathfrak{p}$ or $\operatorname{cont}(g) \subseteq \mathfrak{p}$. In other words, $f \in \mathfrak{p}R[x]$ or $g \in \mathfrak{p}R[x]$.

Remark 3.8 (Nir). Additionally, when R is an integral domain the units of $R[x]$ are precisely the units in $R[x]$. Certainly any unit in R will remain a unit in $R[x]$ because the inverse lives in $R \subseteq R[x]$. However, if $u \in R[x]$ is a unit with inverse v, then the equation $uv = 1$ forces $\deg u = \deg v = 0$, so $u, v \in R$, so $u \in R^\times$.

Now, the key to getting unique factorization in $R[x]$ is to get it via unique factorization in $K[x]$, where $K := \operatorname{Frac}(R)$ is the field of fractions. In particular, recall $K[x]$ is a unique factorization domain because it is a Euclidean domain (see Example 1.32).

Our next step is to create a weak classification of irreducibles in $R[x]$.

Lemma 3.9. Fix R a unique factorization domain. Then if f is a nonconstant irreducible in $R[x]$, then f is irreducible in $K[x]$.

Proof. Fix some nonconstant $f(x)$. We proceed by contraposition; taking f not irreducible in $K[x]$ and showing that it is not irreducible in $R[x]$. Well, in this case we can write $f = g_0h_0$ for some $g_0, h_0 \in K[x]$, where $0 < \deg g_0, \deg h_0 < \deg f$. (Note this factorization exists because f remains not a unit in $K[x]$ because the units in $K[x]$ are constants by Remark 3.8.)

Now we move back to $R[x]$. Callously, let $a \in R$ (respectively, $b \in R$) be the product of all the denominators of all the coefficients of g_0 (respectively, h_0) so that $g := ag_0$ and $h := bh_0$ live in $R[x]$. Then we set $r := ab$, which gives

$$rf = gh$$

where $g, h \in R[x]$. Now that we're in $R[x]$, we can talk about the content. To set up our discussion, we use the fact that R is a unique factorization domain to write

$$r = u\prod_{k=1}^{n} \pi_k$$

for some $u \in R^\times$ and some (not necessarily distinct) irreducibles π_k.

Note that if $n = 0$, then $r = u$ is a unit, so we get the factorization $f = (g/u)h$ in $R[x]$, which witnesses f not being irreducible. (In particular, g/u and h are not units by Remark 3.8.) So we claim that we can find some triple (r, g, h) consisting of elements $r \in R$ and $g, h \in R[x]$ where $rf = gh$ and $n = 0$. Because we already have such an example, we choose r to have minimal n.

To finish, suppose for the sake of contradiction[1] $n > 1$ so that r is divisible by the irreducible element π_n. Because R is a unique factorization domain, Remark 1.31 tells us (π_n) is prime. So by Remark 3.6, we see $gh \in (\pi_1)R[x]$ implies $\operatorname{cont}(gh) \in (\pi_1)$ implies

$$\operatorname{cont}(g) \subseteq (\pi_n) \qquad \text{or} \qquad \operatorname{cont}(h) \subseteq (\pi_n).$$

So without loss of generality, we take $\operatorname{cont}(g) \subseteq (\pi_1)$, so all coefficients of f are divisible by π_n, so $g/\pi_n \in R[x]$, so we can write

$$(r/\pi_n)f = (g/\pi_n)h,$$

so we have a triple $(r/\pi_n, g/\pi_n, h)$ where r/π_n has strictly fewer irreducibles than r. This contradicts the minimality of r, finishing. ■

We can extend our classification to show that all irreducibles are prime in $R[x]$.

[1] It is possible to remove the contradiction by doing induction on n, showing that "for any n, there exists a triple (r, g, h) where r is a unit."

Remark 3.10 (Nir). Taking R to be an integral domain, we note $\pi \in R$ an irreducible in R will remain irreducible in $R[x]$. Indeed, degrees add in integral domains, so if $f, g \in R[x]$ have $fg = \pi$, then $\deg f = \deg g = 0$, so $f, g \in R$. In particular, $\pi = fg$ now forces one of f or g to be a unit in R and hence a unit in $R[x]$.

Lemma 3.11. Fix R a unique factorization domain. If f is irreducible in $R[x]$, then either

- f is a constant irreducible in R, or
- f is a (nonconstant) irreducible in $K[x]$, and $\operatorname{cont}(f) \not\subseteq (\pi)$ for any irreducible $\pi \in R$.

In either case, f is prime in $R[x]$.

Proof. Observe that, if f is a constant, then f will be irreducible in R automatically: writing $f = ab$ for any $a, b \in R$ forces one of a or b to be a unit in $R[x]$ and hence in R (see Remark 3.8). So because R is a unique factorization domain, Remark 1.31 gives (f) is prime in R, so Remark 3.7 gives (f) is prime in $R[x]$ as well.

Otherwise, f is a nonconstant irreducible in $R[x]$. Thus, it is irreducible and hence prime in $K[x]$ by Lemma 3.9. In particular, if $f \mid gh$ in $R[x]$ for $g, h \in R[x]$, then $f \mid gh$ in $K[x]$ as well (namely, the quotient lives in $R[x] \subseteq K[x]$), but because f is prime in $K[x]$, we see $f \mid g$ or $f \mid h$ in $K[x]$.

Without loss of generality take $f \mid g$; setting $fq_0 = g$, we can let r be the product of the denominators of q_0 (note $r \neq 0$) so that $q := rq_0 \in R[x]$ and gives

$$fq = rg.$$

We will now argue akin to Lemma 3.9 to show that $f \mid g$. In particular, we have found some pair $(r, q) \in (R \setminus \{0\}) \times R[x]$ such that $fq = rg$, we can find an r with minimal number of irreducible factors in its factorization into irreducibles.

Note that if r is divisible by no irreducibles, then this will imply that r's factorization into irreducibles merely consists of a unit, so $r \in R^\times$. In particular,

$$f(q/r) = g,$$

where $q/r \in R[x]$, implying $f \mid g$ in $R[x]$. This finishes the primality check for f.

Otherwise, suppose for the sake of contradiction $\pi \mid r$ for some irreducible in $\pi \in R$. Then (π) is a prime ideal by Remark 1.31, so Remark 3.6 tells us that $\operatorname{cont}(fq) \subseteq (\pi)$ implies

$$\operatorname{cont}(f) \subseteq (\pi) \qquad \text{or} \qquad \operatorname{cont}(q) \subseteq (\pi).$$

We take the cases separately.

- In the case where $\operatorname{cont}(q) \subseteq (\pi)$, we see $q/\pi \in R[x]$, so we could write
  $$f(q/\pi) = (r/\pi)g$$
  to create an (r, q) pair with strictly fewer irreducibles in r, thus violating the minimality of r.
- In the case where $\operatorname{cont}(f) \subseteq (\pi)$, we see $f/\pi \in R[x]$, so $f = \pi \cdot f/\pi$ provides a factorization of r into non-units: the only units of $R[x]$ are $R^\times$ by Remark 3.8, but $\pi \in R \setminus R^\times$ and $f \notin R$. So this contradicts the irreducibility of f.

We remark that the argument at the end of the second case actually shows that $\operatorname{cont}(f) \not\subseteq (\pi)$ for any irreducible $\pi \in R$. ■

Remark 3.12 (Nir). In fact, Lemma 3.11 is sharp: if $f \in R[x]$ is an irreducible in R, then f remains irreducible in $R[x]$ by Remark 3.10.

Otherwise, if $f \in R[x]$ is an irreducible in $K[x]$ with $\operatorname{cont}(f) \not\subseteq (\pi)$ for each irreducible $\pi \in R$, then if we factor $f = gh$ where $g, h \in R[x]$, irreducibility in $K[x]$ forces $\deg g = 0$ or $\deg h = 0$, so without loss of generality $\deg g = 0$. But no irreducible π may divide g because then it would divide f, giving $\operatorname{cont}(f) \subseteq (\pi)$.

The above lemma finishes the proof by Remark 1.30: $R[x]$ is Noetherian by Theorem 1.42 and so satisfies the ascending chain condition on principal ideals, and all irreducibles are prime in $R[x]$ by the above lemma. ■

Remark 3.13 (Nir). The above working out was extraordinarily annoying.

Corollary 3.14. The ring $k[x_1, \ldots, x_n]$ is a unique factorization domain.

Proof. We induct on n: when $n = 0$, we note that fields vacuously have unique factorization. The inductive step is to show that $k[x_1, \ldots, x_{n-1}][x_n]$ has unique factorization from $k[x_1, \ldots, x_{n-1}]$, which is precisely Theorem 3.1. ■

Example 3.15. We show that $\left(y^2 - x^3\right) \subseteq k[x, y]$ is prime. Because $k[x, y]$ is a unique factorization domain, it suffices to show that $y^2 - x^3$ is irreducible in $k[x, y] = k[x][y]$, for which it suffices to show that $y^2 - x^3$ is irreducible in $k(x)[y]$ by Remark 3.12.

But $y^2 - x^3$ is a quadratic in $k(x)[y]$ and therefore irreducible because it has no roots: there is no $y = f(x)/g(x)$ such that $f(x)^2/g(x)^2 = x^3$ because this gives

$$f(x)^2 = x^3 g(x)^2,$$

which fails by degree arguments. Namely, $f, g \neq 0$, and $\deg\left(f(x)^2\right)$ is even while $\deg\left(x^3 g(x)^2\right)$ is odd.

Example 3.16. We show that $\left(y^2 - x^3\right) \subseteq k[x, y]$ is prime a different way. Indeed, by sending $x \mapsto t^2$ and $y \mapsto t^3$, there is an embedding

$$\frac{k[x, y]}{\left(y^2 - x^3\right)} \hookrightarrow k\left[t^2, t^3\right]$$

by a homework problem. So the quotient is a domain, so $\left(y^2 - x^3\right)$ is prime.

3.1.2 The Cayley–Hamilton Theorem

Here is the main result we are going to prove.

Theorem 3.17. Fix R a ring and $A \in R^{n \times n}$ a matrix. Further, define $p_A(x) := \det(xI - A) \in R[x]$. Then $p_A(A) = 0^{n \times n} \in R^{n \times n}$, where $p_A(A)$ is evaluated by the ring homomorphism $R[x] \to R^{n \times n}$ by $r \mapsto rI$ and $x \mapsto A$.

Note in particular that the ring homomorphism $R[x] \to R^{n \times n}$ is legal because it is actually outputting in the R-subalgebra of $R^{n \times n}$ generated by A, which is a commutative ring because it is essentially a polynomial ring with coefficients rI. We will make the statement more precise in the proof.

Remark 3.18. Theorem 3.17 is usually stated in linear algebra for matrices over a field, but it is a purely algebraic result, so there is no reason to believe it shouldn't hold for arbitrary rings.

Proof of Theorem 3.17. We need to pick up the following definition for a technical trick at the end.

Definition 3.19 (Cofactor matrix)**.** Fix $A \in R^{n\times n}$. Then we define the *cofactor matrix* by

$$C_{ij} \coloneqq (-1)^{i+j} \det A_{i,j},$$

where $A_{i,j}$ is the matrix A where the ith row and jth column have been removed.

Example 3.20. Set

$$A = \begin{bmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{bmatrix}.$$

Then

$$C = \begin{bmatrix} a_{22} & -a_{21} \\ -a_{12} & a_{11} \end{bmatrix}.$$

Then we can compute

$$C^\intercal A = \begin{bmatrix} a_{22} & -a_{12} \\ -a_{21} & a_{11} \end{bmatrix}\begin{bmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{bmatrix} = \begin{bmatrix} a_{11}a_{22} - a_{21}a_{12} & a_{12}a_{22} - a_{22}a_{12} \\ -a_{11}a_{21} + a_{21}a_{11} & -a_{12}a_{21} + a_{22}a_{11} \end{bmatrix} (\det A)I.$$

The key fact of the cofactor matrix is that it "almost inverts" A, as in the above example.

Lemma 3.21. Fix $A \in R^{n\times n}$ with cofactor matrix C. Then $C^\intercal A = (\det A)I$.

Proof. This is essentially Cramér's rule. Give A coefficients by $A = (a_{ij})_{i,j=1}^n$, and fix some indices i and k. We can compute that

$$(C^\intercal A)_{ik} = \sum_{j=1}^n (C^\intercal)_{ij}\, a_{jk} = \sum_{j=1}^n (C)_{ji} a_{jk} = \sum_{j=1}^n (-1)^{i+j} a_{jk} \det A_{ji},$$

which upon expanding A_{ji} looks like

$$(C^\intercal A)_{ik} = \sum_{j=1}^n (-1)^{i+j} a_{jk} \det \begin{bmatrix} a_{11} & \cdots & a_{1,i-1} & a_{1,i+1} & \cdots & a_{1n} \\ \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ a_{j-1,1} & \cdots & a_{j-1,i-1} & a_{j-1,i+1} & \cdots & a_{j-1,n} \\ a_{j+1,1} & \cdots & a_{j+1,i-1} & a_{j+1,i+1} & \cdots & a_{j+1,n} \\ \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ a_{n1} & \cdots & a_{n,i-1} & a_{n,i+1} & \cdots & a_{nn} \end{bmatrix} \tag{$*$}$$

To compute this sum, we consider the matrix

$$A' \coloneqq \begin{bmatrix} a_{11} & \cdots & a_{1,i-1} & a_{1k} & a_{1,i+1} & \cdots & a_{1n} \\ \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots \\ a_{n1} & \cdots & a_{n,i-1} & a_{nk} & a_{n,i+1} & \cdots & a_{nn} \end{bmatrix}.$$

In particular, A' is equal to the matrix A where the ith column has been replaced with the kth column. The point is that applying Cramér's rule to compute $\det A'_j$ along the red column gives exactly the right-hand side of $(*)$.

We now have two cases.

- If $i = k$, then the substitution process used to get A' from A doesn't actually do anything (we replace a row with itself), so $\det A' = \det A$. Thus, $(C^\intercal A)_i = \det A$ for each i.

- If $i \neq k$, then the substitution process used to get A' will force A' to have two distinct columns equal to the kth column, which forces $\det A' = 0$. To be explicit, A' looks like

$$A' := \begin{bmatrix} a_{11} & \cdots & a_{1,i-1} & a_{1k} & a_{1,i+1} & \cdots & a_{1,k-1} & a_{1k} & a_{1,k+1} & \cdots & a_{1n} \\ \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots \\ a_{n1} & \cdots & a_{n,i-1} & a_{nk} & a_{n,i+1} & \cdots & a_{n,k-1} & a_{nk} & a_{n,k+1} & \cdots & a_{1n} \end{bmatrix}.$$

  (The above representation technically assumes $i < k$, but there is a similar diagram for $k < i$.) Subtracting the ith column from the kth column gives

$$\begin{bmatrix} a_{11} & \cdots & a_{1,i-1} & a_{1k} & a_{1,i+1} & \cdots & a_{1,k-1} & 0 & a_{1,k+1} & \cdots & a_{1n} \\ \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots \\ a_{n1} & \cdots & a_{n,i-1} & a_{nk} & a_{n,i+1} & \cdots & a_{n,k-1} & 0 & a_{n,k+1} & \cdots & a_{1n} \end{bmatrix}.$$

  Doing this column subtraction does not change $\det A'$, but now we can expand along the highlighted column to see that $\det A' = 0$.

Synthesizing the above two cases, we see that $(C^\intercal A)_{ik} = (\det A)1_{i=k} = (\det A)I_{ik}$, so $C^\intercal A = (\det A)I$, which is what we wanted. ■

We now return to the proof.

Warning 3.22. The details in the below proof are somewhat technical because they have to do with matrices. I apologize, but I hope that at least the exposition is clear even if wordy.

The main idea is that we would actually like to substitute $x = A$ into $p_A(x) = \det(xI - A)$, but this does not currently make sense because xI needs to be a scalar-matrix multiplication.

So the key trick is to consider the elements of R as living in $\operatorname{End}_R(R^n)$, alongside with A. For convenience, given R^n the standard basis $e_1, \ldots, e_n$, and give A coefficients by $A = (a_{ij})_{i,j=1}^n$. We have two steps.

- On one hand, we define $\varphi \in \operatorname{End}_R(R^n)$ to correspond to A by

$$\varphi(e_j) = Ae_j = \begin{bmatrix} a_{11} & \cdots & a_{1n} \\ \vdots & \ddots & \vdots \\ a_{n1} & \cdots & a_{nn} \end{bmatrix} e_j = \sum_{i=1}^n a_{ij} e_i.$$

  Because R^n is freely generated by the $e_\bullet$, these equations uniquely determine the R-module homomorphism φ.

- On the other hand, we note that the action of $r \in R$ on R^n defined by $(x_1, \ldots, x_n) \mapsto (rx_1, \ldots, rx_n)$ defines an R-module endomorphism which we name $\mu(r) \in \operatorname{End}_R(R^n)$. In fact, the function $\mu : R \to \operatorname{End}_R(R^n)$ is a ring homomorphism: for any $r, s \in R$ and $v \in R^n$, we see

$$\mu(rs)(v) = (rs)(v) = r(sv) = \mu(r)(\mu(s)v) = (\mu(r) \circ \mu(s))(v),$$

  and

$$\mu(r+s)(v) = (r+s)v = rv + sv = \mu(r)(v) + \mu(s)(v) = (\mu(r) + \mu(s))(v).$$

Thus, we see that we can define a ring homomorphism $\mu : R[x] \to \operatorname{End}_R(R^n)$ by lifting the ring homomorphism $\mu : R \to \operatorname{End}_R(R^n)$ and sending $x \mapsto \varphi$; let this image be $\mu(R)[\varphi]$. For technicality reasons, we quickly note that $\mu(R)[\varphi]$ is a commutative ring[2] because, for any $\mu(f), \mu(g) \in \mu(R)[\varphi]$, we have

$$\mu(f)\mu(g) = \mu(fg) = \mu(gf) = \mu(g)\mu(f).$$

So we have indeed pushed both A and elements of R onto equal footing in $\mu(R)[\varphi]$.

[2] We need to say this in order to take determinants in $\mu(R)[\varphi]$ later because determinants only make sense in commutative rings.

We now attack the proof more directly. We are interested in showing that $p_A(A) = 0^{n\times n} \in R^{n\times n}$. To use the machinery we've developed, we should move this statement into $\mu(R)[\varphi]$. After fully expanding out the determinant $p_A(x) = \det(xI - A) \in R[x]$, we can write out the coefficients

$$p_A(x) = \sum_{k=0}^{n} p_k x^k.$$

Plugging in $x = A$, we are interested in showing that

$$\sum_{k=0}^{n} p_k A^k \stackrel{?}{=} 0^{n\times n}.$$

This is equivalent to showing that

$$\sum_{k=0}^{n} p_k \left(A^k e_j\right) = \left(\sum_{k=0}^{n} p_k A^k\right) e_j \stackrel{?}{=} 0 \in R^n$$

for each basis vector e_j. By definition, we see that $\varphi(e_j) = Ae_j$, so inductively, $A^k e_j = \varphi e_j$. With this in mind, we push in $\mu(R)[\varphi]$ by writing

$$\sum_{k=0}^{n} p_k \left(A^k e_j\right) = \sum_{k=0}^{n} p_k \varphi^k(e_j) = \left(\sum_{k=0}^{n} p_k \varphi^k\right) e_j = \left(\sum_{k=0}^{n} \mu(p_k)\mu(x)\right) e_j = \mu\left(\sum_{k=0}^{n} p_k x^k\right) e_j = \mu(p_A(x))e_j.$$

Showing that $\mu(p_A(x))e_j = 0 \in R^n$ for each e_j is equivalent to showing that $\mu(p_A(x)) = 0 \in \operatorname{End}_R(R^n)$. We note that this is pretty close to literally plugging in A into p_A, but instead we have to plug in φ.

Indeed, we can undo all the determinant expansion for p_A to push the μ inside. Namely, working in $\mu(R)[\varphi]$, the determinant is just a very large polynomial in its coordinates, and polynomials commute with ring homomorphisms, so we can write

$$\begin{aligned}
\mu(p_A(x)) &= \mu\left(\det\begin{bmatrix} x - a_{11} & -a_{12} & \cdots & -a_{1n} \\ -a_{21} & x - a_{22} & \cdots & -a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ -a_{n1} & -a_{n2} & \cdots & x - a_{nn}\end{bmatrix}\right) \\
&= \det\begin{bmatrix} \mu(x - a_{11}) & \mu(-a_{12}) & \cdots & \mu(-a_{1n}) \\ \mu(-a_{21}) & \mu(x - a_{22}) & \cdots & \mu(-a_{2n}) \\ \vdots & \vdots & \ddots & \vdots \\ \mu(-a_{n1}) & \mu(-a_{n2}) & \cdots & \mu(x - a_{nn})\end{bmatrix} \\
&= \det\underbrace{\begin{bmatrix} \varphi - \mu(a_{11}) & -\mu(a_{12}) & \cdots & -\mu(a_{1n}) \\ -\mu(a_{21}) & \varphi - \mu(a_{22}) & \cdots & -\mu(a_{2n}) \\ \vdots & \vdots & \ddots & \vdots \\ -\mu(a_{n1}) & -\mu(a_{n2}) & \cdots & \varphi - \mu(a_{nn})\end{bmatrix}}_{\varphi\mu(I)-\mu(A)}.
\end{aligned}$$

Here, $\varphi\mu(I)-\mu(A)$ is abuse of notation, but it will do. The point is that, indeed, we have basically just plugged in $x = A$ into the determinant.

Warning 3.23. The matrix $\varphi\mu(I) - \mu(A)$ is a matrix whose entire are endomorphisms, not elements of R. Explicitly, $\varphi\mu(I) - \mu(A) \in \operatorname{End}_R(R^n)^{n\times n}$.

To show that $\det(\varphi\mu(I) - \mu(A)) = 0$, we note that $\varphi\mu(I) - \mu(A)$ will vanish on the vector $(\pi_1, \ldots, \pi_n) \in \operatorname{Mor}_{\text{Set}}(R^n, R^n)^n$, where π_k is the function which outputs e_k.[3] (The $\pi_\bullet$ is how we are bringing the basis vectors

[3] Careful readers may object that our vector $(\pi_1, \ldots, \pi_n)$ does not live in $\mu(R)[\varphi]$, and so some linear algebra might not hold. However, we do not have to fear because are still working in an R-module, so we just need to make sure we never do anything that would require anything commuting with the $\pi_\bullet$.

$e_\bullet$ into our world of functions.) Indeed, the jth component of the expansion of

$$\begin{bmatrix} \varphi - \mu(a_{11}) & -\mu(a_{12}) & \cdots & -\mu(a_{1n}) \\ -\mu(a_{21}) & \varphi - \mu(a_{22}) & \cdots & -\mu(a_{2n}) \\ \vdots & \vdots & \ddots & \vdots \\ -\mu(a_{n1}) & -\mu(a_{n2}) & \cdots & \varphi - \mu(a_{nn}) \end{bmatrix}^\intercal \begin{bmatrix} \pi_1 \\ \pi_2 \\ \vdots \\ \pi_n \end{bmatrix}$$

is (note the transpose!)

$$\sum_{i=1}^n (\varphi 1_{i=j} - \mu(a_{ij}))\pi_i = \varphi\pi_j - \sum_{i=1}^n \mu(a_{ij})\pi_i.$$

Evaluating this on any $v \in R^n$, we see $\pi_i v = e_i$ so that

$$\left(\varphi\pi_j - \sum_{i=1}^n \mu(a_{ij})\pi_i\right) v = \varphi(e_j) - \sum_{i=1}^n a_{ij}e_i,$$

which vanishes by the definition of φ. (We needed to use the transpose in the above argument in order to make the above equation actually vanish by definition of φ.)

Thus,

$$(\varphi\mu(I) - \mu(A))^\intercal \begin{bmatrix} \pi_1 \\ \vdots \\ \pi_n \end{bmatrix} = \begin{bmatrix} 0 \\ \vdots \\ 0 \end{bmatrix}.$$

Multiplying on the left by the transpose of the cofactor matrix (!) of $(\varphi\mu(I) - \mu(A))^\intercal$, Lemma 3.21 gives

$$\det\left((\varphi\mu(I) - \mu(A))^\intercal\right) \begin{bmatrix} \pi_1 \\ \vdots \\ \pi_n \end{bmatrix} = \begin{bmatrix} 0 \\ \vdots \\ 0 \end{bmatrix}.$$

Thus, $\det\left((\varphi\mu(I) - \mu(A))^\intercal\right)\pi_j = 0$ for each π_j, so $\det\left((\varphi\mu(I) - \mu(A))^\intercal\right)e_j = 0$ for each e_j after pushing e_j through. So $\det(\varphi\mu(I) - \mu(A)) = \det\left((\varphi\mu(I) - \mu(A))^\intercal\right) = 0$ This finishes the (very long) proof. ■

3.1.3 Applying the Cayley–Hamilton Theorem

Our use of Theorem 3.17 in commutative algebra will be via the following form.

Theorem 3.24. Fix M a finitely generated R-module with n generators. Further, fix $\varphi \in \operatorname{End}_R(M)$. Then there exists some monic polynomial

$$p_\varphi(x) = x^n + p_1x^{n-1} + \cdots + p_n$$

of degree n such that $p_\varphi(\varphi)$ is zero. In fact, if there is an ideal $I \subseteq R$ such that $IM = M$, then we can choose $p_k \in I^k$.

Proof. Note that we may assume such an ideal I exists because certainly $I = R$ works. Let $\{m_1, \ldots, m_n\}$ generate M so that we can conjure constants a_{ij} by

$$\varphi(m_j) = \sum_{i=1}^n a_{ij}m_i \tag{$*$}$$

to give a matrix form for φ, by $A := (a_{ij})_{i,j=1}^n \in R^{n\times n}$; namely, $\varphi(m_j) = Am_j$ for each m_j, by definition of matrix-vector multiplication. This lets us apply Theorem 3.17 to get some polynomial $p_A(x) := \det(xI^{n\times n} - A)$ such that $p_A(A) = 0^{n\times n}$. To be explicit, let

$$p_A(x) = \sum_{k=0}^n r_kx^k.$$

Then, for any m_j, we see that $\varphi m_j = A m_j$

$$p_A(\varphi)(m_j) = \sum_{k=0}^{n} r_k \varphi^k m_j = \sum_{k=0}^{n} r_k A^k m_j = p_A(A) m_j = 0,$$

so $p_A(\varphi)$ vanishes on each of the m_j and therefore is the zero morphism.

We now stare harder at the coefficients of $p_A(x)$ to get the second statement; suppose $I \subseteq R$ with $IM = M$ (certainly some I exists because $I = R$ suffices). As some technical set-up, each m_k generating M has some $x_k \in I$ and $m_k' \in M_k$ such that $m_k = x_k m_k'$. So because the $m_\bullet$ generate M over R, we see

$$M = Rm_1 + \cdots + Rm_n = Rx_1 m_1' + \cdots + Rx_2 m_2' \subseteq Im_1' + \cdots + Im_n',$$

so all elements in M can be written as an I-linear combination of the $\{m_1', \ldots, m_n'\}$. In particular, if we run the above argument again, the matrix representation from ($*$) can have all elements in I, so $A \in I^{n\times n}$. Then the polynomial p_A we generate will be

$$p_A(x) = \det \begin{bmatrix} x - a_{11} & -a_{12} & \cdots & -a_{1n} \\ -a_{21} & x - a_{22} & \cdots & -a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ -a_{n1} & -a_{n2} & \cdots & x - a_{nn} \end{bmatrix} = \sum_{\sigma \in S_n} \left(\prod_{k=1}^{n} (1_{k=\sigma k} x - a_{k,\sigma k}) \right),$$

where we have expanded out the determinant in the last step by hand. After a full expansion, we see that the leading term will be $1x^n$, coming from the $\sigma = \mathrm{id}$ term only. As for the other coefficients, the coefficient p_d of x^{n-d} only occurs when we choose $n-d$ terms of x from the product, leaving d terms of $-a_{k,\sigma k} \in I$ left over to multiply, so $p_d \in I^d$. This finishes. ■

Let's now see an application.

Proposition 3.25. Let M be a finitely generated R-module and $\psi \in \mathrm{End}_R(M)$. Then if ψ is surjective, then ψ is an isomorphism.

Proof. The key trick is to give M an $R[t]$-module structure to M by defining $R[t] \to \mathrm{End}_R(M)$ by lifting the given ring map $R \to \mathrm{End}_R(M)$ and sending $t \mapsto \psi$. (Note M is a finitely generated R-module and hence a finitely generated $R[t]$-module.) In particular, by Theorem 3.24, we get some $p_{\mathrm{id}}(x) \in R[t][x]$ such that

$$p_{\mathrm{id}}(\mathrm{id}) = 0.$$

Further, because ψ is surjective, we see that $(t) \cdot M = M$: every $m \in M$ has some $m' \in M$ such that $tm = \psi(m') = m$, so $m \in tM \subseteq (t)M$. Thus, we can use Theorem 3.24 to write out

$$p_{\mathrm{id}}(x) = x^n + p_1 x^{n-1} + \cdots + p_n \in R[t][x],$$

where $p_d \in \left(t^d\right)$ for each d.

Remark 3.26 (Nir)**.** It may look like conjuring p_{id} shouldn't do anything because the characteristic polynomial for p_{id} should be $(x-1)^n$, where n is the number of generators for M. However, this previous sentence where we invoke Theorem 3.24 to force $p_d \in \left(t^d\right)$ is where we are inputting information about ψ.

In particular, plugging in $x = \mathrm{id}$, we see that

$$0 = \mathrm{id}^n + p_1 \mathrm{id}^{n-1} + \cdots + p_n = \mathrm{id} + t \cdot \underbrace{\left(\frac{p_1}{t} \mathrm{id}^{n-1} + \cdots + \frac{p_n}{t} \mathrm{id}^0 \right)}_{q(t)}$$

in $\mathrm{End}_R(M)$. It follows that t is invertible with inverse $q(t)$. Defining $\varphi := -q(t)$, we see from the above that $\varphi\psi = \psi\varphi = \mathrm{id}$, so φ and ψ are inverses. ■

Remark 3.27. Proposition 3.25 need not be true even in vector spaces which are not finitely generated. For example, fixing a field k, consider

$$V := \bigoplus_{i=1}^{\infty} kv_i$$

for some vectors $\{v_i\}_{i=1}^{\infty}$. Then we have the surjective map defined by $v_1 \mapsto 0$ and $v_i \mapsto v_{i-1}$ for $i > 1$, and this is not an isomorphism because it has kernel.

Remark 3.28. The analogous version of Proposition 3.25 need not be true for injections giving isomorphisms. For example, $\mathbb{Z} \to 2\mathbb{Z} \hookrightarrow \mathbb{Z}$ is injective but not an isomorphism.

Here is a quick corollary to Proposition 3.25.

Corollary 3.29. Fix m and n positive integers. If we have an isomorphism of R-modules, $R^n \cong R^m$, then $m = n$.

Proof. Without loss of generality take $n \ge m$. Then we use the canonical projection $R^n \twoheadrightarrow R^m$ defined by $(x_1, \ldots, x_n) \mapsto (x_1, \ldots, x_m)$ to construct a surjective map

$$R^m \cong R^n \twoheadrightarrow R^m,$$

which must be an isomorphism by Proposition 3.25. However, if $n > m$, then the map $R^n \twoheadrightarrow R^m$ by projection has nontrivial kernel (e.g., $(1_{k>m})_{k=1}^n \in R^n$), so the composite $R^m \cong R^n \twoheadrightarrow R^m$ would have nontrivial kernel (e.g., take the pre-image of $(1_{k>m})_{k=1}^n \in R^n$ under $R^m \cong R^n$), which is a contradiction. So we must have $n = m$. ■

3.1.4 Nakayama's Lemma

To ready our discussion of Nakayama's lemma, we recall the following definition.

Definition 3.30 (Jacobson radical)**.** Fix a ring R. Then we define the *Jacobson radical* by

$$\operatorname{rad} R := \bigcap_{\mathfrak{m}} \mathfrak{m}.$$

Here is the main fact about $\operatorname{rad} R$ that we will need.

Lemma 3.31. Fix R a ring. Then $r \in \operatorname{rad} R$ if and only if $1 - rs \in R^\times$ for each $s \in R$.

Proof. We take our implications separately.

- In one direction, suppose that $r \in R$ has $r \in \operatorname{rad} R$, and pick up any $s \in R$. Then, for each maximal ideal $\mathfrak{m} \subseteq$, we see $r \in \mathfrak{m}$ and so $rs \in \mathfrak{m}$ while $1 \notin \mathfrak{m}$, so $1 - rs \notin \mathfrak{m}$. Thus, the ideal $(1 - rs)$ is not contained in any maximal ideal, so we must have $(1 - rs) = R$, so there exists $u \in R$ such that $(1 - rs)u = (1)$, so $1 - rs \in R^\times$.
- In the other direction, suppose that $r \notin \operatorname{rad} R$ so that there exists a maximal ideal $\mathfrak{m}$ such that $r \notin \mathfrak{m}$. It follows that $[r]_\mathfrak{m} \ne [0]_\mathfrak{m} \in R/\mathfrak{m}$, so because $R/\mathfrak{m}$ is a field, there exists $[s]_\mathfrak{m} \in R/\mathfrak{m}$ with

$$[1 - rs]_\mathfrak{m} = [1]_\mathfrak{m} - [r]_\mathfrak{m} \cdot [s]_\mathfrak{m} = [0]_\mathfrak{m}.$$

  In particular, $1 - rs \in \mathfrak{m}$, so $(1 - rs) \subseteq \mathfrak{m}$, so $1 \notin (1 - rs)$, so $1 - rs$ is not a unit. ■

Remark 3.32. We will mostly use the Jacobson radical in the context where R is a local ring so that $\operatorname{rad} R = \mathfrak{m}$, where $\mathfrak{m}$ is the unique maximal ideal of R.

Here is our result.

Theorem 3.33 (Nakayama's lemma)**.** Fix R a ring and an ideal $I \subseteq \operatorname{rad} R$. If M is a finitely generated R-module such that $IM = M$, then $M = 0$.

Proof. The main idea is in the following lemma.

Lemma 3.34. Fix R a ring and $I \subseteq R$ an ideal. If M is a finitely generated R-module such that $IM = M$, then there exists $r \in I$ with $(1-r)M = 0$.

Proof. The idea is, as usual, to use Theorem 3.24. Using $\operatorname{id} \in \operatorname{End}_R(M)$, the fact that $IM = M$ (!) gives us a polynomial

$$p_{\text{id}}(x) := x^n + p_1 x^{n-1} + \cdots + p_n \in R[x],$$

such that $p_{\text{id}}(\operatorname{id}) = 0$ and $p_k \in I^k$ for each p_k. But plugging in $x = \operatorname{id}$, we see

$$0 = p_{\text{id}}(\operatorname{id}) = \operatorname{id}^n + p_1 \operatorname{id}^{n-1} + \cdots + p_n \operatorname{id}^0 = \big(1 - (-p_1 - \cdots - p_n)\big)\operatorname{id}.$$

In particular, we set $r := -p_1 - \cdots - p_n \in I$ so that $(1-r)m = (1-r)\operatorname{id} m = 0$ for each $m \in M$. This finishes. ■

From this lemma the result directly follows because the promised $1 - r$ is a unit. Indeed, $IM = M$ promises $r \in I$ with $(1-r)M = 0$, and $r \in I \subseteq \operatorname{rad} R$ implies $1 - r \in R^\times$ by Lemma 3.31. So finding $u \in R$ with $u(1-r) = 1$, we see that each $m \in M$ has

$$m = 1m = u(1-r)m = u \cdot 0 = 0,$$

so $M = 0$ is forced. ■

Remark 3.35 (Nir)**.** The condition that M is finitely generated is necessary: in $k[x]_{(x)}$-modules, we see $\operatorname{rad} k[x]_{(x)} = (x)$ because $k[x]_{(x)}$ is local, but $(x) \cdot k(x) = k(x)$ while $k(x)$ is a nonzero $k[x]_{(x)}$-module. The analogous arithmetic example is with $\mathbb{Z}_2$-modules, where $(2) \cdot \mathbb{Q}_2 = \mathbb{Q}_2$ while $\mathbb{Q}_2 \neq 0$.

Let's see a quick application.

Corollary 3.36. Fix a ring R and an ideal $I \subseteq \operatorname{rad} R$. Further, suppose that M is a finitely generated R-module, and we have elements $m_1, \ldots, m_n \in M$. Then if the images $\overline{m_1}, \ldots, \overline{m_n}$ generate M/IM, then the original elements generate M.

Proof. Consider the R-submodule

$$M' := Rm_1 + \cdots + Rm_n \subseteq M.$$

We will show that $M = M'$ by showing $M/M' = 0$, for which we will use Theorem 3.33. Well, it suffices to show that $M/M' = I(M/M')$. To see this, fix any $m \in M$, and we want to find $x \in I$ and $m_0 \in M$ such that $[m]_{M'} = x \cdot [m_0]_{M'}$. Well, $\{[m_1]_I, \ldots, [m_n]_I\}$ generates M/IM, so there exists $r_1, \ldots, r_n$ such that

$$[m]_I = r_1[m_1]_I + \cdots + r_n[m_n]_I.$$

In particular, there is $x \in I$ and $m_0 \in M$ such that

$$m - (r_1 m_1 + \cdots + r_n m_n) = x m_0 \in IM,$$

so $[m]_{M'} = [xm_0]_{M'} = x \cdot [m_0]_{M'} \in I(M/M')$, which is what we wanted. ■

Remark 3.37 (Nir)**.** Again, the initial hypothesis that M is finitely generated is necessary. The same examples as in Remark 3.35 will work because $IM = M$ means that the empty set will generate M/IM but will not generate M with $M \neq 0$.

3.1.5 Support of Tensor Products

Let's see another application of Theorem 3.33: we can finally close the books on Remark 2.89.

Proposition 3.38. Fix R a local ring with M and N finitely generated R-modules. Then $M \otimes_R N = 0$ if and only if $M = 0$ or $N = 0$.

Proof. In one direction, if $M = 0$ or $N = 0$, then of course $M \otimes_R N = 0$. For example, if $M = 0$, then any generator $m \otimes n$ is just $0 \otimes n = (0 \cdot 0) \otimes n = 0(0 \times n) = 0 \otimes 0$.

The other direction is harder. Suppose that $M \neq 0$ with $M \otimes_R N = 0$, and we show that $N = 0$. Further, because R is local, we are promised a single maximal ideal $\mathfrak{m} \subseteq R$, and because this is the only maximal ideal, $\operatorname{rad} R = \mathfrak{m}$. The point is to use the right-exactness of $- \otimes_R N$ (and a healthy amount of Nakayama's lemma), so we begin by encoding $M \neq 0$ into a right-exact sequence.

In particular, $M \neq 0$ (and M is finitely generated!) requires that $M/\mathfrak{m}M \neq 0$ by Theorem 3.33, but $M/\mathfrak{m}M$ is now an $R/\mathfrak{m}$-vector space, with action by

$$[r]_\mathfrak{m} \cdot [m]_{\mathfrak{m}M} = [rm]_{\mathfrak{m}M}.$$

Namely, this is well-defined because $[r]_\mathfrak{m} = [s]_\mathfrak{m}$ implies that $r - s \in \mathfrak{m}$, so $([r]_\mathfrak{m} - [s]_\mathfrak{m}) \cdot [m]_{\mathfrak{m}M} = [(r - s)m]_{\mathfrak{m}M} = [0]_{\mathfrak{m}M}$.

But because $M/\mathfrak{m}M$ is a nonzero $R/\mathfrak{m}$-vector space, linear algebra lets us give $M/\mathfrak{m}M$ a basis over $R/\mathfrak{m}$, and so we have a projection map

$$M/\mathfrak{m}M \twoheadrightarrow R/\mathfrak{m}$$

by choosing any of the coordinates. Composing this projection with $M \twoheadrightarrow M/\mathfrak{m}M$, we have a right-exact sequence

$$\ker \pi \to M \stackrel{\pi}{\to} R/\mathfrak{m} \to 0.$$

To finish, we note that tensoring is right-exact and therefore preserves surjections. Thus, there is an induced surjection

$$N \otimes_R \ker \pi \to N \otimes_R M \stackrel{\pi}{\to} N \otimes_R (R/\mathfrak{m}) \to 0.$$

Now we can unravel. We know that $M \otimes_R N = 0$ by hypothesis, and $N \otimes_R (R/\mathfrak{m}) \cong N/\mathfrak{m}N$ by Proposition 2.96. So the end of our exact sequence is

$$0 \to N/\mathfrak{m}N \to 0,$$

so $N/\mathfrak{m}N = 0$. Thus, using that N is finitely generated, Theorem 3.33 tells us that $N = 0$. ■

Remark 3.39 (Nir)**.** The local condition is necessary: using Exercise 2.40, we see $\mathbb{Z}/3\mathbb{Z} \otimes_\mathbb{Z} \mathbb{Z}/4\mathbb{Z} \cong \mathbb{Z}/\gcd(3,4)\mathbb{Z} = 0$, but neither $\mathbb{Z}/3\mathbb{Z}$ nor $\mathbb{Z}/4\mathbb{Z}$ are zero.

Remark 3.40 (Nir)**.** The finitely generated condition is necessary: working with $\mathbb{Z}_{(2)}$-modules, we note that $\mathbb{Z}_{(2)}/2\mathbb{Z}_{(2)} = \mathbb{Z}/2\mathbb{Z}$ (by considering the kernel of $\mathbb{Z} \hookrightarrow \mathbb{Z}_{(2)} \twoheadrightarrow \mathbb{Z}_{(2)}/2\mathbb{Z}_{(2)}$), so

$$\mathbb{Q} \otimes_{\mathbb{Z}_{(2)}} \mathbb{Z}_{(2)}/2\mathbb{Z}_{(2)} \cong \mathbb{Q} \otimes_{\mathbb{Z}_{(2)}} \mathbb{Z}/2\mathbb{Z} \cong 0,$$

where the last congruence is because $\mathbb{Q}$ is divisible while $\mathbb{Z}/2\mathbb{Z}$ is torsion. Explicitly, any generator $q \otimes b \in \mathbb{Q} \otimes_{\mathbb{Z}_{(2)}} \mathbb{Z}/2\mathbb{Z}$ has $q \otimes b = (q/2) \otimes 2b = (q/2) \otimes 0 = 0$. But of course, $\mathbb{Q} \neq 0$ and $\mathbb{Z}_{(2)}/2\mathbb{Z}_{(2)} \cong \mathbb{Z}/2\mathbb{Z} \neq 0$.

We can even push beyond the local case by localizing.

Corollary 3.41. Fix R a ring with M and N finitely generated R-modules. Then $M \otimes_R N = 0$ if and only if $\operatorname{Ann} M + \operatorname{Ann} N = R$.

Proof. We take the directions independently.

- In one direction, suppose $\operatorname{Ann} M + \operatorname{Ann} N = R$, and we show $M \otimes_R N = 0$. Then we are promised some $a \in \operatorname{Ann} M$ and $b \in \operatorname{Ann} N$ such that $a + b = 1$. Then, for any generator $m \otimes n \in M \otimes_R N$, we see

$$m \otimes n = 1(m \otimes n) = (a+b)(m \otimes n) = (am) \otimes n + m \otimes (bn) = 0 \otimes n + m \otimes 0.$$

  But $0 \otimes n = (0 \cdot 0) \otimes n = 0 \otimes (0n) = 0 \otimes 0$, and similarly, $m \otimes 0 = m \otimes (0 \cdot 0) = (m \cdot 0) \otimes 0 = 0 \otimes 0$. Thus, $m \otimes n = 0 \otimes 0$, so $M \otimes_R N = 0$.

- For the other direction, we localize. Suppose that $I := \operatorname{Ann} M + \operatorname{Ann} N \subsetneq R$, and we show that $M \otimes_R N \neq 0$. Putting I in some maximal ideal $\mathfrak{m}$, we note that we can localize at $\mathfrak{m}$, where we see Corollary 2.103 gives

$$(M \otimes_R N)_{\mathfrak{m}} \cong M_{\mathfrak{m}} \otimes_{R_{\mathfrak{m}}} N_{\mathfrak{m}}.$$

  Now, by Proposition 2.75, we see that $\mathfrak{m} \supseteq I \supseteq \operatorname{Ann} M$ (respectively, $\mathfrak{m} \supseteq \operatorname{Ann} N$), so $\mathfrak{m} \in \operatorname{Supp} M$ (respectively, $\mathfrak{m} \in \operatorname{Ann} N$), so $M_{\mathfrak{m}} \neq 0$ (respectively, $N_{\mathfrak{m}} \neq 0$).

  So now that we are in the local case (note $R_{\mathfrak{m}}$ is local by Proposition 2.15), we see Proposition 3.38 tells us $M_{\mathfrak{m}} \otimes_{R_{\mathfrak{m}}} N_{\mathfrak{m}} \neq 0$. But surely $0_{\mathfrak{m}} \cong 0$, so we must have $M \otimes_R N \neq 0$ to localize to a nonzero module. This finishes. ■

Remark 3.42 (Nir)**.** The backward direction does not need M and N to be finitely generated. The forward direction does: note

$$\mathbb{Q} \otimes_{\mathbb{Z}} \mathbb{Z}/2\mathbb{Z} = 0$$

because $\mathbb{Q}$ is divisible while $\mathbb{Z}/2\mathbb{Z}$ is torsion. (Namely, any generator $q \otimes b = (q/2) \otimes 2b = (q/2) \otimes 0 = 0$ vanishes.) However, $\operatorname{Ann} \mathbb{Q} = \{0\}$ (because $\mathbb{Q}$ is a domain, $aq = 0$ implies $a = 0$ or $q = 0$), and $\operatorname{Ann} \mathbb{Z}/2\mathbb{Z} = 2\mathbb{Z}$ (by Example 2.78), so

$$\operatorname{Ann} \mathbb{Q} + \operatorname{Ann} \mathbb{Z}/2\mathbb{Z} = 0 + 2\mathbb{Z} = 2\mathbb{Z} \subsetneq \mathbb{Z}.$$

Anyways, let's finish off Remark 2.89.

Corollary 3.43. Fix M and N finitely generated R-modules. Then $\operatorname{Supp}(M \otimes_R N) = \operatorname{Supp} M \cap \operatorname{Supp} N$.

Proof. Fix a prime $\mathfrak{p}$. Then we see from Corollary 2.103 that

$$(M \otimes_R N)_{\mathfrak{p}} = M_{\mathfrak{p}} \otimes_{R_{\mathfrak{p}}} N_{\mathfrak{p}}.$$

Now, because $R_{\mathfrak{p}}$ is a local ring (by Proposition 2.15), we see $M_{\mathfrak{p}} \otimes_{R_{\mathfrak{p}}} N_{\mathfrak{p}}$ will vanish if and only if $M_{\mathfrak{p}} = 0$ or $N_{\mathfrak{p}} = 0$ by Proposition 3.38. In other words, $\mathfrak{p} \notin \operatorname{Supp}(M \otimes_R N)$ if and only if $\mathfrak{p} \notin \operatorname{Supp} M$ or $\mathfrak{p} \notin \operatorname{Supp} N$, which is the result. ■

3.1.6 Integrality Preview

We will spend the rest of class on the following result.

Proposition 3.44. Fix R a ring and an R-algebra generated by one element $s \in S$. Letting I be the kernel of $R[x] \to S$ by $x \mapsto s$ so that $S \cong R[x]/I$, we have the following equivalences.

(a) S is finitely generated as an R-module if and only if I contains a monic polynomial (i.e., there is some monic $p(x) \in R[x]$ such that $p(s) = 0$).

(b) S is a free, finitely generated R-module if and only if $I = (p)$ for some monic polynomial p. In fact, S is of rank $\deg p$.

Proof. Here is the proof of (a).

- If S is finitely generated as an R-module with n generators, we apply Theorem 3.24 with $\mu_s \in \operatorname{End}_R(S)$, where $\mu_s(m) := sm$. (This is an endomorphism because $s(r_1m_1 + r_2m_2) = r_1s(m_1) + r_2s(m_2)$.) In particular, Theorem 3.24 gives us some monic polynomial

$$p(x) = x^n + p_1x^{n-1} + \cdots + p_n$$

such that $p(\mu_s) = 0$. In particular, plugging in 1 into $p(\mu_s)$, we see that

$$0 = 0 \cdot 1 = \left(\mu_s^n + p_1\mu_s^{n-1} + \cdots + p_n\mu_s^0\right)(1) = s^n + p_1s^{n-1} + \cdots + p_n = p(s).$$

Under the isomorphism $R[x]/I \cong S$ by $x \mapsto s$, we thus note that $p(s) = 0$ implies that $[p]_I = [0]_I$ and $p \in I$ is forced. So I does contain a monic polynomial.

- In the other direction, suppose

$$p(x) := x^n + p_1x^{n-1} + \cdots + p_n \in R[x]$$

is a monic polynomial in I. Then we claim $\{1, s, s^2, \ldots, s^{n-1}\}$ will generate S as an R-module. To start, we notice that $S = R[s] \cong R[x]/I$ means that any element $m \in S$ can be written as

$$m = \sum_{k=0}^{\infty} a_ks^k$$

for some coefficients $a_\bullet \in R$, where all but finitely many vanish. Thus, to show that $m \in \sum_{i=0}^{n-1} Rs^i$, it suffices to show that $s^k \in \sum_{i=0}^{n-1} Rs^i$ for each s^k.

For this, we induct. If $k < n$, then $s^k \in \{1, s, s^2, \ldots, s^{n-1}\}$, so s^k provides its own R-linear combination to fit in $\sum_{i=0}^{n-1} Rs^i$. Otherwise, take $k \geq n$, and suppose $Rs^\ell \in \sum_{i=0}^{n-1} Rs^i$ for each $\ell < k$. By hypothesis, we see that

$$0 = s^n + p_1s^{n-1} + \cdots + p_n,$$

so upon multiplying by s^k and rearranging, we find

$$s^k = -p_1s^{k-1} - p_2s^{k-2} - \cdots - p_ns^{k-n} \in \sum_{k=1}^{n-1} Rs^k.$$

But by the inductive hypothesis, $Rs^\ell \in \sum_{i=0}^{n-1} Rs^i$ for each $\ell < n$, so $s^k \in \sum_{i=0}^{n-1} Rs^i$. This finishes.

And here is the proof of (b).

- In one direction, take S to be a free, finitely generated R-module by n generators. Our work in (the first direction of) (a) provides us some monic polynomial p in I of degree n. Further, the work in the second direction in (a) shows that

$$\{1, s, s^2, \ldots, s^{n-1}\}$$

generates S as an R-module, but S is freely generated by n elements, so S must be freely generated by the above n elements.[4]

We claim that $I = (p)$. Certainly $(p) \subseteq I$, so we have left to show $I \subseteq (p)$. Well, suppose that $f \in I$. Because p is monic, we may do Euclidean division with it (!), so we write

$$f = pq + r,$$

where we can expand

$$r(x) = \sum_{k=0}^{d} r_k x^k \in R[x],$$

where $d < n$. We claim that $r_\bullet = 0$ for each $r_\bullet$, which will finish because it will imply $f = pq$, so $f \in (p)$.

So we note that $r = f - pq \in I$, so applying $R[x] \to S$ by $x \mapsto s$, we see that

$$\sum_{k=0}^{d} r_k s^k = 0.$$

But because $d < n$, the set $\{s^0, \ldots, s^d\}$ is R-linearly independent (formally, add in the terms $0s^k$ for $d \le k < n$ to reduce to the set $\{s^0, \ldots, s^n\}$, which freely generates). So it does follow that $r_\bullet = 0$ for each $r_\bullet$.

- The second direction is similar to the second direction in (a). To be explicit, suppose that $I = (p)$ for $p \in R[x]$ where $n = \deg p$. In (a) above, we showed that $\{1, s, \ldots, s^{n-1}\}$ will generate S as an R-module. We claim that these generators are in fact free: suppose that we have some linear relation

$$\sum_{k=0}^{n-1} c_k s^k = 0$$

for coefficients $c_\bullet \in R$.

Now, let $f(x) := \sum_{k=0}^{n-1} c_k x^k$ so that we are given $f(s) = 0$. In particular, f lives in the kernel $R[x] \to S$ by $x \mapsto s$, so $f \in I$. But then $f = pq$ for some $q \in R[x]$. We claim $q = 0$, which will follow from a degree-counting argument. Indeed, if $q \neq 0$, then we can expand $p(x) = \sum_{k=0}^{n} a_k x^k$ and $q = \sum_{\ell=0}^{m} b_\ell x^\ell$ so that

$$(pq)(x) = \sum_{d=0}^{n+m} \left(\sum_{k+\ell=d} a_k b_\ell \right) x^d,$$

where we have extended the $a_\bullet$ and $b_\bullet$ to be zero where previously undefined.

In particular, the largest a_k with $a_k \neq 0$ is $k = n$, and the largest b_ℓ with $b_\ell \neq 0$ is $\ell = m$, so the largest we can achieve is $k + \ell \le n + m$, with equality on $k = n$ and $b_\ell = m$. Thus, our leading term would be $a_n b_m x^{m+n}$, which is nonzero because $a_n = 1$ (!) and $b_m \neq 0$, but this term is zero in f, which is our contradiction.

So instead, we have $q = 0$, so $f = pq = 0$, so $c_\bullet = 0$ for each $c_\bullet$.

We conclude by noting the above proof of (b) provided a power of basis for S as an R-module with $\deg p$ total generators. ■

We close with some definitions.

> **Definition 3.45** (Finite). Fix S an R-algebra. Then S is *finite* over R if and only if S is finitely generated over R as an R-module.

[4] Formally, this set of n elements provides us a surjection $R^n \twoheadrightarrow S$ by $(r_0, \ldots, r_{n-1}) \mapsto r_0 s^0 + \cdots + r_{n-1} s^{n-1}$. But $S \cong R^n$, so we have a composite surjection $R^n \twoheadrightarrow S \cong R^n$, which must be an isomorphism by Proposition 3.25. In particular, $R^n \twoheadrightarrow S$ is injective, finishing.

Definition 3.46 (Integral)**.** Fix S an R-algebra. Then an element $s \in S$ is *integral over* R if and only if s is a root of some monic polynomial in $R[x]$. If all elements $s \in S$ are integral over R, then we say S is *integral over* R.

3.2 February 15

Here we go.

Convention 3.47. For today's lecture, an R-algebra S should be thought of as providing an embedding $R \subseteq S$ (though we will not actually assume that this ring map is injective until the end).

3.2.1 A Better Integrality

Last time we introduced the following proposition.

Proposition 3.44. Fix R a ring and an R-algebra generated by one element $s \in S$. Letting I be the kernel of $R[x] \to S$ by $x \mapsto s$ so that $S \cong R[x]/I$, we have the following equivalences.

(a) S is finitely generated as an R-module if and only if I contains a monic polynomial (i.e., there is some monic $p(x) \in R[x]$ such that $p(s) = 0$).

(b) S is a free, finitely generated R-module if and only if $I = (p)$ for some monic polynomial p. In fact, S is of rank $\deg p$.

This gave rise to the following definition.

Definition 3.46 (Integral)**.** Fix S an R-algebra. Then an element $s \in S$ is *integral over* R if and only if s is a root of some monic polynomial in $R[x]$. If all elements $s \in S$ are integral over R, then we say S is *integral over* R.

Being integral is intended to be a generalization of having a finite extension of fields. Along these lines, we get the following definition.

Definition 3.45 (Finite)**.** Fix S an R-algebra. Then S is *finite* over R if and only if S is finitely generated over R as an R-module.

As with fields, we know that any finite field extension must be algebraic, so we might hope that an integral extension is also finite.

Lemma 3.48. Every finite R-algebra S is integral.

Proof. We use the Cayley–Hamilton theorem. Fix any element $s \in S$ so that we want to show s is integral over R. The key point is that $\mu_s : x \mapsto sx$ is an endomorphism $\mu_s : S \to S$ of S as an R-module. Namely, for $s_1, s_2 \in S$ and $r_1, r_2 \in R$, we merely have to check that

$$\mu_s(r_1s_1 + r_2s_2) = sr_1s_1 + sr_2s_2 = r_1ss_1 + s_2ss_2 = r_1\mu_s(s_1) + r_2\mu_s(s_2).$$

Thus, Theorem 3.24 promises a monic polynomial

$$p_{\mu_s}(x) = x^n + \sum_{k=0}^{n-1} r_k x^k$$

such that $p_{\mu_s}(\mu_s) = 0$. In particular, we see that

$$0 = 0 \cdot 1 = p_{\mu_s}(\mu_s)(1) = \left(\mu_s^n + \sum_{k=0}^{n-1} r_k \mu_s^k\right)(1) = \mu_s^n(1) + \sum_{k=0}^{n-1} r_k \mu_s^k(1) = s^n + \sum_{k=0}^{n-1} r_k s^k,$$

which verifies that s is the root of a monic polynomial $p_{\mu_s}(x) \in R[x]$. ■

In fact, we can provide a converse.

Lemma 3.49. Fix S an R-algebra. Then S is finite if and only if it is finitely generated as an R-algebra with integral generators.

Proof. We show the two directions independently. The key to the backwards direction will be the following lemma.

Lemma 3.50. If $A \subseteq B \subseteq C$ are rings, then if C is finite over B and B is finite over A, then C is finite over A.

Proof. Because C is finite over B, we get generators $c_1, \ldots, c_n$. Similarly, because B is finite over A, we get generators $b_1, \ldots, b_m$. We claim that the $b_i c_j$ generate C as an A-module, which will finish the proof.

Indeed, any $c \in C$ we can write as

$$c = \sum_{j=1}^{n} r_j c_j$$

where $r_j \in B$. Then, expanding the r_j along the generators $b_1, \ldots, b_m$, we get

$$r_j = \sum_{i=1}^{m} s_{ij} b_i.$$

Distributing, we see that

$$c = \sum_{j=1}^{n} \sum_{i=1}^{n} s_{ij}(b_i c_j),$$

which finishes the proof. ■

We now attack the proof directly.

- In one direction, suppose that $S = R[s_1, \ldots, s_n]$ where the elements $s_1, \ldots, s_n$ are all integral over R. The key is to consider the chain

  $$R \subseteq R[s_1] \subseteq R[s_1, s_2] \subseteq \cdots \subseteq R[s_1, \ldots, s_n].$$

  We show that $R[s_1, \ldots, s_k]$ is finite over R by induction on k; when $k = 0$, there is nothing to say. For the inductive step, suppose that some $R[s_1, \ldots, s_k]$ is finite over R by the elements $\{x_1, \ldots, x_m\}$, and we show $R[s_1, \ldots, s_{k+1}]$ is finite over R.

  Well, s_{k+1} is the root of some monic polynomial which we name $p \in R[x]$. But $p \in R[s_0, \ldots, s_k]$ as well, so s_{k+1} is integral over $R[s_0, \ldots, s_k]$. Thus, by Proposition 3.44, $R[s_1, \ldots, s_k][s_{k+1}]$ will still be finitely generated as an $R[s_1, \ldots, s_k]$-module.

  It follows that $R[s_1, \ldots, s_{k+1}]$ is finitely generated as an R-module by Lemma 3.50.

- In the other direction, take S a finite R-algebra. In particular, we see that $S = Rs_0 + \cdots + s_n R$ for some elements $s_0, \ldots, s_n \in S$. But Lemma 3.48 now forces the elements s_k to all be integral, so we see that S is finite over R with generators which are integral. ■

Remark 3.51 (Nir)**.** The real point of the above discussion is to give a better description of integral elements looks like: they generate finite algebras. (Again, note the analogy with fields: algebraic elements generate finite field extensions.) This will be more apparent in Proposition 3.54.

3.2.2 The Integral Closure

Sometimes an algebra isn't integral, but we can always make an integral extension.

Definition 3.52 (Integral closure)**.** Fix S an R-algebra. Then the *integral closure* S' of S over R is the set of all elements of S which are integral over R.

Remark 3.53. The integral closure depends on the choice of S: making S bigger permits more integral elements. This is analogous to the algebraic closure of a field technically depending on our choice of parent field.

Proposition 3.54. Fix S an R-algebra. Then the integral closure S' of S is an R-subalgebra of S. In particular, if $s_1, s_2 \in S$ are integral elements, then $s_1 + s_2$ and $s_1 s_2$ are also both integral elements.

Proof. The main idea is to use Lemma 3.49, emulating the proof that the set of algebraic elements is a (sub)field. Namely, for any elements $s_1, s_2 \in S$ which are integral over R, Lemma 3.49 tells us that

$$R[s_1, s_2]$$

is a finite R-algebra, so all of its elements are integral by Lemma 3.48. Thus, $s_1 s_1$ and $s_1 + s_2$ are integral.

The above argument shows that the integral closure S' is closed under addition and multiplication, so S' is a subring of S. Lastly, we note that, for any $r \in R$, the polynomial $x - r \in R[x]$ shows that each $r \in$ is integral. So closure of S' under multiplication shows that S' is also closed under R-multiplication, which is the R-action. Thus, S' is an R-subalgebra of S. ■

Remark 3.55 (Nir)**.** Here is another corollary of Lemma 3.49. Suppose that $s \in S$ is the root of some monic polynomial

$$s^n + s_{n-1} s^{n-1} + \cdots + s_1 s + s_0 = 0$$

where $s_{n-1}, \ldots, s_1 \in S$ are all integral elements. Then we show s is integral. Indeed, $R[s_0, \ldots, s_{n-1}]$ is integral and hence finite over R by Lemma 3.49.

Thus, s is integral over $R[s_0, \ldots, s_{n-1}]$, so it follows $R[s_0, \ldots, s_{n-1}, s]$ is integral and hence finite over $R[s_0, \ldots, s_{n-1}]$ by Lemma 3.49. Then $R[s_0, \ldots, s_{n-1}, s]$ is finite over R by Lemma 3.50, so s is integral over R by Lemma 3.48, finishing.

Remark 3.56 (Nir)**.** The real reason we care about Remark 3.55 is to show that the integral closure S' of S over R is "integrally closed": we show that any element $s \in S'$ integral over S' has $s \in S'$. Indeed, $s \in S$ being integral over S' means that we get a monic polynomial

$$s^n + s_{n-1} s^{n-1} + \cdots + s_1 s + s_0 = 0,$$

where $s_{n-1}, \ldots, s_0 \in S'$. But this means the s_k are integral over R by definition of S', so s is integral over R by Remark 3.55, so $s \in S'$. (Note the analogy between this and showing that the algebraic closure is algebraically closed.)

We close our discussion by quickly discussing localization: localization commutes with the integral closure.

Proposition 3.57. Fix S an R-algebra with integral closure S'; further take $U \subseteq R$ a multiplicative subset. Then $S'\left[U^{-1}\right]$ is the integral closure of $R\left[U^{-1}\right]$ in $S\left[U^{-1}\right]$.

Proof. We will show $\frac{s}{u} \in S\left[U^{-1}\right]$ is integral over $R\left[U^{-1}\right]$ if and only if $\frac{s}{u} = \frac{s'}{u'}$ for some $s' \in S$ is integral over R. For this, we attack the directions independently.

- Suppose that $s \in S$ is integral over R. Further, fixing any $u \in U$, we show that $\frac{s}{u}$ is integral over $R\left[U^{-1}\right]$. (It will follow that any $\frac{t}{v}$ equal to such a $\frac{s}{u}$ is also integral.) Well, integrality of s promises a monic polynomial
$$s^n + r_{n-1}s^{n-1} + \cdots + r_1 s + r_0 = 0$$
with coefficients in R. Transporting to $R\left[U^{-1}\right]$, we multiply everything by $\frac{1}{u^n}$ to find
$$\left(\frac{s}{u}\right)^n + \frac{r_{n-1}}{u}\left(\frac{s}{u}\right)^{n-1} + \cdots + \frac{r_1}{u^{n-1}}\left(\frac{s}{u}\right) + \frac{r_0}{u^n} = 0.$$
So $\frac{s}{u}$ is the root of a monic polynomial over $R\left[U^{-1}\right]$, finishing.

- Conversely, suppose that $\frac{s}{u}$ is integral over $R\left[U^{-1}\right]$. We show that $\frac{s}{u} = \frac{s'}{u'}$ for some $\frac{s'}{u'}$ such that s' is integral over R. This grants us a monic polynomial
$$\left(\frac{s}{u}\right)^n + \frac{r_{n-1}}{u_{n-1}}\left(\frac{s}{u}\right)^{n-1} + \cdots + \frac{r_1}{u_1}\left(\frac{s}{u}\right) + \frac{r_0}{u_0} = 0.$$
Now, set $v := u_0 u_1 \cdots u_{n-1}$ and multiply through by $(uv)^n$ to get
$$(vs)^n + \left((uv) \cdot \frac{r_{n-1}}{u_{n-1}}\right)(vs)^{n-1} + \cdots + \left((uv)^{n-1} \cdot \frac{r_1}{u_1}\right)(vs) + (uv)^n \cdot \frac{r_0}{u_0} = 0.$$
Each of the coefficients can be made equal to $\frac{r'_\bullet}{1}$ for some $r'_\bullet \in R$ because v contains within it a factor of each $u_\bullet$. In particular, we see that
$$\frac{(vs)^n + r'_{n-1}(vs)^{n-1} + \cdots + r'_1(vs) + r'_0}{1} = \frac{0}{1},$$
so there exists some $v' \in U$ such that $v' \cdot \left((vs)^n + r'_{n-1}(vs)^{n-1} + \cdots + r'_1(vs) + r'_0\right) = 0$. In particular, multiplying through by an additional $(v')^{n-1}$, we get
$$(v'vs)^n + v'r'_{n-1}(v'vs)^{n-1} + \cdots + (v')^{n-1}r'_1(v'vs) + (v')^n r'_0 = 0,$$
so $v'vs$ is the root of the monic polynomial in R and hence integral over R. So we finish by noting $\frac{s}{u} = \frac{v'vs}{v'vu}$ because $v'v \in U$. ■

Corollary 3.58. Fix S an integral R-algebra. Then $S\left[U^{-1}\right]$ is an integral $R\left[U^{-1}\right]$-algebra.

Proof. Because S is integral over R, we see that S is the integral closure of R in S. Thus, by the proposition, $S\left[U^{-1}\right]$ is the integral closure of $R\left[U^{-1}\right]$ in $S\left[U^{-1}\right]$, so $S\left[U^{-1}\right]$ is an integral $R\left[U^{-1}\right]$-algebra. ■

3.2.3 Normality

We have the following definitions.

Definition 3.59 (Normal)**.** Fix R a domain with field of fractions $K(R)$. Then R is *normal* if and only if R is integrally closed in $K(R)$; i.e., the integral closure of R in $K(R)$ is R.

Definition 3.60 (Normalization)**.** Fix R a domain with field of fractions $K(R)$. We can define the *normalization* of R to be the integral closure of R in $K(R)$.

Let's see some examples.

Example 3.61. The ring $\mathbb{Z}$ is normal. This will follow from the following proposition.

Proposition 3.62. Fix R a unique factorization domain. Then R is normal.

Proof. Fix any integral element $\frac{a}{b} \in K(R)$ with $b \neq 0$. If $a = 0$, then we note that $\frac{a}{b} = \frac{0}{1}$, which is integral, witnessed by the monic polynomial $x \in R[x]$.

Otherwise, we have $a, b \in R \setminus \{0\}$ so that they each have a unique factorization into irreducibles. The outline is to choose a and b minimally and show that b is a unit to get $\frac{a}{b} \in R$. We quickly outsource some work to a lemma.

Lemma 3.63. Fix R a unique factorization domain and $\frac{a}{b} \in K(R) \setminus \{0\}$. Then we can choose a' and b' such that $\frac{a}{b} = \frac{a'}{b'}$ such that no irreducible π divides both a' and b'.

Proof. Let $q = \frac{a}{b}$ and consider all pairs $(a, b) \in R^2$ such that $q = \frac{a}{b}$. Note that $q \neq 0$ implies that $a, b \neq 0$ in all cases because R is an integral domain. Now, it is possible that a and b some number of irreducibles in their factorizations, so choose a and b to minimize the number of shared irreducibles.

We claim that a and b have no common irreducibles. Indeed, suppose $\pi \in R$ is irreducible and $\pi \mid a, b$ with π^α and π^β the largest powers of π dividing a and b respectively. In particular, writing out the factorizations for $a = \pi^\alpha \cdot a/\pi^\alpha$ and $b = \pi^\beta \cdot b/\pi^\beta$, we see α and β are the exponents in the factorizations.

Now, without loss of generality, we take $\beta \geq \alpha$ and note

$$\frac{a}{b} = \frac{a/\pi^\alpha}{b/\pi^\alpha},$$

witnessed by $\pi^\alpha \in R \setminus \{0\}$. But now we see that a/π^α does not feature the irreducible π in its factorization, so a/π^α and b/π^α share one fewer irreducible, which contradicts the minimality of the chosen a and b. ■

So we can choose a and b to share no common factors. We claim that b is a unit. The main trick of the proof, now, is to use the integrality condition on $\frac{a}{b}$ to write a monic polynomial

$$\left(\frac{a}{b}\right)^n + r_{n-1}\left(\frac{a}{b}\right)^{n-1} + \cdots r_1\left(\frac{a}{b}\right) + r_0 = \frac{0}{1}.$$

Multiplying through by b^n, we see

$$\frac{a^n + r_{n-1}a^{n-1}b + \cdots r_1 ab^n + r_0 b^n}{1} = \frac{0}{1},$$

so because R is a domain, we get

$$a^n + r_{n-1}a^{n-1}b + \cdots r_1 ab^n + r_0 b^n = 0$$

in R. Rearranging, we have

$$a^n = -b\left(r_{n-1}a^{n-1} + \cdots r_1 ab^n + r_0 b^{n-1}\right).$$

In particular, each irreducible $\pi \in R$ dividing b will divide into a^n. Because irreducibles are prime in unique factorization domains (Remark 1.31), we see $\pi \mid a^n$ forces $\pi \mid a$, so π actually divides both a and b!

But no such irreducible π may exist, so b is divisible by no irreducible, so b is a unit by unique factorization. Thus,

$$\frac{a}{b} = \frac{ab^{-1}}{bb^{-1}} = \frac{ab^{-1}}{1},$$

so $ab^{-1}/1$ lived in R all along. This finishes. ■

Example 3.64. The ring $\mathbb{Z}[i]$ is a unique factorization domain and hence integrally closed in $K(\mathbb{Z}[i]) = \mathbb{Q}(i)$.

Non-Example 3.65. The ring $\mathbb{Z}\left[\sqrt{5}\right]$ is not normal. Indeed, our the field of fractions is $\mathbb{Q}(\sqrt{5})$, so we may consider $\frac{1+\sqrt{5}}{2} \in \mathbb{Q}(\sqrt{5}) \setminus \mathbb{Z}\left[\sqrt{5}\right]$, which is the root of the polynomial

$$x^2 - x - 1$$

by the quadratic formula. However, one can check that the integral closure is $\mathbb{Z}\left[\frac{1+\sqrt{5}}{2}\right]$, so $\frac{1+\sqrt{5}}{2}$ is essentially the only exception. We will not prove this claim because it is on the homework.

Example 3.66. The integral closure $\overline{\mathbb{Z}}$ of $\mathbb{Z}$ in $\mathbb{C}$ is the ring of all the roots of monic polynomials; these are called the algebraic integers. For example, $\overline{\mathbb{Z}} \subseteq \overline{\mathbb{Q}}$ because being the root of a monic polynomial implies being the root of some polynomial.

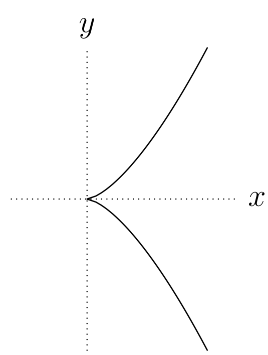
Remark 3.67. Of course, not all normal rings are unique factorization domains. For example, $\mathbb{Z}\left[\sqrt{-5}\right]$ is normal but not a unique factorization domain (by Warning 1.28). The fact that $\mathbb{Z}[\sqrt{-5}]$ is normal in $\mathbb{Q}(\sqrt{-5})$ is a problem on the homework.

3.2.4 Normality via Geometry

There is also a context for normality in algebraic geometry; roughly speaking, it is about trying to make the curve smoother.

Exercise 3.68. We compute the integral closure of the ring $R = k[x,y]/\left(y^2 - x^3\right)$ as $R[y/x]$.

Proof. Here is our image.



The issue here is the "cusp" at 0. To normalize, we need to make this curve look more like a line and normalize as a line.

So the main point is that there is a map $\varphi : k[x,y] \to k[t]$ by sending $x \mapsto t^2$ and $y \mapsto t^3$, and it is not too hard to check that the kernel of this map is $y^2 - x^3$. Indeed, certainly

$$\varphi\left(y^2 - x^3\right) = t^6 - t^6 = 0,$$

so $\left(y^2 - x^3\right) \subseteq \ker\varphi$. Conversely, if $f(x,y) \in \ker\varphi$, then we can use the fact $y^2 \equiv x^3 \pmod{y^2 - x^3}$ to write

$$f(x,y) \coloneqq \sum_{k,\ell\in\mathbb{N}} a_{k,\ell} x^k y^\ell \equiv \sum_{k=0}^\infty b_k x^k + y \sum_{k=0}^\infty c_k x^k \pmod{y^2 - x^3},$$

where b_k and c_k are some sequences which vanish for all but finitely many values. Then, passing this through φ, we see that the left- and right-hand polynomials go to the same polynomials, but the right-hand side evaluates as

$$\sum_{k=0}^{\infty} b_k t^{2k} + \sum_{k=0}^{\infty} c_k t^{2k+3},$$

which must vanish component-wise. So indeed, $f \equiv 0 \pmod{I}$, so $f \in I$.

It follows that we have an embedding $\varphi : R \hookrightarrow k[t]$, and in fact we can track the image as $k\left[t^2, t^3\right] \subseteq k[t]$; in the other direction, note that we can extend this to an isomorphism $K(R) \to k(t)$. So it suffices to compute the integral closure of $k\left[t^2, t^3\right]$ in $k(t)$ and then pull back.

Well, $t \in k(t)$ is the root of the polynomial $x^2 - t^2 = 0$ in $k\left[t^2, t^3\right][x]$, so the integral closure must contain $k[t]$. However, $k[t]$ itself is integrally closed (by Proposition 3.62), so it is the integral closure of $k\left[t^2, t^3\right]$; more explicitly, if f is integral over $k\left[t^2, t^3\right]$, then it will be integral over $k[t]$ (because the coefficients of f's polynomial also live in $k[t]$), so it will be in $k[t]$.

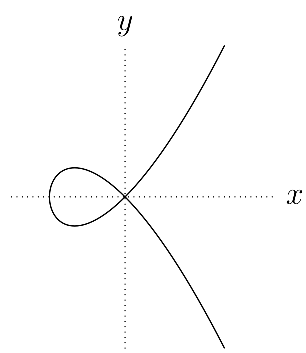
So to finish, we note that $\varphi(y/x) = t$, so because $\varphi : K(R) \to k(t)$ is injective, we see that we can just callously pull t back to y/x. In particular, our integral closure is

$$\varphi^{-1}(k[t]) = \boxed{R[y/x]},$$

which is our answer. ■

Exercise 3.69. We compute the integral closure of $R = k[x, y]/\left(y^2 - x^2(x+1)\right)$ as $R[y/x]$.

Proof. Here is our image.



Once more, the issue here is the singularity at 0. So to normalize, we will make this look more like a line and then normalize as a line.

The key to effect this plan is to note that we have a map $\varphi : k[x, y] \to k[t]$ by sending

$$x \mapsto t^2 - 1 \qquad \text{and} \qquad y \mapsto t\left(t^2 - 1\right).$$

We can again check that the kernel of this mapping is $y^2 - x^2(x+1)$, but we will be a little sketchier. On one hand, we compute

$$\varphi\left(y^2 - x^2(x+1)\right) = t^2\left(t^2 - 1\right) - \left(t^2 - 1\right)^2\left(t^2 - 1 + 1\right) = 0.$$

On the other hand, if $f(x, y) \in \ker \varphi$, then we can use the fact that $y^2 \equiv x^2(x+1) \pmod{y^2 - x^2(x+1)}$ to reduce the exponent of y and write

$$f(x, y) \equiv \sum_{k=0}^{\infty} b_k x^k + \sum_{k=0}^{\infty} c_k x^k y \pmod{y^2 - x^2(x+1)}.$$

Because $\left(y^2 - x^2(x+1)\right) \subseteq \ker \varphi$, both sides of this equivalence will go to the same place upon being pushed through φ. However, upon pushing through φ, we see that the left-hand sum only creates terms of even degree, and the right-hand sum only creates terms of odd degree, so it is not too hard to see that we must have $b_k = c_k = 0$ for each k. Explicitly, the term of the largest degree in either sum must vanish by looking in $k[t]$.

The rest of the argument proceeds as before. We note that

$$\operatorname{im}\varphi = k\left[t^2-1, t\left(t^2-1\right)\right],$$

and we will compute the integral closure of $\operatorname{im}\varphi$. As before, we note that t is a root of

$$x^2 - \left(t^2-1\right) - 1 \in (\operatorname{im}\varphi)[x],$$

so t must live in the integral closure. However, $k[t] \supseteq k\left[t^2-1, t\left(t^2-1\right)\right]$ is integrally closed, so this now must be our integral closure. Pulling back, we note that $\varphi(y/x) = t$, so our integral closure is

$$\varphi^{-1}(k[t]) = \boxed{R[y/x]},$$

which is what we wanted. ■

> **Remark 3.70** (Nir). Somewhere around here Professor Serganova gave a more rigorously sound discussion of normality via geometry, but I did not follow it. My notes are included in the comments on this file, but they are pretty incomprehensible.

3.2.5 Normality and Factorization

Proposition 3.62 suggests some connection between normality and unique factorization, but the connection is clearer when working in the polynomial ring. To start, we have the following proposition.

> **Proposition 3.71.** Fix S an R-algebra by an injective map $\varphi : R \hookrightarrow S$. If we can factor a monic polynomial $f \in R[x]$ by $f = gh$ for monic $g, h \in S[x]$, then the coefficients of g and h are integral over R.

Proof. The idea is to force a factorization. To start off, we note that g is monic, we can work in the ring

$$\frac{S[\alpha_1]}{(g(\alpha_1))},$$

which is a finite, free S-algebra generated by a power basis, from Proposition 3.44. In particular, there is an embedding $S \hookrightarrow S[\alpha_1]/(g(\alpha_1))$. The point of doing this is that $g(\alpha_1) = 0$, so doing long division by $(x - \alpha_1)$ by hand gives

$$g(x) = (x - \alpha_1)g_1(x),$$

where $g_1(x)$ is again monic by comparing leading coefficients (which makes sense as long as the leading coefficients are not zero-divisors). In particular, if the leading term of $g(x)$ is x^n, then the leading term of $g_1(x)$ will have to be x^{n-1} to be able to achieve x^n and no further.

Thus, $g_1(x)$ is monic of strictly smaller degree, so we can inductively continue this process to get

$$g(x) = (x-\alpha_1)(x-\alpha_2)\cdots(x-\alpha_n)$$

with coefficients in $S[\alpha_1, \ldots, \alpha_n]$.

Running the same process for h but now starting with $S[\alpha_1, \ldots, \alpha_n]$, we see that we can factor

$$h(x) = (x-\beta_1)(x-\beta_2)\cdots(x-\beta_m)$$

with coefficients in $S[\alpha_1, \ldots, \alpha_n, \beta_1, \ldots, \beta_m]$.

The key trick, now, is to imagine working in $R[\alpha_1, \ldots, \alpha_n, \beta_1, \ldots, \beta_m] \subseteq S[\alpha_1, \ldots, \alpha_n, \beta_1, \ldots, \beta_m]$. The point is that

$$f(x) = g(x)h(x) = (x - \alpha_1)(x - \alpha_2) \cdots (x - \alpha_n) \cdot (x - \beta_1)(x - \beta_2) \cdots (x - \beta_m),$$

so each of the $\alpha_\bullet$s and $\beta_\bullet$s are in fact the roots of the monic polynomial $f(x) \in R[x]$ and therefore integral over R. In particular, $R[\alpha_1, \ldots, \alpha_n, \beta_1, \ldots, \beta_m]$ is generated by finitely many integral elements, so it is finite and hence integral by Lemma 3.49. So when we expand

$$g(x) = (x - \alpha_1)(x - \alpha_2) \cdots (x - \alpha_n) \qquad \text{and} \qquad h(x) = (x - \beta_1)(x - \beta_2) \cdots (x - \beta_m),$$

we see that their coefficients will live in $R[\alpha_1, \ldots, \alpha_n, \beta_1, \ldots, \beta_m]$ and so must be integral over R. ■

And here is our application.

Corollary 3.72. Fix R a normal domain. Then, if $f(x) \in R[x]$ is a monic irreducible, then $f(x)$ is prime.

Proof. Fix $f(x) \in R[x]$. Then we claim f will remain irreducible in $K(R)$, which comes from the above proposition: if we factor $f = g_0h_0$ in $K(R)$, comparing leading coefficients of g_0 and h_0 lets us force g_0 and h_0 to be monic. Namely, if the leading coefficient of g_0 is ax^d, and the leading coefficient of h_0 is bx^e, then the leading coefficient of f is abx^{d+e}, which must be $ab = 1 \in R$. So by replacing

$$g = bg_0 \qquad \text{and} h = ah_0,$$

we will have $gh = abg_0h_0 = f$ while g and h are now monic.

The point of all this is that $f = gh$ with g and h monic force the coefficients of g and h to be integral by the above proposition. But R is normal (!), so $g, h \in R[x]$, so with f irreducible in $R[x]$, we have one of g or h a unit in $R[x]$ and hence in $K(R)[x]$. So f is irreducible and hence prime in $K(R)[x]$, where we are using Remark 1.31 on $K(R)[x]$.

So to finish, we create an embedding

$$\frac{R[x]}{(f(x))} \hookrightarrow \frac{K[x]}{(f(x))}$$

by lifting $R \hookrightarrow K(R)$ to $R[x] \to K(R)[x]/(f(x))$ and computing the kernel as $R[x] \cap f(x)K(R)[x]$, which we claim equals $f(x)R[x]$. If the kernel is in fact $f(x)R[x]$, then the above is an embedding, so we see that $R[x]/(f(x))$ embeds into an integral domain and hence is an integral domain.

So we have left to show $R[x] \cap f(x)K(R)[x] = f(x)R[x]$. This will hold for arbitrary domains R. Indeed, if we have some $f(x)q_0(x) = g(x) \in R[x] \cap f(x)K(R)[x]$, then clearing deminators of $q(x)$ of lets us assume that

$$f(x)q(x) = c \cdot g(x)$$

for some $q \in R[x]$. We claim that $c \mid q(x)$, from which $q_0(x) \in R[x]$ will follow. Indeed, if $c \nmid q(x)$, then we expand

$$f(x) = \sum_{k=0}^{K} a_k x^k \qquad \text{and} \qquad q(x) = \sum_{\ell=0}^{L} b_\ell x^\ell$$

where $a_K = 1$ and $b_L \neq 0$, and we can write

$$f(x)q(x) = \sum_{n=0}^{\infty} \left(\sum_{k+\ell=n} a_k b_\ell \right) x^n \in (c).$$

We know show that $b_\ell \in (c)$ for each ℓ by inducting downwards. For example, the $n = K + L$ term above will have only the nonzero term $a_K b_L = b_L \in (c)$. More generally speaking, if all terms above b_ℓ are in (c), then we can look at the $n = K + \ell$ term

$$a_K b_\ell + \sum_{i=0}^{K-1} a_i \underbrace{b_{K+\ell-i}}_{\in (c)} \in (c)$$

so that we see $b_\ell = a_K b_\ell \in (c)$. So we are done. ■

Remark 3.73. This generalizes the result that, if R is a unique factorization domain, then $R[x]$ is also a unique factorization domain.

3.2.6 Lifting Primes

Speaking generally for a moment, suppose we have an R-algebra S. Then, if $\varphi : R \to S$ is our promised map, we note that we have a map $\operatorname{Spec} S \to \operatorname{Spec} R$ by $\varphi^{-1} : \mathfrak{q} \mapsto \varphi^{-1}(\mathfrak{q})$. In particular, thinking of φ as providing an "embedding" $R \subseteq S$, we get that primes $\mathfrak{q}$ of S go to

$$\varphi^{-1}(\mathfrak{q}) = \{r \in R : \varphi(r) \in \mathfrak{q}\} =: \mathfrak{q} \cap R,$$

where we are setting this equal to $\mathfrak{q} \cap R$ by abuse of notation.

Mostly for psychological reasons, we will make this abuse of notation no longer abuse.

Convention 3.74. For the rest of this section, we will take our ring extensions to actually be embeddings and will notate this by $R \subseteq S$.

Remark 3.75 (Nir)**.** Here is one reason to not be so nervous about this: $R \subseteq S$ being an injection behaves well with the universal property of localization. Explicitly, suppose that we have an injective map $\varphi : R \hookrightarrow S$ of domains where all elements of some multiplicative set $U \subseteq R$ go to units $\varphi(U) \subseteq S^\times$. Then we claim the induced map

$$\overline{\varphi} : R\left[U^{-1}\right] \to S$$

is also injective. Indeed, $\overline{\varphi}(r/u) = 0$ implies $\varphi(r)/\varphi(u) = 0$, so $\varphi(r) = 0$, so $r = 0$, where the last step is because φ is injective.

So we will actually get to write $\mathfrak{q} \cap R$ without feeling guilty.

Now, when $R \subseteq S$ is an integral extension, we get some control of the map φ^{-1}.

Definition 3.76 (Lying over)**.** Fix $R \subseteq S$ an integral extension. Given a prime $\mathfrak{p} \in \operatorname{Spec} R$, we say that a prime $\mathfrak{q} \in \operatorname{Spec} S$ *lies over* $\mathfrak{p}$ if and only if $\mathfrak{q} \cap R = \mathfrak{p}$.

Proposition 3.77. Fix $R \subseteq S$ an integral extension by $\varphi : R \hookrightarrow S$. Then the map $\varphi^{-1} : \operatorname{Spec} S \to \operatorname{Spec} R$ is surjective. In other words, for any $\mathfrak{p} \in \operatorname{Spec} R$, there exists a prime $\mathfrak{q} \in \operatorname{Spec} S$ lying over $\mathfrak{p}$ so that $\mathfrak{q} \cap R = \mathfrak{p}$.

Proof. If $R = 0$, then $S = 0$ follows (because $0_S = 0_R = 1_R = 1_S$), so $\operatorname{Spec} S = \operatorname{Spec} R = \varnothing$, so the statement holds vacuously.

Otherwise, we may assume $R \neq 0$. Set $U := R \setminus \mathfrak{p}$, and we will localize at U to get a local ring and then will use Nakayama's lemma to finish. We take this proof in steps, taking the following reductions.

- We quickly say that it will be enough to find a prime of $S\left[U^{-1}\right]$ over $\mathfrak{p}R\left[U^{-1}\right]$. Indeed, by Theorem 2.29, we see that

$$\operatorname{Spec} S\left[U^{-1}\right] = \left\{\mathfrak{q}S\left[U^{-1}\right] : \mathfrak{q} \in \operatorname{Spec} S \text{ and } \mathfrak{q} \cap U = \varnothing\right\},$$

  so a prime $\mathfrak{q}S\left[U^{-1}\right]$ lying over $\mathfrak{p}R\left[U^{-1}\right]$ will automatically have $\mathfrak{q} \cap U = \varnothing$ and therefore $\mathfrak{q} \cap R \subseteq \mathfrak{p}$. But in fact, lying over tells us stronger: we know

$$\mathfrak{q}S\left[U^{-1}\right] \cap R\left[U^{-1}\right] = \mathfrak{p}R\left[U^{-1}\right],$$

and so, for any $x \in \mathfrak{p}$, we have $\frac{x}{1} \in \mathfrak{p}R\left[U^{-1}\right]$, so $\frac{x}{1} \in \mathfrak{q}S\left[U^{-1}\right]$, so we may write

$$\frac{x}{1} = \frac{y}{u}$$

for some $y \in \mathfrak{q}$ and $u \in U$. This implies $vy = vxu$ for some $v \in U$, so $vux \in \mathfrak{q}$, but $vu \notin \mathfrak{q}$ (because $\mathfrak{q} \cap U = \varnothing$), so $x \in \mathfrak{q}$. So indeed, $\mathfrak{p} \supseteq \mathfrak{q} \cap R$ follows, and we get $\mathfrak{q} \cap R = \mathfrak{p}$.

- So we have reduced to the case of finding a prime of $S\left[U^{-1}\right]$ lying over the maximal ideal $\mathfrak{p}R\left[U^{-1}\right]$ of the local ring $R\left[U^{-1}\right]$.

  However, we note that $S\left[U^{-1}\right]$ is still an integral $R\left[U^{-1}\right]$-extension (by Corollary 3.58), and in fact $R\left[U^{-1}\right] \subseteq S\left[U^{-1}\right]$ still (by Proposition 2.52), so we might as well rename $S\left[U^{-1}\right]$ to S and $R\left[U^{-1}\right]$ to R and $\mathfrak{p}R\left[U^{-1}\right]$ to $\mathfrak{p}$. So now we are showing that S contains a prime lying over the (unique) maximal ideal $\mathfrak{p}$ of R.

  Very quickly, we consider the ideal $\mathfrak{p}S$. Any ideal $\mathfrak{q}$ containing $\mathfrak{p}S$ will have pre-image $\mathfrak{q} \cap R \supseteq \mathfrak{p}$. In fact, if we force $\mathfrak{q}$ to be a prime containing $\mathfrak{p}S$, then we get

$$\mathfrak{q} \cap R \supseteq \mathfrak{p},$$

  but $\mathfrak{q}$ is a prime (and hence proper) ideal containing the maximal ideal $\mathfrak{p}$, so we will get $\mathfrak{q} \cap R = \mathfrak{p}$ for free, as needed.

- So we need a prime of S containing $\mathfrak{p}S$, for which we could take any maximal ideal containing $\mathfrak{p}S$ if only we knew that $\mathfrak{p}S$ is proper. Well, if $1 \in \mathfrak{p}S$, then we can write 1 as an element of $\mathfrak{p}S$, which means we can write

$$1 = p_1 s_1 + \cdots + p_n s_n$$

  for some $p_1, \ldots, p_n \in \mathfrak{p}$ and $s_1, \ldots, s_n \in S$. Now, each of the elements $s_1, \ldots, s_n$ are integral, so $M = R[s_1, \ldots, s_n]$ is an R-subalgebra generated by finitely many integral elements and therefore finitely generated as an R-module (by Lemma 3.49).

  In fact, we have $\mathfrak{p}M = M$ (because of the above equation), so we get $M = 0$ by Theorem 3.33, which forces $R \subseteq M$ to vanish; in particular, $R = 0$. But we have already dealt with the case of $R = 0$, so we are done. ■

Remark 3.78 (Nir). The requirement that $R \hookrightarrow S$ by injective is actually necessary here. For example, $\mathbb{F}_p$ is a $\mathbb{Z}$-algebra by $\pi : \mathbb{Z} \twoheadrightarrow \mathbb{F}_p$, but $\pi^{-1} : \operatorname{Spec} \mathbb{F}_p \to \operatorname{Spec} \mathbb{Z}$ is definitely not surjective: the $\operatorname{Spec} \mathbb{F}_p$ has only one element!

Remark 3.79 (Nir). It is somewhat subtle to figure out where we actually used the fact that $R \hookrightarrow S$ is injective. The place we used this is at the end: saying that $R[s_1, \ldots, s_n] = 0$ implies that $1_R = 0_R$ and so $R = 0$ is assuming that the map $R \hookrightarrow R[s_1, \ldots, s_n]$ is nonzero.

It is interesting to track through $R = \mathbb{Z}$ and $S = \mathbb{F}_2$ with $\mathfrak{p} = (3)$. After localizing, we get $R = \mathbb{Z}_{(3)}$ while $S = 0$, so indeed $M = R[s_1, \ldots, s_n]$ will still vanish because the R-action on S is the zero action, but this no longer implies that R vanishes.

In fact, we have the following slightly stronger statement.

Corollary 3.80. Fix $R \subseteq S$ an integral extension. Further, if $I \subseteq R$ is an ideal with $I \subseteq \mathfrak{p}$ for some $\mathfrak{p} \in \operatorname{Spec} R$, then we can choose $\mathfrak{q} \in \operatorname{Spec} S$ with $\mathfrak{q} \cap R = \mathfrak{p}$ which contains IS.

Proof. The point here is to mod out by I everywhere. We have the following checks.

- We see S/IS is an integral R/I-algebra. (Here, $R/I \hookrightarrow S/IS$ is defined by $[x]_I \mapsto [x]_{IS}$.) Indeed, every element $[s]_{IS} \in S/IS$ will have s the root of some monic polynomial in $R[x]$, which we can then mod out by I to see that $[s]_{IS}$ is the root of a monic polynomial in $(R/I)[x]$.

- We see $\mathfrak{p}+I$ is a prime ideal of R/I: if $[a]_I \cdot [b]_I \in \mathfrak{p}+I$, then $ab = x+i$ where $x \in \mathfrak{p}$ and $i \in I$. But $I \subseteq \mathfrak{p}$, so actually $ab \in \mathfrak{p}$, so $a \in \mathfrak{p}$ or $b \in \mathfrak{p}$, so $[a]_I \in \mathfrak{p}+I$ or $[b]_I \in \mathfrak{p}+I$.
- Thus, the proposition promises some prime ideal $\mathfrak{q} \in \operatorname{Spec} S/IS$ such that $\mathfrak{q} \cap (R/I) = \mathfrak{p}+I$. In particular, we take
$$\mathfrak{q}+IS,$$
which is prime as the pull-back of $\mathfrak{q}$ under $S \twoheadrightarrow S/IS$. Now, $r \in R$ will have $r \in \mathfrak{q}+IS$ if and only if $[r]_{IS} \in \mathfrak{q}$ if and only if $[r]_I \in \mathfrak{q}$ (because of how $R/I \hookrightarrow S/IS$ is defined) if and only if $[r]_I \in \mathfrak{p}+I$ if and only if $r \in \mathfrak{p}+I$ if and only if $r \in \mathfrak{p}$. So $(\mathfrak{q}+IS) \cap R = \mathfrak{p}$.

So we see that $\mathfrak{q}+IS$ satisfies the needed constraints, so we are done. ■

3.2.7 Integral Domains

In the case of domains, we get a little more structure out of our integral extensions by appealing to field extensions. For example, we have the following.

Lemma 3.81. Fix $R \subseteq S$ an integral extension of domains. Then $K(S)$ is algebraic over $K(R)$.

Proof. Even though Corollary 3.58 doesn't technically apply, we may imitate its proof. Fix any element $\frac{s}{u} \in K(S)$. Because $s \in S$ and s is integral over R, we see that s will satisfy some monic polynomial

$$s^n + a_{n-1}s^{n-1} + a_{n-2}s^{n-2} + \cdots + a_1 s + a_0 = 0$$

with coefficients in R. But, porting this over to $K(S)$ and dividing by u^n, we see that

$$\left(\frac{s}{u}\right)^n + ua_{n-1}\left(\frac{s}{u}\right)^{n-1} + a_{n-2}\left(\frac{s}{u}\right)^{n-2} + \cdots + a_1\left(\frac{s}{u}\right) + a_0 = 0,$$

so indeed, $\frac{s}{u}$ is algebraic over $K(R)$. ■

Remark 3.82 (Nir)**.** The converse is not true: taking $R = \mathbb{Z}$ and $S = K(R) = \mathbb{Q}$, we note that S is not an integral extension of R (indeed, the integral closure of R in S is R by Proposition 3.62, but $R \subsetneq S$). But surely the extension $K(S)/K(R)$ is algebraic because $K(S) = K(R)$.

This gives us the following lack of "avoidance" in integral domains.

Proposition 3.83. Fix $R \subseteq S$ an integral extension of domains. If $I \neq 0$ is a nonzero ideal of S, then $I \cap R \neq 0$.

Proof. Fix any $b \in I \setminus \{0\}$, and we will focus on this element alone.[5] Using Lemma 3.81, we may write out the polynomial

$$\sum_{k=0}^{n} \frac{a_k}{u_k}\left(\frac{b}{1}\right)^k = 0,$$

where $\frac{a_n}{u_n} \neq 0$. Note that each denominator $u_\bullet$ is nonzero, so we may safely multiply through by $u_0u_1\cdots u_n$ to get the polynomial

$$\sum_{k=0}^{n} r_k b^k = 0$$

for some $r_1, \ldots, r_n \in R$. Technically, removing the deminators tells us that $\frac{\sum_{k=0}^n r_k b^k}{1} = \frac{0}{1}$ in $K(S)$, but because S is an integral domain, the above equation follows.

[5] At a high level, we are basically "replacing" I with (b), for which the statement must hold anyways.

We will read off the nonzero element of $I \cap R$ from the constant term of this polynomial. We note that, if $r_0 = 0$, then we would have

$$b \cdot \sum_{k=0}^{n-1} r_{k+1} b^k = 0,$$

so $b \neq 0$ forces $\sum_{k=0}^{n-1} r_{k+1} b^k = 0$. Thus, by choosing the degree of our polynomial to be as small as possible, we may assume that $r_0 \neq 0$, lest we would be able to make the degree smaller. Rearranging, we see that

$$r_0 = -\sum_{k=1}^{n} r_k b^k = b\left(\sum_{k=1}^{n} r_k b^{k-1}\right).$$

In particular, we see that $r_0 \in (b) \subseteq I$ while $r_0 \neq 0$, so $r_0 \in I \cap (R \setminus \{0\})$. This is what we wanted. ■

Remark 3.84 (Nir)**.** In fact, the above proof technically only needed the fact that $K(R)/K(S)$ is an algebraic extension, not that S is an integral R-algebra.

To close off, we use our avoidance of ideal structure to create an avoidance of field structure.

Proposition 3.85. Fix $R \subseteq S$ an integral extension of integral domains. Then, R is a field if and only if S is a field.

Proof. We show the directions independently.

- Suppose that R is a field. Picking up any $x \in S \setminus \{0\}$, we need to show that x is a unit. Well, we note that $(x) \subseteq S$ is a nonzero ideal, so Proposition 3.83 tells us that $(x) \cap R \neq 0$. So find $u \in R$ with $u = sx \neq 0$ for some $sx \in (x)$.

  Now, $u \neq 0$ implies that u is a unit in the field R. So find $v \in R$ with $uv = 1$. Thus,

  $$(vs) \cdot x = v \cdot (sx) = vu = 1,$$

  so we see that x is indeed a unit.

- Suppose that S is a field. To show that R is a field, it suffices to show that (0) is a maximal ideal because then all proper ideals will contain (0) and hence equal (0).

  Well, pick up any prime ideal $\mathfrak{p}$ of R. By Proposition 3.77, we are promised some prime ideal $\mathfrak{q}$ of S such that $\mathfrak{q} \cap R = \mathfrak{p}$. However, because S is a field, the only prime ideal of S is $\mathfrak{q} = (0)$. Thus, all prime ideals $\mathfrak{p}$ of R are equal to

  $$\mathfrak{p} = (0) \cap R = (0).$$

  In particular, fixing $\mathfrak{m}$ as one of R's maximal ideals, we see that $\mathfrak{m} = (0)$, so (0) is a maximal ideal. ■

Remark 3.86 (Nir)**.** Here is a nice application of Proposition 3.85. If $\mathfrak{m} \subseteq S$ is a maximal ideal, then we claim $\mathfrak{m} \cap R \subseteq R$ is also a maximal ideal. Indeed, the kernel of $R \hookrightarrow S \twoheadrightarrow S/\mathfrak{m}$ is the ideal $\mathfrak{m} \cap R$, so we have an embedding

$$\frac{R}{\mathfrak{m} \cap R} \hookrightarrow \frac{S}{\mathfrak{m}}.$$

Note both are integral domains because $S/\mathfrak{m}$ is a field. In fact, this extension is also integral: any $[s]_\mathfrak{m} \in S/\mathfrak{m}$ can use the same monic polynomial as $s \in S$ and then mod out by $\mathfrak{m} \cap R$. So Proposition 3.85 kicks in to tell us that $S/\mathfrak{m}$ is a field requires $R/(\mathfrak{m} \cap R)$ to be a field, so $\mathfrak{m} \cap R$ is maximal.

To close this day's notes, we insert a result from the book that we will need a little later and fits best here in our story.

Lemma 3.87 (Incomparability)**.** Fix $R \subseteq S$ an integral extension of rings. If we have primes $\mathfrak{q}, \mathfrak{q}' \in \operatorname{Spec} S$ lying over the prime $\mathfrak{p} \in \operatorname{Spec} R$, then $\mathfrak{q} \subseteq \mathfrak{q}'$ requires $\mathfrak{q} = \mathfrak{q}'$. In other words, primes lying over $\mathfrak{p} \in \operatorname{Spec} R$ are incomparable.

Proof. The point is to reduce to Proposition 3.83. In particular, we let $\varphi : R \hookrightarrow S$ be the promised embedding, and we claim that $\overline{\varphi} : R/\mathfrak{p} \to S/\mathfrak{q}$ is an integral embedding of domains. We have domains because $\mathfrak{p}$ and $\mathfrak{q}$ are primes, and $\overline{\varphi}$ is well-defined and injective because $\varphi^{-1}(\mathfrak{p}) = \mathfrak{q}$ by definition of lying over.

It remains to show that $\overline{\varphi}$ gives us an integral extension of rings. Well, for any $s + \mathfrak{q} \in S/\mathfrak{q}$, we note that s is integral over R, so we have a monic polynomial

$$s^n + \sum_{k=0}^{n-1} \varphi(a_k) s^k = 0$$

such that $a_0, \ldots, a_{n-1} \in R$. Taking $\pmod{\mathfrak{q}}$, we see

$$(s + \mathfrak{q})^n + \sum_{k=0}^{n-1} \varphi(a_k)(s + \mathfrak{q})^k = 0,$$

but $\varphi(a_k) \cdot (x + \mathfrak{q}) = \overline{\varphi}(a_k + \mathfrak{p}) \cdot (x + \mathfrak{q})$ by construction of $\overline{\varphi}$. So indeed, the above equation provides a monic polynomial for $s + \mathfrak{q}$ over $R/\mathfrak{p}$.

Thus, we have an integral extension of rings $R/\mathfrak{p} \subseteq S/\mathfrak{q}$. Notably, $\mathfrak{q}' + \mathfrak{q} \subseteq S/\mathfrak{q}$ will have

$$\begin{aligned}
\overline{\varphi}^{-1}(\mathfrak{q}' + \mathfrak{q}) &= \{a + \mathfrak{p} : \overline{\varphi}(a + \mathfrak{p}) \in \mathfrak{q}' + \mathfrak{q}\} \\
&= \{a + \mathfrak{p} : \varphi(a) \in \mathfrak{q}' + \mathfrak{q}\} \\
&= \{a + \mathfrak{p} : \varphi(a) \in \mathfrak{q}'\} \\
&= \left\{a + \mathfrak{p} : a \in \varphi^{-1}(\mathfrak{q}')\right\} \\
&= \{a + \mathfrak{p} : a \in \mathfrak{p}\} \\
&= \{0 + \mathfrak{p}\}.
\end{aligned}$$

Thus, by Proposition 3.83, we see that $\mathfrak{q}' + \mathfrak{q} \subseteq S/\mathfrak{q}$ must be the zero ideal, so $\mathfrak{q}' + \mathfrak{q} = \mathfrak{q}$, so $\mathfrak{q}' \subseteq \mathfrak{q}$, so $\mathfrak{q}' = \mathfrak{q}$. This finishes. ■

3.3 February 17

Here we go.

3.3.1 The Nullstellensatz

Today we prove Hilbert's Nullstellensatz. Here is the statement.

Theorem 3.88 (Nullstellensatz)**.** Fix k an algebraically closed field.

(a) There are bijections between algebraic sets $X \subseteq \mathbb{A}^n(k)$ and radical ideals $J \subseteq k[x_1, \ldots, x_n]$ by taking

$$X \mapsto I(X) := \{f \in k[x_1, \ldots, x_n] : f(p) = 0 \text{ for all } p \in X\},$$

and

$$J \mapsto Z(J) := \{p \in \mathbb{A}^n(k) : f(p) = 0 \text{ for all } p \in J\}.$$

In particular, $I(Z(J)) = J$ and $Z(I(X)) = X$.

(b) Points p of an algebraic set $X \subseteq \mathbb{A}^n(k)$ are in bijection with maximal ideals of $k[x_1, \ldots, x_n]/I(X)$, which are in bijection with maximal ideals of $k[x_1, \ldots, x_n]$ containing $I(X)$.

Before jumping into the proof, we give some remarks on what we can show without too much effort. For example, back in Remark 1.78, we showed that $Z(I(X)) = X$, so the harder direction is that $I(Z(J)) = J$ for J a radical ideal.

In fact, we note that $J \subseteq I(Z(J))$ is fairly easy as well: for each $f \in J$, we note that f will vanish on any $a \in Z(J)$ by definition of $Z(J)$, so $f \in I(Z(J))$ follows. Thus, the hart part of (a) is showing

$$J \stackrel{?}{\supseteq} I(Z(J)).$$

We also remark that the last claim of (b) is merely ring theory.

Lemma 3.89. Fix R a ring and $I \subseteq R$ an ideal. Then maximal ideals of R/I are in bijection with maximal ideals of R containing I.

Proof. Let $\pi : R \twoheadrightarrow R/I$ be the canonical projection. We send maximal ideals $\mathfrak{m}$ of R containing I to the ideal $\pi(\mathfrak{m}) \subseteq R/I$; conversely, we send maximal ideals $\mathfrak{m} \subseteq R/I$ to the ideal $\pi^{-1}(\mathfrak{m})$. We have the following checks.

- Fix J an ideal containing I. We claim $\pi^{-1}(\pi(J)) = J$. To see this, we note $x \in \pi^{-1}(\pi(J))$ if and only if $\pi(x) \in \pi(J)$ if and only if $[x]_I = [y]_I$ for some $y \in J$ if and only if $x - y \in I \subseteq J$ if and only if $x \in J$.
- Similarly, fix an ideal $J \subseteq R/I$. We claim $\pi\left(\pi^{-1}(J)\right) = J$. To see this, we note $\pi(y) \in \pi\left(\pi^{-1}(J)\right)$ if and only if $y \in \pi^{-1}(J)$ if and only if $\pi(y) \in J$.
- Fix $\mathfrak{m} \subseteq R/I$, and we show that $\pi^{-1}(\mathfrak{m})$ is a maximal ideal of R. Now, we know that $\pi^{-1}(\mathfrak{m})$ is proper because it is prime. Additionally, if $\pi^{-1}(\mathfrak{m}) \subseteq J$ for some ideal J, then $\mathfrak{m} \subseteq \pi(J)$, so $\pi(J) = \mathfrak{m}$ or $\pi(J) = R/I$. In the former case, $\pi^{-1}(\mathfrak{m}) = J$; in the latter case, $J = \pi^{-1}(R/I) = R$.
- Fix $\mathfrak{m} \subseteq R$ a maximal ideal containing I, and we show that $\pi(\mathfrak{m})$ is a maximal ideal of R/I. Note $[1]_I \in \pi(\mathfrak{m})$ would imply that $1 + x \in \mathfrak{m}$ for some $x \in I$, so $1 \in \mathfrak{m}$ because $I \subseteq \mathfrak{m}$. But $1 \in \mathfrak{m}$ is false, so we see that $\pi(\mathfrak{m})$ is proper.

  Now, $\pi(\mathfrak{m}) \subseteq J$ for some ideal $J \subseteq R/I$ implies that $\mathfrak{m} \subseteq \pi^{-1}(J)$, so $\pi^{-1}(J) = \mathfrak{m}$ or $\pi^{-1}(J) = R$. Note that $[0]_I \in J$ implies $I \subseteq \pi^{-1}(J)$. So we may say that, in the former case, $J = \pi(\mathfrak{m})$; in the latter case, $J = \pi(R) = R/I$.

So we see that the described maps are mutually inverses and well-defined, so we are done. ■

There is a little more that we can say about (b): it is not too hard to reduce it to the case where $X = \mathbb{A}^n(k)$ and $I(X) = \varnothing$.

Lemma 3.90. Suppose that all maximal ideals of $k[x_1, \ldots, x_n]$ take the form $(x_1 - a_1, \ldots, x_n - a_n)$ for $(a_1, \ldots, a_n) \in \mathbb{A}^n(k)$. Then (b) of Theorem 3.88 holds.

Proof. By the previous lemma, we only have to show the first sentence of (b). Our bijection will be by

$$(a_1, \ldots, a_n) \in X \longmapsto (x_1 - a_1, \ldots, x_n - a_n) \subseteq k[x_1, \ldots, x_n].$$

We have the following checks to show (b).

- We check that $(x_1 - a_1, \ldots, x_n - a_n)$ is maximal. To see this, we claim that $(x_1 - a_1, \ldots, x_n - a_n)$ is the kernel of the surjective map

  $$\varphi \in k[x_1, \ldots, x_n] \to k$$

  defined by lifting $\mathrm{id}_k : k \to k$ by $x_i \mapsto a_i$, which will be enough. To see this, note that certainly each $x_i - a_i$ will live in the kernel. Conversely, for any $f \in k[x_1, \ldots, x_n]$, we can apply the division algorithm to f by each of the $x_i - a_i$ to write

  $$f(x_1, \ldots, x_n) = f(a_1, \ldots, a_n) + \sum_{i=1}^{n} (x_i - a_i) q_i(x).$$

Formally, one should show this by induction on n, but we won't bother. The point is that $f \in \ker\varphi$ implies that $f(a_1,\ldots,a_n) \in \ker\varphi$, so $f(a_1,\ldots,a_n) = 0$, so $f \in (x_1 - a_1,\ldots,x_n - a_n)$.

- We check that $(x_1-a_1,\ldots,x_n-a_n)$ contains $I(X)$. Indeed, if $f \in I(X)$, then f vanishes on $(a_1,\ldots,a_n)$, so f lives in the kernel $\ker\varphi$ constructed above, so $f \in (x_1 - a_1,\ldots,x_n - a_n)$.
- We show the map is injective. The key claim is that

$$Z((x_1 - a_1,\ldots,x_n - a_n)) = \{(a_1,\ldots,a_n)\}.$$

Indeed, if $(b_1,\ldots,b_n)$ lives in this vanishing set, then $b_i - a_i = 0$ for each i, so $(a_1,\ldots,a_n) = (b_1,\ldots,b_n)$. Of course, each $x_i - a_i$ does vanish on $(a_1,\ldots,a_n)$, so we are done.

So to finish, we note that $(x_1 - a_1,\ldots,x_n - a_n) = (x_1 - a_1',\ldots,x_n - a_n')$ implies that their vanishing sets match, so $(a_1,\ldots,a_n) = (a_1',\ldots,a_n')$, so we are done.

- We show the map is surjective. This requires some trickery. Suppose $\mathfrak{m}$ is a maximal containing $I(X)$. Because $\mathfrak{m}$ is maximal, we do know that

$$\mathfrak{m} = (x_1 - a_1,\ldots,x_n - a_n)$$

by hypothesis. So we see that $\mathfrak{m} \supseteq I(X)$ implies that

$$X = Z(I(X)) \supseteq Z(\mathfrak{m}) = \{(a_1,\ldots,a_n)\},$$

where we have used Remark 1.78 in the first equality. Thus, $\mathfrak{m}$ is indeed of the required form, so we are done. ■

3.3.2 The Uncountable Case

Let's start with an easier special case.

Proof of Theorem 3.88 for uncountable fields. We prove Theorem 3.88 where k is an uncountable field; in other words, one should read $k = \mathbb{C}$ into the following proof. We will actually start by showing (b) in the case where $X = \mathbb{A}^n(k)$ and $I(X) = \varnothing$. The following will be the way we use that k is uncountable.

Lemma 3.91. Fix k an uncountable field and F/k a field extension with $[F:k] < \#k$. Then the extension F/k is algebraic.

Proof. We show the contrapositive. Suppose that F/k is not algebraic, and we show that $[F:k] \geq \#k$. Because F/k is not algebraic, we are promised some element $x \in F$ which is not algebraic over k. But then $k(x) \subseteq F$ is a very large subfield, so we consider the set

$$S \coloneqq \left\{\frac{1}{x-a} : a \in k\right\}.$$

We quickly observe that these elements are legal: note that $x \neq a$ for each $a \in k$ because k/k is an algebraic extension; thus, $\frac{1}{x-a}$ is a legal element of F.

We claim that $S \subseteq k(x)$ is k-linearly independent, which will show that $[F:k] = \dim_k F \geq \dim_k k(x) \geq \#S = \#k$, which is what we want. Now, to show that S is k-linearly independent, suppose that we have a relation

$$\sum_{i=1}^n r_i \cdot \frac{1}{x-a_i} = 0$$

for some $r_1,\ldots,r_n \in k$ and distinct $a_1,\ldots,a_n \in k$. We need to show that $r_i = 0$ for each r_i. For this, we note that

$$0 = \left(\prod_{i=1}^n (x-a_i)\right)\left(\sum_{i=1}^n \frac{r_i}{x-a_i}\right) = \sum_{i=1}^n \left(r_i \prod_{\substack{j=1\\ j\neq i}}^n (x-a_j)\right). \tag{$*$}$$

Now, though this equation is technically taking place in $k(x)$, we may pull it back to an equation in $k[x]$ (noting that $k[x] \hookrightarrow k(x)$ is injective).

But with our equation holding in $k[x]$, we note that $k[x] \subseteq F$ is a free k-algebra,[6] so we may apply the universal property of $k[x]$ to note there is a morphism $k[x] \to k$ extending $\mathrm{id}_k : k \to k$ by sending $x \mapsto a_m$ for any a_m. Pushing $(*)$ through this morphism, we see

$$\sum_{i=1}^{n}\left(r_i \prod_{\substack{j=1\\ j\neq i}}^{n}(a_m - a_j)\right) = 0.$$

All terms of the sum will vanish except when $i = m$ because the product will feature a $(a_m - a_m)$ term otherwise. So we see

$$r_m \prod_{\substack{j=1\\ j\neq m}}^{n}(a_m - a_j) = 0.$$

Because the a_i are all distinct, we see $a_m - a_j \neq 0$ for each $m \neq j$, so the entire product is nonzero (k is an integral domain), so $r_m = 0$. This finishes. ■

Corollary 3.92. Fix k an uncountable field. Then, for any maximal ideal $\mathfrak{m} \subseteq k[x_1, \ldots, x_n]$, the field extension

$$\frac{k[x_1, \ldots, x_n]}{\mathfrak{m}} \supseteq k$$

is algebraic.

Proof. We quickly note that $\mathfrak{m} \cap k = (0)$ because otherwise $\mathfrak{m}$ would contain a unit; thus, the map $k \hookrightarrow k[x_1, \ldots, x_n]/\mathfrak{m}$ is indeed injective, so we do have a sane field extension.

Now, recall that any element $k[x_1, \ldots, x_n]$ can be written (uniquely) in the form

$$\sum_{(d_1,\ldots,d_n)\in\mathbb{N}^n} a_{(d_1,\ldots,d_n)} x_1^{d_1}\cdots x_n^{d_n},$$

where all but finitely many of the $a_\bullet \in k$ vanish. Thus, the monomials $x_1^{d_1}\cdots x_n^{d_n}$ will generate $k[x_1, \ldots, x_n]$ and hence span $k[x_1, \ldots, x_n]/\mathfrak{m}$. In particular,

$$\dim_k \frac{k[x_1, \ldots, x_n]}{\mathfrak{m}} \leq \#\left\{x_1^{d_1}\cdots x_n^{d_n} : (d_1, \ldots, d_n) \in \mathbb{N}^n\right\} = \#\left(\mathbb{N}^n\right).$$

However, $\mathbb{N}^n$ is countable, so $\dim_k \frac{k[x_1,\ldots,x_n]}{\mathfrak{m}} \leq \#\mathbb{N} < \#k$, so Lemma 3.91 assures us that the extension $\frac{k[x_1,\ldots,x_n]}{\mathfrak{m}} \supseteq k$ is an algebraic extension. ■

So now we can show the hypothesis of Lemma 3.90 without tears. As discussed, we need to show that all maximal ideals $\mathfrak{m} \subseteq k[x_1, \ldots, x_n]$ take the form $(x_1 - a_1, \ldots, x_n - a_n)$.

Well, picking up some maximal ideal $\mathfrak{m} \subseteq k[x_1, \ldots, x_n]$ is maximal, we have that

$$\frac{k[x_1, \ldots, x_n]}{\mathfrak{m}}$$

is an algebraic extension of k by Corollary 3.92, but k is algebraically closed, so this field must equal k. In particular, we are promised an isomorphism

$$\varphi : \frac{k[x_1, \ldots, x_n]}{\mathfrak{m}} \cong k.$$

[6] More formally, note there is a morphism $k[T] \to k[x]$ extending $\mathrm{id}_k : k \to k$ by sending $T \mapsto x$. It is not hard to see that this is surjective, and it is injective because it has trivial kernel because x is transcendental. So $k[x] \cong k[T]$.

We can lift this to a map
$$\overline{\varphi} : k[x_1, \ldots, x_n] \to k$$
with kernel $\mathfrak{m}$. But $x_i - \varphi(x_i)$ must certainly live in the kernel of $\overline{\varphi}$, so
$$(x_1 - \varphi(x_1), \ldots, x_n - \varphi(x_n)) \subseteq \mathfrak{m}.$$
But the left-hand ideal is maximal, so equality follows. So indeed, all maximal ideals of $k[x_1, \ldots, x_n]$ have the requested form.

Now we attack part (a). In addition to (b), we will need the following technical result.

Lemma 3.93. Fix k an algebraically closed field, and let $R := k[x_1, \ldots, x_n]$. Then any prime ideal $\mathfrak{p} \subseteq R$ is the intersection of the maximal ideals containing $\mathfrak{p}$.

Proof. If $\mathfrak{p}$ is maximal, then there is nothing to say. Thus, we may take $\mathfrak{p}$ prime but not maximal so that $R/\mathfrak{p}$ is a domain but not a field. In one direction, we note that
$$\mathfrak{p} = \bigcap_{\mathfrak{m} \supseteq \mathfrak{p}} \mathfrak{p} \subseteq \bigcap_{\mathfrak{m} \supseteq \mathfrak{p}} \mathfrak{m}.$$
The other inclusion is harder. To show it, we proceed by contraposition: pick up $b \notin \mathfrak{p}$, and we find some maximal ideal $\mathfrak{m}$ containing $\mathfrak{p}$ but not b so that $b \notin \bigcap_{\mathfrak{m} \supseteq \mathfrak{p}} \mathfrak{m}$.

For this, we work in $R/\mathfrak{p}\left[[b]_\mathfrak{p}^{-1}\right]$. We claim that $R/\mathfrak{p}\left[[b]_\mathfrak{p}^{-1}\right]$ is not a field. If $R/\mathfrak{p}\left[[b]_\mathfrak{p}^{-1}\right]$ is a field, then because it has countable degree over k (it is spanned by products of powers of b^{-1} and monomials of R, of which there are countably many), we see that
$$k \subseteq R/\mathfrak{p}\left[[b]_\mathfrak{p}^{-1}\right]$$
is an algebraic extension by Corollary 3.92. But because k is algebraically closed, this extension must collapse, implying that $[b]_\mathfrak{p}^{-1}$ is algebraic over k. Because k is a field, we may give $[b]_\mathfrak{p}^{-1}$ a monic polynomial in $k[x]$, which we notate by
$$\left([b]_\mathfrak{p}^{-1}\right)^m + a_{m-1}\left([b]_\mathfrak{p}^{-1}\right)^{m-1} + \cdots + a_1\left([b]_\mathfrak{p}^{-1}\right) + a_0 = 0.$$
However, this polynomial also shows that $[b]_\mathfrak{p}^{-1}$ is the root of some monic polynomial in $(R/\mathfrak{p})[x]$, so $[b]_\mathfrak{p}^{-1}$ is integral over $R/\mathfrak{p}$. But now we note $R/\mathfrak{p}$ is an integral domain and $[b]_\mathfrak{p} \neq 0$ implies that
$$R/\mathfrak{p} \subseteq (R/\mathfrak{p})\left[[b]_\mathfrak{p}^{-1}\right]$$
is an embedding (Example 2.24), so $R/\mathfrak{p}$ is a field by Proposition 3.85. But we presupposed that $R/\mathfrak{p}$ is not a field, so we have hit a contradiction.

So because $R/\mathfrak{p}\left[b^{-1}\right]$ is not a field, we have the following movements.

- We will have some nonzero maximal ideal $\mathfrak{m} \subseteq R/\mathfrak{p}\left[[b]_\mathfrak{p}^{-1}\right]$.
- Because we still know
$$R/\mathfrak{p} \subseteq (R/\mathfrak{p})\left[[b]_\mathfrak{p}^{-1}\right]$$
is an integral extension of domains, we can use Remark 3.86 to pull $\mathfrak{m}$ back to a maximal ideal $\mathfrak{m}'$ of $R/\mathfrak{p}$. Note $\mathfrak{m}'$ will not contain $[b]_\mathfrak{p}$ by Theorem 2.29.
- Lastly, we can pull $\mathfrak{m}' \subseteq R/\mathfrak{p}$ to a maximal ideal $\mathfrak{m}' + \mathfrak{p} \subseteq R$ containing $\mathfrak{p}$ by Lemma 3.89. Because $[b]_\mathfrak{p} \notin \mathfrak{m}'$, we see $b \notin \mathfrak{m}' + \mathfrak{p}$ as well.

So we see that $\mathfrak{m}' + \mathfrak{p} \subseteq R$ is the maximal ideal we are looking for. ■

Now we show part (a). Fix J a radical ideal, and we will show $J \supseteq I(Z(J))$. We can use Proposition 2.138 to write

$$J = \bigcap_{\mathfrak{p}\supseteq J} \mathfrak{p} \stackrel{*}{=} \bigcap_{\mathfrak{p}\supseteq J} \bigcap_{\mathfrak{m}\supseteq \mathfrak{p}} \mathfrak{m} = \bigcap_{\mathfrak{m}\supseteq J} \mathfrak{m},$$

where we have used Lemma 3.93 in $\stackrel{*}{=}$. Thus, fixing $f \in I(Z(J))$, it will suffice to show that $f \in \mathfrak{m}$ for any $\mathfrak{m} \supseteq J$.

However, we classified our maximal ideals above! So we get to write $\mathfrak{m} = (x_1 - a_1, \ldots, x_n - a_n)$, which is the kernel of the "evaluation at $(a_1, \ldots, a_n)$" map by Lemma 3.90. In particular, we note $\mathfrak{m} \supseteq J$ tells us that

$$Z(J) \supseteq Z(\mathfrak{m}) = \{(a_1, \ldots, a_n)\},$$

as computed in Lemma 3.90. So $f \in I(Z(J))$ implies that f vanishes on $Z(J)$, so f vanishes on $(a_1, \ldots, a_n)$, so f lives in the kernel of the "evaluation at $(a_1, \ldots, a_n)$" map, so $f \in \mathfrak{m}$. This finishes. ■

3.3.3 Rabinowitch's Trick

We now provide an alternative, more general proof. For this, we pick up the following definition.

Definition 3.94 (Jacobson)**.** A ring R is *Jacobson* if and only if any prime ideal is the intersection of some maximal ideals.

Remark 3.95 (Nir)**.** We note that J is Jacobson if and only if, for each prime $\mathfrak{p}$,

$$\bigcap_{\mathfrak{m}\supseteq \mathfrak{p}} \mathfrak{m} = \mathfrak{p}. \qquad (*)$$

Namely, if the above holds, then $\mathfrak{p}$ is the intersection of some maximal ideals; and if $\mathfrak{p}$ is the intersection of the maximal ideals in some set S, then $\mathfrak{m} \in S$ implies $\mathfrak{p} \supseteq \mathfrak{p}$, so

$$\bigcap_{\mathfrak{m}\in S} \mathfrak{m} = \mathfrak{p} \subseteq \bigcap_{\mathfrak{m}\supseteq \mathfrak{p}} \mathfrak{m} \subseteq \bigcap_{\mathfrak{m}\in S} \mathfrak{m}.$$

Further, $(*)$ is equivalent to $\operatorname{rad} R/\mathfrak{p} = (0)$: letting $\pi : R \twoheadrightarrow R/\mathfrak{p}$ be the canonical projection, Lemma 3.89 says that (maximal) ideals $R/\mathfrak{p}$ are in bijection (maximal) ideals of R containing $\mathfrak{p}$ by π, so

$$\pi^{-1}\left(\bigcap_{\overline{\mathfrak{m}}\subseteq R/\mathfrak{p}} \overline{\mathfrak{m}}\right) = \bigcap_{\mathfrak{m}\supseteq \mathfrak{p}} \mathfrak{m} \quad \stackrel{\pi}{\Longrightarrow} \quad \bigcap_{\overline{\mathfrak{m}}\subseteq R/\mathfrak{p}} \overline{\mathfrak{m}} = \pi\left(\bigcap_{\mathfrak{m}\supseteq \mathfrak{p}} \mathfrak{m}\right).$$

Example 3.96. The ring $\mathbb{Z}$ is Jacobson because all nonzero primes are maximal ($\mathbb{Z}/p\mathbb{Z}$ is a field for prime $p > 0$), and

$$(0) = \bigcap_{p\neq 0} (p).$$

Example 3.97. Similarly, R is Jacobson for any principal ideal domain. To start, $(0) = \bigcap_{\mathfrak{m}} \mathfrak{m}$ because $f \neq 0$ will have $f \notin \mathfrak{m}$ for any $\mathfrak{m}$ if $f \in R^\times$; otherwise, we can place $f + 1$ in a maximal ideal $\mathfrak{m}$, and we see $1 \notin \mathfrak{m}$ requires $f \notin \mathfrak{m}$ and so $f \notin \bigcap_{\mathfrak{m}} \mathfrak{m}$.

Otherwise, fix $\mathfrak{p} \subseteq R$ a nonzero prime ideal; because R is a principal ideal domain, we can write $\mathfrak{p} = (\pi)$ for some nonzero prime $\pi \in R$. Then the argument from Theorem 1.25 shows that all prime elements are maximal, so $\mathfrak{p}$ is actually a maximal ideal.

Non-Example 3.98. A local domain which is not a field is not Jacobson; e.g., $\mathbb{Z}_2$ is not Jacobson. The issue is that being local implies that there is only one maximal ideal, but it is not (0) because we are not in a field. Thus, (0) is some prime (because we are in a domain) which is not the intersection of some number of maximal ideals (of which there is only one).

Our main goal is to show that $k[x_1, \ldots, x_n]$ is Jacobson, akin to Lemma 3.93. In an attempt to generalize the argument given there, we have the following lemma.

Lemma 3.99. Fix R a domain but not a field. Then $\operatorname{rad} R = (0)$ if and only if $R\left[b^{-1}\right]$ is not a field for any $b \in R \setminus \{0\}$.

Proof. The main point is that prime ideals of $R\left[b^{-1}\right]$ are in one-to-one correspondence with prime ideals of R which avoid b. We show our directions independently.

- Suppose that $R\left[b^{-1}\right]$ is a field for some $b \in R \setminus \{0\}$. Then, for any maximal ideal $\mathfrak{m} \subseteq R$, we claim that $b \in \mathfrak{m}$, which will finish. Well, $\mathfrak{m}R\left[b^{-1}\right]$ is some ideal, and it is nonzero because $\mathfrak{m}$ is nonzero; explicitly, the map $R \to R\left[b^{-1}\right]$ is injective by Example 2.24.

  But $R\left[b^{-1}\right]$ is a field and so all nonzero ideals must be all of $R\left[b^{-1}\right]$. Thus, $\frac{1}{1} \in \mathfrak{m}R\left[b^{-1}\right]$, so $\frac{x}{u} = \frac{1}{1}$ and then $b^k\left(x - b^\ell\right) = 0$ for some $b^k, b^\ell \in \{b^n : n \in \mathbb{N}\}$. But $b \neq 0$, so $b^k \neq 0$, so
  $$x = b^\ell \in \mathfrak{m}.$$
  Because $\mathfrak{m}$ is proper, we conclude $\ell > 0$, and because $\mathfrak{m}$ is prime, we conclude $b \in \mathfrak{m}$.

- Suppose that
  $$\bigcap_{\mathfrak{m}} \mathfrak{m} = (0).$$
  Then we claim that $R\left[b^{-1}\right]$ is not a field. We do this by exhibiting a nonzero proper ideal of $R\left[b^{-1}\right]$.

  Well, $b \neq 0$, so the above intersection promises us some maximal ideal $\mathfrak{m}$ such that $b \notin \mathfrak{m}$. It follows that $\mathfrak{m} \cap \{b^n : n \in \mathbb{N}\} = \varnothing$, so Theorem 2.29 tells us that
  $$\mathfrak{m}R\left[b^{-1}\right]$$
  is a prime ideal and hence proper. Further, as noted above, Example 2.24 tells us $R \to R\left[b^{-1}\right]$ is injective, so the fact that $\mathfrak{m}$ is nonzero (R is not a field, so (0) is not maximal) implies that $\mathfrak{m}R\left[b^{-1}\right]$ is also nonzero ■

This gives the following corollary.

Corollary 3.100 (Rabinowitch). Fix R a ring. Then R is Jacobson if and only if each non-maximal prime $\mathfrak{p}$ has $R/\mathfrak{p}\left[[b]_\mathfrak{p}^{-1}\right]$ not a field for each $b \notin \mathfrak{p}$. Equivalently, R is Jacobson if and only if, for each prime $\mathfrak{p}$, $(R/\mathfrak{p})\left[b^{-1}\right]$ for some $b \in (R/\mathfrak{p}) \setminus \{0\}$ implies that $R/\mathfrak{p}$ is a field.

Proof. Fix $\mathfrak{p}$ any prime so that we want to show $\operatorname{rad} R/\mathfrak{p} = (0)$ by Remark 3.95. If $\mathfrak{p}$ is maximal, then $R/\mathfrak{p}$ is a field, so (0) is the only maximal ideal, so $\operatorname{rad} R/\mathfrak{p} = (0)$ follows.

Otherwise, we have a non-maximal ideal $\mathfrak{p}$. By Lemma 3.99, we want to show that $\operatorname{rad} R/\mathfrak{p} = (0)$. Well, by Lemma 3.99, this is equivalent to $(R/\mathfrak{p})\left[[b]_\mathfrak{p}^{-1}\right]$ not being a field for all $[b]_\mathfrak{p} \neq 0$ (i.e., for all $b \notin \mathfrak{p}$). ■

3.3.4 The General Case

And now we can more or less proceed as in the earlier proof of the Nullstellensatz. Here is our "abstract" version of the Nullstellensatz.

Theorem 3.101 (General Nullstellensatz)**.** Fix R a Jacobson ring and S a finitely generated R-algebra by $\varphi : R \to S$ (which we do not assume to be injective).

(a) Then S is a Jacobson ring.

(b) For each maximal ideal $\mathfrak{m} \subseteq S$, we have $\mathfrak{m} \cap R$ maximal in R, and

$$\frac{R}{\mathfrak{m} \cap R} \subseteq \frac{S}{\mathfrak{m}}$$

is a finite extension of fields. (Recall $\mathfrak{m} \cap R := \varphi^{-1}(\mathfrak{m})$.)

Theorem 3.88 will follow from this, essentially using the same argument from before. We will be more explicit afterwards.

Proof of Theorem 3.101. By induction, it will suffice to show the case where S is generated by a single element over R; we will be more explicit about this induction at the end. So for now, let $S \cong R[t]/J$ for some $J \subseteq R[t]$.

We begin with (a). The main point is to use Corollary 3.100. Well, fix $\mathfrak{p}$ a prime of S. Now, we note that we have an extension of domains

$$\underbrace{\frac{R}{\varphi^{-1}(\mathfrak{p})}}_{R':=} \overset{\varphi}{\hookrightarrow} \underbrace{\frac{S}{\mathfrak{p}}}_{S':=}.$$

Now, we still have a projection $R[t] \twoheadrightarrow S \twoheadrightarrow S'$ with kernel containing $\varphi^{-1}(\mathfrak{p}) \subseteq R$, so we have a projection $R'[t] \twoheadrightarrow S'$. In particular, we can write $S' \cong R'[t]/\mathfrak{P}$ for some ideal $\mathfrak{P} \subseteq R'[t]$. Note $\mathfrak{P}$ is prime because S' is a domain.

Now, to use Corollary 3.100, we need to show that, if $\mathfrak{p}$ is prime but not maximal, then $(S/\mathfrak{p})\left[b^{-1}\right] = S'\left[b^{-1}\right]$ is not a field for any $b \in S' \setminus \{0\}$. By contraposition, we will actually suppose that we found $b \in S' \setminus \{0\}$ such that $S'\left[b^{-1}\right]$ is a field, then S' is a field, which implies $\mathfrak{p}$ is maximal. We proceed by casework on $\mathfrak{P}$.

(i) Suppose $\mathfrak{P} = 0$ so that $S' \cong R'[t]$. Then $R'[t]\left[b^{-1}\right]$ being a field will imply that $K(R')[t]\left[b^{-1}\right]$ is a field (e.g., clear denominators and then find the inverse in $R'[t]$), but now Corollary 3.100 says that $\left(K(R')[t]/(0)\right)\left[b^{-1}\right]$ being a field will force $(0) \subseteq K(R')[t]$ to be a maximal ideal because $K(R')[t]$ is Jacobson by Example 3.97. In other words, $K(R')[t]$ is a field, which simply does not make sense.

It might be surprising that we hit a contradiction here, but this simply means that $R'[t]\left[b^{-1}\right]$ should never be a field.

(ii) Otherwise, $\mathfrak{P} \neq 0$ so that $R'[t] \twoheadrightarrow S'$ has some nontrivial kernel. Our idea, now, is to force our elements to be integral in the rudest way possible. We have two steps.

- We make t integral. Fixing $a(t) \in \mathfrak{P} \setminus \{0\}$, we note that $t \in S$ must vanish on $a(t)$, which we expand as out

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

where $a_\bullet \in R'$ have $a_n \neq 0$ in R'. The point of this equation is to make t integral over some localization of R': $\varphi(a_n) \in S'\left[b^{-1}\right]$ will also be nonzero in $S'\left[b^{-1}\right]$, so because $S'\left[b^{-1}\right]$ is a field, $\varphi(a_n)$ is a unit

In particular, we see that we can extend φ to a map $R'\left[a_n^{-1}\right][t] \to S'\left[b^{-1}\right]$, which turns $S'\left[b^{-1}\right]$ into an $R'\left[a_n^{-1}\right]$-algebra. In fact, the map $R'\left[a_n^{-1}\right] \to S'\left[b^{-1}\right]$ is still injective by Remark 3.75 because the map $R' \hookrightarrow S' \hookrightarrow S'\left[b^{-1}\right]$ is also injective.

Now, when viewing $S'\left[b^{-1}\right]$ as an $R'\left[a_n^{-1}\right]$-algebra, we can write

$$t^n + a_n^{-1}a_{n-1}t^{n-1} + \cdots + a_n^{-1}a_1t + a_n^{-1}a_0 = 0,$$

thus making t integral over $R'\left[a_n^{-1}\right]$.

- We make b integral. Noting that all nonzero elements of R' go to units in $K(S')$, we see that Remark 3.75 promises us an embedding $K(R') \subseteq K(S')$. Extending this by sending $t \mapsto t$, we have the familiar surjection $R'[t] \twoheadrightarrow S'$ becoming $K(R')[t] \twoheadrightarrow K(S')$, so $K(S')$ is $K(R')$-spanned by powers of t.

  However, the polynomial $a(t)$ from the previous point tells us that there is a relation among the elements $\{1, \ldots, t^n\}$, so we can inductively write any exponent t^N for $N \geq n$ in terms of smaller-degree terms. Thus, $K(S')$ is $K(R')$-spanned by a finite number of elements and in particular is a finite field extension.

  This is all to say that the powers $\{1, b, b^2, \ldots\} \subseteq K(S')$ must get a $K(R')$-relation eventually, which we label by

  $$c_mb^m + \cdots + c_1b + c_0 = 0,$$

  where not all the terms vanish. By taking m as small as possible, we note that we cannot have $c_0 = 0$, for otherwise we could divide out by b (recall $b \in S'$ lives in an integral domain).

  Now, clearing denominators, we may assume that the $c_\bullet$ all live in R', so we actually have created a relation for b. In fact, porting this equation over to $S\left[b^{-1}\right]$, we can multiply through by $\left(b^{-1}\right)^m$ to see

  $$c_0\left(b^{-1}\right)^m + \cdots + c_{m-1}b^{-1} + c_m = 0.$$

  In particular, extending the embedding $R'\left[a_n^{-1}\right] \hookrightarrow S'$ to

  $$R'\left[(c_0a_n)^{-1}\right] \hookrightarrow S' \hookrightarrow S'\left[b^{-1}\right]$$

  (the former is an embedding by Remark 3.75, and the latter is an embedding by Example 2.24), we see that b^{-1} is now the solution of an equation in $R'\left[(c_0a_n)^{-1}\right]$ with unit leading coefficient, so b^{-1} is now integral over $R'\left[(c_0a_n)^{-1}\right]$.

For technicality reasons, we are forced to admit that t remains integral over $R'\left[(c_0a_n)^{-1}\right]$ using the same equation. So now we have an embedding of domains

$$R'\left[(c_0a_n)^{-1}\right] \subseteq S'\left[b^{-1}\right],$$

where $S'\left[b^{-1}\right] = R'[t]\left[b^{-1}\right]$ is generated by integral elements. So in fact the above is an integral extension of domains by Lemma 3.49.

To finish, we see that $S'\left[b^{-1}\right]$ is a field implies that $R'\left[(c_0a_n)^{-1}\right]$ is a field (by Proposition 3.85) implies that R' is a field (because R is Jacobson). Thus, the equation $a(t)$ for t can be made monic without tears, so t is integral over S', so S' is integral over R' by Lemma 3.49. Thus, S' is a field by Proposition 3.85.

Technically, the above two points do finish the proof of part (a), but we note that considering $\mathfrak{p} \subseteq S$ to be a maximal ideal will give (b), as follows. We quickly remark that there certainly exists a $b \in S' \setminus \{0\}$ for which $S'\left[b^{-1}\right]$ because $S' = S/\mathfrak{p}$ is a field, so we can simply set $b = 1$.

Now, we see that the map $R'[t] \twoheadrightarrow S'$ is forced to have nontrivial kernel because we derived contradiction in (i), so we must live case (ii) of the above. Here, the arguments of (ii) show that $R' = R/\varphi^{-1}(\mathfrak{p})$ is a field, so $\varphi^{-1}(\mathfrak{P})$ is indeed maximal. Further, (ii) showed that $S' = K(S')$ is spanned finitely by $R' = K(R')$, so $R' \subseteq S'$ is a finite field extension.

The above completes the proof in the case that S is generated over R by a single element. We now provide the induction. Indeed, suppose that S is generated over R by $r+1$ elements so that we are promised a surjection

$$\pi : R[x_1, \ldots, x_{r+1}] \twoheadrightarrow S.$$

Now, we set $S_0 := k[x_1, \ldots, x_r]$ so that S_0 is generated over R by r elements, meaning we can use the inductive hypothesis when viewing S_0 as an R-algebra. And then further, π above becomes a surjection $\pi : S_0[x_{r+1}] \twoheadrightarrow S$; for the sake of notation, we let $\iota_0 : R \hookrightarrow S_0$ be the embedding. We now attack our claims in sequence.

(a) By the inductive hypothesis, R being Jacobson implies that S_0 is Jacobson, and the work in the one-variable case then shows that S is Jacobson.

(b) Fix $\mathfrak{m} \subseteq S$ a maximal ideal. By the one-variable case, we see that $\pi^{-1}(\mathfrak{m})$ is a maximal ideal, and the field extension $S_0/\pi^{-1}(\mathfrak{m}) \subseteq S/\mathfrak{m}$ is finite. Continuing, by the inductive hypothesis, pulling $\pi^{-1}(\mathfrak{m}) \subseteq S_0$ to $\iota^{-1}\left(\pi^{-1}(\mathfrak{m})\right) \subseteq R$ remains a maximal ideal, and in fact

$$\iota^{-1}\left(\pi^{-1}(\mathfrak{m})\right) = \varphi^{-1}(\mathfrak{m}).$$

Indeed, we see $r \in \varphi^{-1}(\mathfrak{m})$ if and only if $\pi(\iota(r)) = \varphi(r) \in \mathfrak{m}$. So $\varphi^{-1}(\mathfrak{m}) \subseteq R$ is a maximal ideal where $R/\varphi^{-1}(\mathfrak{m}) \subseteq S_0/\pi^{-1}(\mathfrak{m})$ is a finite extension. So we have the chain

$$R/\varphi^{-1}(\mathfrak{m}) \subseteq S_0/\pi^{-1}(\mathfrak{m}) \subseteq S/\mathfrak{m}$$

of finite extensions, from which we conclude that $R/\varphi^{-1}(\mathfrak{m}) \subseteq S/\mathfrak{m}$ is a finite extension. ■

Now we prove Theorem 3.88. All the logic is borrowed from the specific case, but we merely change the proof of the key lemmas Corollary 3.92 and Lemma 3.93 to use Theorem 3.101.

General proof of Theorem 3.88. We follow the argument from the special case. To start, note that k is Jacobson because it is (stupidly) a principal ideal domain, so $k \subseteq k[x_1, \ldots, x_r]$ satisfies the hypotheses of Theorem 3.101. We have the following.

- We see that Corollary 3.92 holds for general algebraically closed fields k by part (b) of Theorem 3.101, which was what we needed for part (b) of Theorem 3.88.
- Additionally, we get Lemma 3.93 in the general case by part (a) of Theorem 3.101, which when combined with (b) of Theorem 3.88 is what we needed to prove part (a) of Theorem 3.88.

The above proves all of Theorem 3.88. ■

Remark 3.102. The midterm will only include up to Nakayama's lemma because we have not done homework on the content past then.

3.3.5 Example Problems

Let's do some example problems, to review.

Exercise 3.103. Fix a field k. We work in $k^{n\times n}$. We show that the ideal

$$\det \begin{bmatrix} x_{11} & \cdots & x_{1n} \\ \vdots & \ddots & \vdots \\ x_{n1} & \cdots & x_{nn} \end{bmatrix} =: \det X$$

is a prime ideal in $k[x_{ij}]$. Note that it suffices to show $\det X$ is irreducible.

Example 3.104. In the case of $n = 2$, we are showing $\det X = x_{11}x_{22} - x_{12}x_{21}$ is irreducible. Well, for any x_{ij}, if we could write

$$\det X = f(X)g(X),$$

then we must have $\deg_{x_{ij}} f = 0$ or $\deg_{x_{ij}} g = 0$. In particular, we have two cases.

- We might have $(x_{11}x_{22} - b)c$ for some b and c. But then this forces $c = 1$.
- We might have $(x_{11} - b)(x_{22} - c)$ for some b and c. But then cx_{11} would have to live in the polynomial, so $cx_{11} = 0$, and similar for bx_{22}, causing everything to collapse.

Proof of Exercise 3.103. Use expansion by minors to write

$$\det X = x_{11} \det X_{11} - q,$$

where X_{11} is X without the top and left row. By induction, we may assume that $\det X_{11}$ is irreducible.

Now we attempt to factor $\det X = fg$. By looking at the degree of x_{11}, we see that exactly one of f or g will have the linear term x_{11}. Similarly, because $\det X_{11}$ is irreducible, we cannot split it between f and g, so it must wholesale appear in one of the factors. This gives us the following cases.

- We might have $\det X = (x_{11} + b)(\det X_{11} + c)$. Now, because $x_{11} \det X_{11}$ contains all terms with an x_{11}, so $c = 0$ is forced. But then $\det X_{11} \mid \det X$, which does not make sense. For example, running the above argument again for x_{12} shows that the analogously defined X_{12} has $\det X_{12} \mid \det X$, but $\det X_{11}$ and $\det X_{12}$ are distinct irreducibles and hence coprime, which forces

$$\deg \det X \geq \deg \det X_{11} + \deg \det X_{12},$$

which does not make sense.

- We might have $\det X = (x_{11} \det X_{11} + b)c$. But by degree arguments, we see that c is constant, which means that c is a unit already.

In particular, no other factorizations are possible because they would require factoring $\det X_{11}$, which is irreducible. ■

Exercise 3.105. Fix k be algebraically closed, and fix $R = k[x, y]$ and $M = k[x, y]/\left(x^2, xy\right)$.

- We compute $\operatorname{Ass} M$.
- We compute $\operatorname{Supp} M$.
- We compute $H_M(s)$.

Proof. Let's start with $H_M(s)$. Let's tabulate.

- $H_M(0) = 1$, with 1.
- $H_M(1) = 2$, with x and y.
- $H_M(2) = 1$ with y^2.
- In fact, $H_M(s) = 1$ for $s > 1$ with y^s because all other monomials have xy and therefore are killed.

Now we compute $\operatorname{Supp} M$. Because M is a finitely generated module, Proposition 2.75 says the support consists of the primes $\mathfrak{p} \subseteq k[x, y]$ containing $\operatorname{Ann} M = \left(x^2, xy\right)$. Well, any such prime $\mathfrak{p}$ must contain x^2 and therefore x and therefore (x), but of course $\mathfrak{p} \supseteq (x)$ implies $\mathfrak{p} \supseteq \left(x^2, xy\right)$. Thus,

$$\operatorname{Supp} M = \{\mathfrak{p} : \mathfrak{p} \supseteq (x)\}.$$

We finish by concluding that the only primes containing (x) are either (x) or of the form $(x, y - a)$ for some $a \in k$, which we can see because any prime $\mathfrak{p}$ containing (x) can be projected on by

$$k[y] \cong k[x, y]/(x) \twoheadrightarrow k[x, y]/\mathfrak{m},$$

and the only way to lift $\mathfrak{m}$ to a prime of $k[y]$ is by $y - a$. (Notably, k is algebraically closed.)

Lastly, we compute $\operatorname{Ass} M$. Well, $(x) \cap (x, y)^2 = \left(x^2, xy\right)$ is a primary decomposition where no primary ideal can be removed ((x) is (x)-primary, and $(x, y)^2$ is (x, y)-primary), so Theorem 2.193 tells us that $\operatorname{Ass} M = \{(x), (x, y)\}$. ■

Remark 3.106. Professor Serganova recommends doing exercises 2.19, 2.22, and 4.11 from Eisenbud.

3.4 February 22

There was no class today. We had a midterm.

Theme 4
Working in Chains

But this is like trying to scale a glacier. It's hard to get your footing, and your fingertips get all red and frozen and torn up.

—Anne Lamott

4.1 February 24

So it's the day after death.

4.1.1 Midterm Review

Let's start talking about the second problem on the midterm.

Exercise 4.1. Identify matrices $X \in \mathbb{C}^{2\times 2}$ with $\mathbb{A}^4(\mathbb{C})$ by

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix} \mapsto (a,b,c,d).$$

Let $Z := \left\{X \in \mathbb{C}^{2\times 2} : X^2 = 0\right\}$. Then show that the ideal $I(Z)$ is prime.

Proof. We start by showing

$$Z = \{(a,b,c,d) : a+d = ad-bc = 0\}.$$

In one direction, we note that $X^2 = 0$ implies that all eigenvalues are 0, so the characteristic polynomial of X will be $X^2 = 0$, so we see that $\operatorname{tr} X = \det X = 0$. Thus, $(a,b,c,d) \in I$ implies $a+d = ad-bc = 0$.

Conversely, if (a,b,c,d) have $a+d = ad-bc = 0$, then the associated matrix X satisfies the equation

$$x^2 = x^2 - (\operatorname{tr} X)x + \det X = 0$$

by Theorem 3.17, so we conclude that $X^2 = 0$.

Now, we see that $Z = Z(a+d, ad-bc)$, so by Theorem 3.88,

$$I(Z) = \operatorname{rad}(a+d, ad-bc).$$

So we claim that $(a+d, ad-bc)$ is prime, which will show that it is radical and therefore showing $I(Z) = (a+d, ad-bc)$ is prime. To show $(a+d, ad-bc)$ is prime, we note that we have a map

$$\mathbb{C}[a,b,c,d] \to \mathbb{C}[a,b,c]$$

by sending $d \mapsto -a$. It is not too hard to check that $(a+d)$ is the kernel of this map, so we have an embedding

$$\frac{\mathbb{C}[a,b,c,d]}{(a+d)} \hookrightarrow \mathbb{C}[a,b,c].$$

Now, if we want to mod out the left by $(ad-bc)$, this goes to $\left(-a^2-bc\right) = \left(a^2+bc\right)$ on the right. In fact, the pre-image of $\left(a^2+bc\right)$ we can check will actually be $(a+d)$, so we get an embedding

$$\frac{\mathbb{C}[a,b,c,d]}{(a+d, ad-bc)} \hookrightarrow \frac{\mathbb{C}[a,b,c]}{(a^2+bc)}.$$

Now, to show that $(a+d, ad-bc)$ is prime, it suffices to show that the left-hand ring is an integral domain, for which it suffices to show that $\mathbb{C}[a,b,c]/\left(a^2+bc\right)$ is an integral domain, for which it suffices to show that a^2+bc is an irreducible element because $\mathbb{C}[a,b,c]$ is a unique factorization domain. Well, by degree arguments with a, the only way to factor this would be as

$$(a+f)(a+g) \qquad \text{or} \qquad \left(a^2+f\right)g,$$

where f and g feature no as. The former would force ag and af, but a^2+bc has no terms other than a^2 with an a. The latter would force $g=1$ because of the a^2g term, so this factorization is trivial. ■

4.1.2 Filtrations of Rings

Today we are talking about the Artin–Rees lemma, which requires us talking about filtrations. Here is our definition.

Definition 4.2 (Filtration, rings)**.** Fix R a ring. Then a *filtration* of R is a sequence of ideals $\{I_p\}_{p\in\mathbb{N}}$ forming the chain

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

such that $I_pI_q \subseteq I_{p+q}$.

While we're here, we record the following philosophy.

Idea 4.3. Filtrations are useful to understand an object in smaller steps.

Anyways, the condition $I_pI_q \subseteq I_{p+q}$ should remind us of grading, and indeed graded rings have nice filtrations.

Exercise 4.4 ("Graded" filtration)**.** Fix $R = R_0 \oplus R_1 \oplus R_2 \oplus \cdots$ a graded ring. Then the ideals

$$I_p := \bigoplus_{i \geq p} R_i$$

form a filtration.

Proof. We see that $R = I_0$ and $I_p \supseteq I_{p+1}$ is by construction, so we are allowed to write

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

Additionally, for any $f \in I_p$ and $g \in I_q$, then we can write out

$$f = \sum_{i \geq p} a_i \qquad \text{and} \qquad g = \sum_{j \geq q} b_j$$

with $a_i \in R_i$ and $b_j \in R_j$ so that, upon distributing,

$$fg = \sum_{i \geq p, j \geq q} a_i b_j.$$

Each term $a_i b_j$ lives in $R_i R_j \subseteq R_{i+j} \subseteq I_{p+q}$, so $fg \in I_{p+q}$. ■

Here is our other chief example of filtration.

Definition 4.5 (I-adic filtration)**.** Fix R a ring and $I \subseteq R$ an ideal. Then

$$R = I^0 \supseteq I^1 \supseteq I^2 \supseteq I^3 \supseteq \cdots$$

is a filtration. This is called the *I-adic filtration*.

As a brief justification, we see that $R = I^0$ by definition of I^0; $I^p \supseteq I^{p+1}$ is because $II^k \subseteq RI^k = I^k$; and lastly, $I^p I^q = I^{p+q} \subseteq I^{p+1}$.

Exercise 4.6. The graded filtration produced by grading $R = k[x_1, \ldots, x_n]$ by degree and using Exercise 4.4 is the $(x_1, \ldots, x_n)$-adic filtration.

Proof. Let $R_d \subseteq k[x_1, \ldots, x_n]$ be the union of $\{0\}$ and the polynomials homogeneous of degree d. Then, fixing some nonnegative integer p, we are asserting that

$$\bigoplus_{i \geq d} R_d \stackrel{?}{=} (x_1, \ldots, x_n)^d.$$

But this is true essentially by tracking through what everything means. By definition,

$$(x_1, \ldots, x_n)^d = \left(x_1^{d_1} \cdots x_n^{d_n} : d_1 + \cdots + d_n = d \right).$$

In particular, $(x_1, \ldots, x_n)^d$ is generated by elements in $R_d \subseteq \bigoplus_{i \geq d} R_d$.

In the other direction, suppose that we have any $f \in \bigoplus_{i \geq d} R_d$. Then we can decompose

$$f = \sum_{i \geq d} f_i,$$

where $f_i \in R_i$. We claim that each f_i lives in $(x_1, \ldots, x_n)^d$, which will finish by showing $f \in (x_1, \ldots, x_n)^d$. Well, by definition of R_i, we can write

$$f_i(x_1, \ldots, x_n) = \sum_{d_1 + \cdots + d_n = i} a_{(d_1, \ldots, d_n)} x_1^{d_1} \cdots x_n^{d_n}.$$

Now, $d_1 + \cdots + d_n = i \geq d$, so the monomial $x_1^{d_1} \cdots x_n^{d_n}$ is divisible by a polynomial of degree d and therefore lives in $(x_1, \ldots, x_n)^d$.[1] So each monomial in the expansion of f_i lives in $x_1^{d_1} \cdots x_n^{d_n}$, so f_i lives in $x_1^{d_1} \cdots x_n^{d_n}$. ■

[1] Writing this out would be very annoying; here is one way: find the largest $m \geq 0$ such that $d_1 + \cdots + d_m < d$. Note $m < n$ because $d < i$. Then $x_1^{d_1} \cdots x_m^{d_m} x_{m+1}^{n-(d_1+\cdots+d_m)}$ divides $x_1^{d_1} \cdots x_n^{d_n}$.

Remark 4.7 (Nir, Miles)**.** Fix a graded ring R and I the irrelevant ideal. It is not in general true that the "graded" filtration from Exercise 4.4 is the same as the I-adic filtration. For example, consider $R := k\left[x^2\right]$ graded by degree; namely,

$$R_{2d} = kx^{2d} \qquad \text{and} \qquad R_{2d+1} = 0.$$

Then we see that I contains no nonzero linear polynomials, so I^2 will contain no nonzero quadratic polynomials, so the second term of the I-adic filtration has no quadratics. However, the graded filtration has the second term as $R_2 \oplus R_3 \oplus \cdots$, which definitely contains quadratics.

To set up the discussion that follows, we note that, if we have a filtration

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

we might be interested in the "bottom" of this filtration

$$I := \bigcap_{i=0}^{\infty} I_i.$$

It is not too hard to check that this is an ideal: $x, y \in I$ and $r, s \in R$ have $x, y \in I_i$ and therefore $rx + sy \in I_i$ for any i, so $rx + sy \in I$. Now, if we have a "good" filtration, we might hope that $I = 0$ so that our filtration can actually see to the bottom of R. Of course, we will need some conditions on the filtration to guarantee this.

4.1.3 Associated Graded Rings

We saw that gradings give filtrations back in Exercise 4.4. We can partially go the other way as well.

Definition 4.8 (Associated graded ring)**.** Fix a ring R and a filtration $\mathcal{J}$ notated

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

Then we set $R_i := I_i/I_{i+1}$ and define

$$\operatorname{gr}_{\mathcal{J}} R := \bigoplus_{p \geq 0} I_p/I_{p+1}$$

to be the *associated graded ring*. If $\mathcal{J}$ is the I-adic filtration, we denote the associated graded ring by $\operatorname{gr}_I(R)$. If the filtration is obvious, we will omit the subscript entirely.

A priori, the associated graded ring is only some very large module, but we can give it a ring structure as follows: if we have terms $[a] \in I_p/I_{p+1}$ and $[b] \in I_q/I_{q+1}$, then we can lift them to some $a \in I_p$ and $b \in I_q$ so that $ab \in I_pI_q \subseteq I_{p+q}$, so we set

$$[a] \cdot [b] := [ab] \in I_{p+q}/I_{p+q+1}.$$

We now run the following checks.

Lemma 4.9. Fix R a ring and filtration $\mathcal{J}$ notated

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

The above multiplication on $\operatorname{gr}_{\mathcal{J}} R$ makes $\operatorname{gr}_{\mathcal{J}} R$ into a graded ring in the natural way by $(\operatorname{gr}_{\mathcal{J}} R)_p := I_p/I_{p+1}$.

Proof. We start by showing that the multiplication of our "homogeneous" elements is well-defined. If $a \equiv a' \pmod{I_{p+1}}$ both represent $[a]$ and $b \equiv b' \pmod{I_{q+1}}$ both represent $[b]$, then

$$ab - a'b' = ab - ab' + ab' - a'b' = a(b - b') + (a - a')b'.$$

Now, $a \in I_p$ and $b - b' \in I_{q+1}$, so $a(b - b') \in I_{p+q+1}$; similarly, $a - a' \in I_{p+1}$ and $b' \in I_q$, so $(a - a')b \in I_{p+q+1}$. Thus, the entire element lives in I_{p+q+1}, so $ab \equiv a'b' \pmod{I_{p+q+1}}$.

Now we acknowledge that the above multiplication law extends distributively as

$$\left(\sum_{p\geq 0}[a_p]_{I_{p+1}}\right)\left(\sum_{q\geq 0}[b_q]_{I_q}\right) := \sum_{n\geq 0}\left(\sum_{p+q=n}[a_pb_q]_{I_{n+1}}\right).$$

So we have indeed defined a multiplication on all of $\operatorname{gr}_{\mathcal{J}} R$. We remark that we can see somewhat directly that one could imagine showing that the multiplication commutes (this is not so bad), associates (the point is to write the inner sum as $p + q + r = n$), and distributes (cry), but we will not write out these checks; the curious can port over the proof that multiplication in $R[x]$ forms a ring structure.

It remains to show that the ring is actually graded in the natural way. Specifically, we need to show that

$$(\operatorname{gr}_{\mathcal{J}} R)_p(\operatorname{gr}_{\mathcal{J}} R)_q \subseteq (\operatorname{gr}_{\mathcal{J}} R)_{p+q}.$$

But this is by definition of our multiplication: we see that $(\operatorname{gr}_{\mathcal{J}} R)_p(\operatorname{gr}_{\mathcal{J}} R)_q$ is generated by products

$$[a]_{I_{p+1}}[b]_{I_{q+1}} = [ab]_{I_{p+q+1}} \in (\operatorname{gr}_{\mathcal{J}} R)_{p+q},$$

where $[a]_{I_{p+1}} \in (\operatorname{gr}_{\mathcal{J}} R)_p$ and $[b]_{I_{q+1}} \in (\operatorname{gr}_{\mathcal{J}} R)_q$. ■

Remark 4.10. Technically we should say that the element

$$[1]_I + [0]_{I^2} + [0]_{I^3} + \cdots$$

is our unit element. Indeed, we can compute

$$([1]_I + [0]_{I^2} + [0]_{I^3} + \cdots) \cdot [a]_{I^n} = [a]_I^n$$

by looking component-wise, and our identity will extend to all of $\operatorname{gr}_{\mathcal{J}} R$ by how we defined our multiplication.

Remark 4.11 (Nir)**.** In fact, $\operatorname{gr}_I R$ is an R/I-module. Indeed, our map $R \to \operatorname{End}_R(\operatorname{gr}_I R)$ is created by stitching together the maps

$$R \to \operatorname{End}_R\left(I^p/I^{p+1}\right)$$

by $r \mapsto ([x] \mapsto [rx])$. However, we note that if $r \in I$ with $[x] \in I^p/I^{p+1}$, then $[rx] \in I^{p+1}/I^{p+1}$, so $[rx] = 0$. In particular, the above map has I in its kernel, so we actually get to stitch together the maps

$$R/I \to \operatorname{End}_R\left(I^p/I^{p+1}\right)$$

to a map $R/I \to \operatorname{End}_R(\operatorname{gr}_I R)$.

Aligned with the previous remark, we can use our grading to show that $\operatorname{gr}_I R$ is Noetherian in most cases we care about.

Lemma 4.12. Fix a Noetherian ring R endowed with some I-adic filtration. Then $\operatorname{gr}_I R$ is Noetherian.

Proof. Note R/I is Noetherian. Further, we can generate $\operatorname{gr}_I R$ as an R/I-algebra by the elements of I/I^2: it suffices to show how to generate any homogeneous element $[f]_{I^{k+1}}$, but $f \in I^k$ implies that we can write $f = f_1 \cdot \ldots \cdot f_k$ for $f_\bullet \in I^k$, so

$$[f]_{I^{k+1}} = [f_1]_{I^2} \cdot \ldots \cdot [f_k]_{I^2}$$

by using the multiplication of $\operatorname{gr}_I R$. But note $I \subseteq R$ is a finitely generated module over a Noetherian ring R and hence Noetherian, so I/I^2 is finitely generated over R and hence over R/I because the R-action is just an R/I-action.

Thus, $\operatorname{gr}_I R$ can use the finitely many generators of I/I^2 to be finitely generated as an R/I-algebra. It follows $\operatorname{gr}_I R$ is Noetherian by taking a quotient of Corollary 1.43. ■

Anyways, let's see some examples.

Exercise 4.13. Fix $R := k[\![x]\!]$ and $I := (x)$. We show that $\operatorname{gr}_I R \cong k[x]$ as graded rings.

Proof. Here we are using the I-adic filtration given by $I^n = (x)^n = (x^n)$. In particular, given any

$$f(x) = \sum_{d \geq n} a_d x^d \in (x^n)\,,$$

we see that $\sum_{d \geq n+1} a_d x^d \in \left(x^{n+1}\right)$, so we can give $f(x) \in I^n/I^{n+1}$ a fairly natural representative by

$$f(x) = a_n x^n + \sum_{d \geq n+1} a_d x^d \equiv a_n x^n \pmod{I^{n+1}}.$$

So, given $f(x) \in I^n/I^{n+1}$, we define $\varphi_n(f(x)) := a_n x^n$ so that $\varphi_n : I^n/I^{n+1} \to kx^n$. As such, we can assemble the φ_n into a map

$$\varphi : \bigoplus_{n \geq 0} I^n/I^{n+1} \to \bigoplus_{n \geq 0} kx^n$$

component-wise. Now, we observe that the domain of φ is $\operatorname{gr}_I R$ and the codomain is $k[x]$, so it remains to show that φ is an isomorphism of graded rings.

We start by showing that φ is a graded homomorphism. The grading part is fairly simple because φ restricts to $\varphi_n : I^n/I^{n+1} \to kx^n$ on each component, so φ does preserve the grading. Now, by the universal property of direct sums, it suffices to show that each φ_n is a group homomorphism. Well, if we pick up

$$f(x) = \sum_{d \geq n} a_d x^d \qquad \text{and} \qquad g(x) = \sum_{d \geq n} b_d x^d,$$

and we compute

$$\varphi_n\left([f]_{I^{n+1}} + [g]_{I^{n+1}}\right) = \varphi_n\left([f+g]_{I^{n+1}}\right) = a_n x^n + b_n x^n = \varphi_n\left([f]_{I^{n+1}}\right) + \varphi_n\left([g]_{I^{n+1}}\right).$$

Continuing, we see that φ preserves identity because

$$\varphi(1) = \varphi\left(\sum_{n \geq 0} [1_{n=0}]_{I^{n+1}}\right) = \sum_{n \geq 0} 1_{n=0} = 1.$$

Lastly, to check that φ is multiplicative, we note that our multiplication was uniquely determined by what it did to homogeneous elements, so it suffices to show that φ is multiplicative on homogeneous elements, for this will extend by distributivity. So pick up

$$f_n(x) = \sum_{d \geq n} a_d x^d \qquad \text{and} \qquad g_m(x) = \sum_{e \geq m} b_e x^e$$

so that $\varphi_n(f_n) = a_d$ and $\varphi_m(g_m) = b_m x^m$. Then $[f_n]_{I^{n+1}} = [a_n x^n]_{I^{n+1}}$ and $[g_m]_{I^{m+1}} = [b_m x^m]_{I^{m+1}}$ so that the well-definedness of our multiplication promises

$$\varphi_{n+m}\left([f_n]_{I^{n+1}} \cdot [g_m]_{I^{m+1}}\right) = \varphi_{n+m}\left([a_n b_m x^{n+m}]_{I^{n+m+1}}\right) = a_n x^n \cdot b_m x^m = \varphi_n\left([f_n]_{I^{n+1}}\right) \cdot \varphi_m\left([g_m]_{I^{m+1}}\right),$$

which is what we wanted. To be convinced that our distributivity hand-waving is legitimate, we note that we could write out

$$\varphi\left(\sum_{p\ge 0}[f_p] \cdot \sum_{q\ge 0}[g_q]\right) = \varphi\left(\sum_{p+q=n}[f_p g_q]\right) = \sum_{p+q=n}\varphi_{p+q}([f_p g_q]) = \sum_{p+q=n}\varphi_p([f_p])\varphi_q([g_q]),$$

which we can then distribute backwards to $\varphi\left(\sum_p [f_p]\right)\varphi\left(\sum_q [g_q]\right)$.

It remains to show that φ is a bijection. For this, it suffices to show that φ is an isomorphism of R-modules, for which we note that it suffices to check that φ restricts to an isomorphism on each component $\varphi_n : I^n/I^{n+1} \to kx^n$. In fact, we already know that this is a group homomorphism (because φ is additive), so we merely need to know that φ_n is bijective.

- We show that φ_n is surjective. Well, given $a_n x^n$, we see that $\varphi_n\left([a_n x^n]_{I^{n+1}}\right) = a_n x^n$.
- We show that φ_n is injective. Well, suppose that $f \in I^n$ has $\varphi_n\left([f]_{I^{n+1}}\right) = 0x^n$. Then, by definition, our expansion
$$f(x) = \sum_{d\ge n} a_d x^d$$
has $a_n = 0$. In particular, we can write $f(x) = \sum_{d\ge n+1} a_d x^d$ so that $f(x) \in I^{n+1}$, so $[f]_{I^{n+1}} = [0]_{I^{n+1}}$, which is what we wanted.

The above checks finish the proof that φ is an isomorphism. ■

We will be briefer with our next examples because they are similar.

Example 4.14. Fix $R = \mathbb{Z}$ and $I = (p)$ a prime ideal, where $p > 0$ is a positive prime. Then, in $I^n/I^{n+1} = p^n\mathbb{Z}/p^{n+1}\mathbb{Z}$, all elements have a unique representative as $[p^n a]_{p^{n+1}}$ for $a \in \mathbb{Z}/p\mathbb{Z}$, so we can represent anyone in $\operatorname{gr}_I R$ by

$$a_0 + a_1 p + a_2 p^2 + \cdots$$

where $a_0, a_1, a_2 \ldots \in \mathbb{Z}/p\mathbb{Z}$. Thus, we can see that multiplication of homogeneous elements behaves as

$$\left[a_k p^k\right]_{p^{k+1}} \cdot \left[b_\ell p^\ell\right]_{p^{\ell+1}} = \left[a_k b_\ell p^{k+\ell}\right]_{p^{k+\ell+1}}.$$

In particular, if we imagine taking $p \mapsto x$, the above is really the polynomial grading, so we see that extending $p \mapsto x$ to all of $\operatorname{gr}_{(p)} \mathbb{Z}$ gives an isomorphism $\operatorname{gr}_{(p)} \mathbb{Z} \cong (\mathbb{Z}/p\mathbb{Z})[x]$.

Remark 4.15 (Nir)**.** Essentially the same reasoning as Exercise 4.13 can show that $\operatorname{gr}_{(x)} k[x] \cong k[x]$. In fact, the reasoning generalizes to

$$\operatorname{gr}_{(x_1,\ldots,x_n)} k[x_1,\ldots,x_n] \cong k[x_1,\ldots,x_n]$$

by again just matching up graded components, but we won't write this out.

4.1.4 Initial Forms

We begin with the following warning.

Warning 4.16. There is no natural ring homomorphism $R \to \operatorname{gr}_{\mathcal{J}} R$.

This is sad because we would like to use the associated graded ring to understand the original ring, so not having a natural map significantly hinders our ability.

However, there is a natural map of sets.

Definition 4.17 (Initial form)**.** Fix R a ring and $\mathcal{J}$ a filtration notated

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

Then, fix $f \in R$, and we define the *initial form of f* $\operatorname{in} f \in \operatorname{gr}_I R$ as follows.

- If $f \in I_p$ for all p, then $\operatorname{in} f = 0$.
- If $f \in I_p$ but $f \notin I_{p+1}$, then $\operatorname{in} f = [f]_{I_{p+1}}$.

Intuitively, in extracts the smallest "homogeneous" part of f to put in $\operatorname{gr}_I R$; we return 0 when this is impossible.

This map of sets really does not have extra structure, though it feels like it comes close, which is reassuring.

Remark 4.18 (Nir)**.** To see that in is not a ring homomorphism, we see that it is not additive. Consider $R = k[x]$ given the (x)-adic filtration.

- Take $f = x$ so that $\operatorname{in} f = [x]_{x^2}$.
- Take $g = x^2$ so that $\operatorname{in} g = \left[x^2\right]_{x^3}$.
- Then $f + g = x + x^2$ so that $\operatorname{in}(f + g) = [x]_{x^2}$.

Notably, $\operatorname{in} f + \operatorname{in} g$ is not even homogeneous, but the image of in always is.

There is a partial salvage for the above remark, however.

Proposition 4.19. Fix R a ring and $\mathcal{J}$ a filtration

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

Then, given $f, g \in R$, if $\operatorname{in} f + \operatorname{in} g \neq 0$, then we have $\operatorname{in}(f + g) \in \{0, \operatorname{in} f, \operatorname{in} g, \operatorname{in} f + \operatorname{in} g\}$.

Proof. This is a proof by tinkering.

If $\operatorname{in} f = 0$ and $\operatorname{in} g = 0$, then $f + g \in I^s$ for all s, so $\operatorname{in}(f + g) = 0$. So we may assume at least one of $\operatorname{in} f \neq 0$ or $\operatorname{in} g \neq 0$; without loss of generality, take $\operatorname{in} f \neq 0$ with $f \in I^s$ while $f \notin I^{s+1}$. Now, if $\operatorname{in} g = 0$, we see $f + g \equiv f \not\equiv 0 \pmod{I^{s+1}}$, so

$$\operatorname{in}(f + g) = [f]_{I^{s+1}} = \operatorname{in}(f).$$

Otherwise, we can assume that $g \in I^q$ while $g \notin I^{q+1}$ for some s and q; in particular, $\operatorname{in} f = [f]_{I^{s+1}}$ and $\operatorname{in} g = [g]_{I^{q+1}}$. Without loss of generality, we take $s \le q$. We have the following cases.

- If $s < q$, then $g \in I^{s+1}$, so $f + g \equiv f \pmod{I^{s+1}}$, so $\operatorname{in}(f + g) = \operatorname{in} f$.
- Otherwise, $s = q$. Only now do we bring in the hypothesis that $\operatorname{in} f + \operatorname{in} g \neq 0$, for which we see that $f + g \in I^{s+1}$ is impossible because it would give

$$\operatorname{in} f + \operatorname{in} g = [f]_{I^{s+1}} + [g]_{I^{s+1}} = [0]_{I^{s+1}}.$$

Thus, $f+g\notin I^{s+1}$, but certainly $f,g\in I^s$ implies $f+g\in I^s$, so

$$\operatorname{in}(f+g)=[f+g]_{I^s}=[f]_{I^s}+[g]_{I^s}=\operatorname{in}f+\operatorname{in}g,$$

which covers our last case.

The above casework has now covered all possibilities, so we are done. ■

In fact, in need not even be multiplicative, though it is almost multiplicative.

Proposition 4.20. Fix R a ring and $\mathcal{J}$ a filtration

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

Then, given $f,g\in R$, we have $\operatorname{in}f\cdot\operatorname{in}g\in\{\operatorname{in}(fg),0\}$. If $\operatorname{gr}_{\mathcal{J}}R$ is an integral domain, then $\operatorname{in}f\cdot\operatorname{in}g=\operatorname{in}(fg)$.

Proof. Very quickly, suppose that one of f or g lives in I_p for all P. Without loss of generality, say that $f\in I_p$ for all I_p, so $fg\in I_p\in I_p$ for all p, so

$$\operatorname{in}(fg)=0=\operatorname{in}f=\cdot\operatorname{in}f\cdot\operatorname{in}g,$$

dealing with the case of $\operatorname{gr}_{\mathcal{J}}R$ an integral domain automatically as well.

Otherwise, we have $f\in I_p\setminus I_{p+1}$ and $g\in I_q\setminus I_{q+1}$ for some p and q so that $\operatorname{in}f=[f]_{I_{p+1}}$ and $\operatorname{in}g=[g]_{I_{q+1}}$. Because $\mathcal{J}$ is a filtration, we see that

$$fg\in I_pI_q\subseteq I_{p+q}.$$

We now have two cases.

- If $fg\notin I_{p+q+1}$, then $\operatorname{in}(fg)=[fg]_{I_{p+q+1}}=[f]_{I_{p+1}}\cdot[g]_{I_{q+1}}=\operatorname{in}f\cdot\operatorname{in}g$.
- If $fg\in I_{p+q+1}$, then $\operatorname{in}f\cdot\operatorname{in}g=[fg]_{I_{p+q+1}}=0$.

The above casework finishes the proof of the general case. When $\operatorname{gr}_{\mathcal{J}}R$ is an integral domain, we note that $\operatorname{in}f,\operatorname{in}g\neq 0$ disallows the second case, so we will always have $\operatorname{in}f\cdot\operatorname{in}g=\operatorname{in}(fg)$. ■

4.1.5 Tangent Cone

It turns out that the associated graded ring has a nice geometric application.

Proposition 4.21. We work in $\mathbb{A}^n(k)$. Fix $J\subseteq k[x_1,\ldots,x_n]$ an ideal with $X\subseteq\mathbb{A}^n(k)$ a Zariski closed set with $X=Z(J)$. Further, suppose $J\subseteq(x_1,\ldots,x_n)=:\mathfrak{m}$ so that $0\in X$. Then we claim that

$$\operatorname{in}J\subseteq\operatorname{gr}_{\mathfrak{m}}A(X)$$

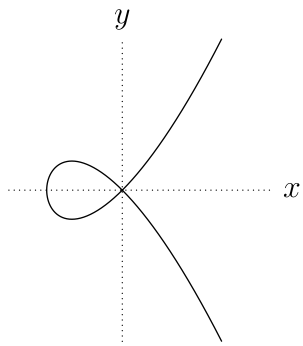
defines the coordinate ring of the "tangent cone of X at 0," made up of the lines tangent to X at 0.

Proof. We will omit this proof. ■

Nevertheless, we will give two motivating examples for Proposition 4.21.

Exercise 4.22. We work through Proposition 4.21 for the affine variety defined by $y^2=x^2(x+1)$.

Proof. Here, $J=\left(y^2-x^2(x+1)\right)$, and X looks like the following.



Notably, $J \subseteq (x,y)$, so $0 \in X$. Visually, we can see that X has two tangent lines at 0; let's compute them. Differentiating $y^2 = x^3 + x$ implicitly, we see that

$$2yy' = 3x^2 + 2x,$$

so away from $(0,0)$ we have

$$(y')^2 = \frac{\left(3x^2+2x\right)^2}{4y^2} = \frac{\left(2x+3x^2\right)^2}{4x^2(x+1)} = \frac{(2+3x)^2}{4(1+x)}.$$

Assuming that our derivatives are continuous because look at them, we send $x \to 0$ to conclude that $(y')^2 = 1$ at $(0,0)$. But this permits $y' = 1$ or $y' = -1$, which we see are indeed both legal solutions to our diagram.

Now, $y' = 1$ and $y' = -1$ correspond to the lines $x = y$ and $x = -y$, so the tangent cone is the union of these two lines, which is the variety defined by the equation $x^2 - y^2 = (x-y)(x+y) = 0$. Thus, the coordinate ring of the tangent cone is

$$\frac{k[x,y]}{(x^2-y^2)}.$$

We now turn to algebra to verify this; we are staring at

$$\operatorname{in} J \subseteq \operatorname{gr}_{\mathfrak{m}} k[x,y].$$

Note $\operatorname{gr}_{\mathfrak{m}} k[x,y] = k[x,y]$ from Remark 4.15, so we just need to track $\operatorname{in} J$ through this isomorphism, which basically means that we need to compute $\operatorname{in} J$. Well, because $\operatorname{gr}_{\mathfrak{m}} k[x,y]$ is a domain, we see from Proposition 4.20 that any $r\left(y^2 - x^2(x+1)\right) \in J$ has

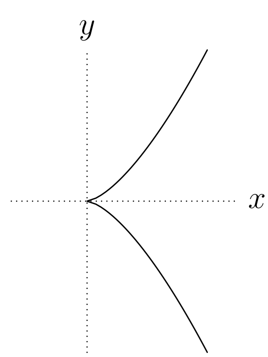
$$\operatorname{in}\left(r\left(y^2 - x^2(x+1)\right)\right) = \operatorname{in}(r)\operatorname{in}\left(y^2 - x^2(x+1)\right) = \operatorname{in}(r)\operatorname{in}\left(y^2 - x^2 + x^3\right) = \operatorname{in}(r)\cdot\left[y^2 - x^2\right]_{(x,y)^3}.$$

Now, because $\operatorname{in}(r)$ does cover all of $\operatorname{gr}_{\mathfrak{m}} k[x,y]$, we see that $\operatorname{in} J = \left([y^2-x^2]_{\mathfrak{m}^3}\right)$.

So upon tracking our graded isomorphism from Remark 4.15 through, we see that we are looking at the variety defined by $y^2 - x^2 \subseteq k[x,y]$, which is exactly the two lines $y = x$ and $y = -x$ that we wanted. ■

Exercise 4.23. We work through Proposition 4.21 for the affine variety defined by $y^2 = x^3$.

Proof. Here, $J = \left(y^2 - x^3\right)$, and X looks like the following.



Notably, $J \subseteq (x, y)$, so $0 \in X$. Visually, we can see that X has only the one tangent line $y = 0$ at $(0, 0)$. Indeed, differentiating $y^2 = x^3$ implicitly, we get $2yy' = 3x^2$, so

$$2x^3 y' = 2y^2 (y')^2 = 9x^4,$$

so $y' = \frac{9}{2}x$ away from $(0, 0)$. Sending x to 0 does recover $y' = 0$. In particular, our tangent cone should be $y = 0$, whose coordinate ring is

$$\frac{k[x, y]}{(y)}.$$

And now for algebra. Using the same logic as before, we have from Proposition 4.20 that

$$\operatorname{in} J = \operatorname{in}\left(\left(y^2 - x^3\right) k[x, y]\right) = \operatorname{in}\left(y^2 - x^3\right) \operatorname{in} k[x, y] = \left(\left[y^2\right]_{(x,y)^3}\right).$$

In particular, tracking Remark 4.15 through, we are looking at the variety defined by $y^2 \in k[x, y]$, which is exactly the line $y = 0$ that we wanted. ■

4.1.6 Filtrations of Modules

Consider the following construction.

Definition 4.24 (Hilbert function, rings)**.** Fix R a local Noetherian ring with maximal ideal $\mathfrak{m}$. Then we define the *Hilbert function of R* as

$$H_R(s) := \dim_{R/\mathfrak{m}} (\operatorname{gr}_{\mathfrak{m}} R)_s = \dim_{R/\mathfrak{m}} \left(\mathfrak{m}^s / \mathfrak{m}^{s+1}\right).$$

Note that this definition is well-formed because R/I is a field.

We note that the definition of $H_R(s)$ is well-formed: $\mathfrak{m}^s / \mathfrak{m}^{s+1}$ is in fact an $R/\mathfrak{m}$-module by Remark 4.11, which is actually an $R/\mathfrak{m}$-vector space because $R/\mathfrak{m}$ is a field. As for finiteness, $\mathfrak{m}^s$ is a finitely generated R-module (because R is Noetherian), so $\mathfrak{m}^s / \mathfrak{m}^{s+1}$ is as well, so $\mathfrak{m}^s / \mathfrak{m}^{s+1}$ is a finite-dimensional $R/\mathfrak{m}$-vector space.

The theory of the Hilbert function was actually stated for modules, so we would like to generalize this to modules. We have the following series of definitions.

Definition 4.25 (Filtration, modules)**.** Given an R-module M, a *filtration* is a descending chain

$$M = M_0 \supseteq M_1 \supseteq M_2 \supseteq \cdots.$$

Given an ideal I, the above is an *I-filtration* if and only if $IM_q \subseteq M_{q+1}$. Note that this last condition is equivalent to $I^s M_q \subseteq M_{s+q}$ by an induction.

Note there is no multiplicative condition on the filtration because M has no multiplication.

As before, from filtrations we can build the associated graded module.

Definition 4.26 (Associated graded module)**.** Fix an R-module M with a filtration $\mathcal{J}$, denoted by

$$M = M_0 \supseteq M_1 \supseteq M_2 \supseteq \cdots.$$

Then we define

$$\operatorname{gr}_{\mathcal{J}} M := \bigoplus_{s \geq 0} M_s / M_{s+1} = M/M_1 \oplus M_1/M_2 \oplus \cdots.$$

A priori, $\operatorname{gr}_{\mathcal{J}} M$ merely has an R-module structure inherited as a direct sum, but when $\mathcal{J}$ is an I-filtration, then we do get a graded structure from our graded module.

Lemma 4.27. Fix an R-module and $I \subseteq R$ an ideal. If M is an R-module with an I-filtration $\mathcal{J}$ denoted by

$$M = M_0 \supseteq M_1 \supseteq M_2 \supseteq \cdots,$$

then $\operatorname{gr}_{\mathcal{J}} M$ is a $\operatorname{gr}_I R$-module.

Proof. We start by describing our action. Given $[a]_{I^{s+1}} \in I^s/I^{s+1}$ and $[b]_{M_{q+1}} \in M_q/M_{q+1}$, we see that

$$ab \in I^s M_q \subseteq M_{s+q}.$$

In fact, if we pick up another representative $[a] = [a']$ and $[b] = [b']$, then

$$ab - a'b' = ab - ab' + ab' - a'b' = a(b - b') + (a - a')b' \in I^s M_{q+1} + I^{s+1} M_q \subseteq M_{s+q+1}.$$

Thus, the representative $[ab]_{M_{s+q+1}} \in M_{s+q}/M_{s+q+1}$ is unique of the exact choice of representative for a and b. We have the following checks on this action.

- Fix $[a]_{I^{s+1}}$; then the action on M_q is R-linear: we compute

  $$[a]_{I^{s+1}} \cdot \left(r_1[b_1]_{M_{q+1}} + r_2[b_2]_{M_{q+1}}\right) = [ar_1b_1 + ar_2b_2]_{M_{q+1}} = r_1\left([a]_{I^{s+1}} \cdot [b_1]_{M_{q+1}}\right) + r_2\left([a]_{I^{s+1}} \cdot [b_2]_{M_{q+1}}\right).$$

  In particular, we see that we have defined a function

  $$(\operatorname{gr}_I R)_s \to \operatorname{Hom}_R\left((\operatorname{gr}_{\mathcal{J}} M)_q, (\operatorname{gr}_{\mathcal{J}} M)_{q+s}\right)$$

- The function defined in the previous point is R-linear. Namely, we compute

  $$(r_1[a_1]_{I^{s+1}} + r_2[a_2]_{I^{s+1}}) \cdot [b]_{M_{q+1}} = [r_1a_2b + r_2a_2b]_{I^{s+1}} = [r_1a_1 + r_2a_2]_{I^{s+1}} \cdot [b]_{M_{q+1}},$$

  so it follows that the action by $r_1[a_1]_{I^{s+1}} + r_2[a_2]_{I^{s+1}}$ is equal to the action by $[r_1a_1 + r_2a_2]_{I^{s+1}}$.

So we have an R-module homomorphism

$$(\operatorname{gr}_I R)_s \to \operatorname{Hom}_R\left((\operatorname{gr}_{\mathcal{J}} M)_q, (\operatorname{gr}_{\mathcal{J}} M)_{q+s}\right)$$

is in fact an R-module homomorphism. By the tensor-hom adjunction, this induces a morphism

$$(\operatorname{gr}_I R)_s \otimes_R (\operatorname{gr}_{\mathcal{J}} M)_q \to (\operatorname{gr}_{\mathcal{J}} M)_{q+s} \hookrightarrow \operatorname{gr}_{\mathcal{J}} M$$

by $[a]_{I^{s+1}} \otimes [b]_{M_{q+1}} \mapsto [ab]_{M_{q+s+1}}$. We see that we can assemble the above morphisms into a large morphism

$$\bigoplus_{s,q \geq 0} \left((\operatorname{gr}_I R)_s \otimes_R (\operatorname{gr}_{\mathcal{J}} M)_q\right) \to \operatorname{gr}_{\mathcal{J}} M$$

by $\sum_{s,q}[a_s]_{I^{s+1}} \otimes [b_q]_{M_{q+1}} \mapsto \sum_{s,q}[a_sb_q]_{M_{q+s+1}}$. Because tensor products commute with tensor products, we get a morphism

$$(\operatorname{gr}_I R) \otimes_R (\operatorname{gr}_{\mathcal{J}} M) \to \operatorname{gr}_{\mathcal{J}} M$$

by $(\sum_s [a_s]_{I^{s+1}}) \otimes \left(\sum_q [b_q]_{M_{q+1}}\right) \mapsto \sum_{s,q}[a_sb_q]_{M_{q+s+1}}$. Using the tensor-hom adjuction once more, we get an R-module homomorphism

$$\operatorname{gr}_I R \to \operatorname{End}_R(\operatorname{gr}_{\mathcal{J}} M),$$

which verifies that we have an action by

$$\left(\sum_{s \geq 0}[a_s]_{I^{s+1}}\right) \cdot \left(\sum_{q \geq 0}[b_q]_{M_{q+1}}\right) = \sum_{s,q \geq 0} [a_sb_q]_{M_{q+s+1}}.$$

In particular, we see that $(\operatorname{gr}_{\mathcal{I}} R)_s \cdot (\operatorname{gr}_{\mathcal{J}} M)_q \subseteq (\operatorname{gr}_{\mathcal{J}} M)_{q+s}$ by construction of our action: either we can check this directly above as $[a_s]_{I^{s+1}} \cdot [b_q]_{M_{q+1}} = [a_sb_q]_{M_{q+s+1}}$, or we can see it from the original construction. So our action in fact makes a graded module, as we wanted. ■

It is somewhat natural to expect that the "best" I-filtration for a module M is the filtration

$$M \supseteq IM \supseteq I^2M \supseteq \cdots .$$

This specific filtration will turn out to be overly restrictive for our purposes, so we have the following definition.

Definition 4.28 (Stable)**.** An I-filtration of an R-module M, denoted by

$$M = M_0 \supseteq M_1 \supseteq M_2 \supseteq \cdots ,$$

is I*-stable* if and only if $M_{j+1} = IM_j$ for sufficiently large j.

As a sign that we have done something good, it turns out that stability will communicate nicely with the module structure of $\operatorname{gr}_{\mathcal{J}} M$.

Proposition 4.29. Fix $I \subseteq R$ an ideal. Further, take M to be a finitely generated R-module with a stable I-filtration $\mathcal{J}$ by finitely generated modules. Then $\operatorname{gr}_{\mathcal{J}} M$ is a finitely generated $\operatorname{gr}_I R$-module.

Proof. We definition-chase. Let our filtration $\mathcal{J}$ be

$$M = M_0 \supseteq M_1 \supseteq M_2 \supseteq \cdots .$$

Because $\mathcal{J}$ is I-stable, we are promised some N such that $M_{N+p} = I^pM_N$ for $p \geq 0$. As such, we choose generators for $M_0, \ldots, M_n$ over R to generate $\operatorname{gr}_{\mathcal{J}} M$ as a $\operatorname{gr}_I R$-module.

More explicitly by extending our number of generators, we can find m elements to generate each M_i for $0 \leq i \leq n$ (e.g., set m to be the largest number of generators used for any M_i and then add 0s until done); observe we may find finitely any generators for each M_i by hypothesis. Now, label the m generators for M_i by $\{x_{i1}, \ldots, x_{im}\}$. We would like to use these elements to generate

$$\operatorname{gr}_{\mathcal{J}} M = \bigoplus_{i \geq 0} M_i/M_{i+1}.$$

We have two cases.

- Fix $0 \leq i \leq N$ so that we claim the $\left\{[x_{ij}]_{M_{i+1}}\right\}_{j=1}^m$ will generate M_i/M_{i+1}. Well, fix any element $x \in M_i$, and by construction, we may write

  $$x = \sum_{j=1}^m r_jx_{ij}$$

  for some elements $r_1, \ldots, r_j \in R$. Modding out, we have

  $$[x]_{M_{i+1}} = \sum_{j=1}^m \cdot [r_jx_{ij}]_{M_{i+1}},$$

  where this is taking place in M_i/M_{i+1} as an R-module.

  If $r_j \in I$, then $r_jx_{ij} \in IM_i \subseteq M_{i+1}$, so this term vanishes, and we may erase it completely. Similarly, if $x_{ij} \in M_{i+1}$, then the term vanishes, and we may erase it. So we write

  $$[x]_{M_{i+1}} = \sum_{\substack{j=1 \\ r_j \notin I, x_{ij} \notin M_{i+1}}}^m r_j \cdot [x_{ij}]_{M_{i+1}}.$$

However, for each of the remaining terms, we see that $\operatorname{in} r_j = [r_j]_I$ and $\operatorname{in} x_{ij} = [x_{ij}]_{M_{i+1}}$ with $[r_j]_I \cdot [x_{ij}]_{M_{i+1}} = [r_j x_{ij}]_{M_{i+1}}$ by definition of our action. This tells us that

$$[x]_{M_{i+1}} = \sum_{\substack{j=1 \\ r_j \notin I, x_{ij} \notin M_{i+1}}}^{m} [r_j]_I \cdot [x_{ij}]_{M_{i+1}},$$

where now this equation lives in $\operatorname{gr}_{\mathcal{J}} M$ as a $\operatorname{gr}_I R$-module. So we are done.

- Now fix $N + i > N + 1$ so that we claim the $\{[x_{Nj}]_{M_{N+1}}\}_{j=1}^m$ will generate M_{i+N}/M_{i+N+1} in $\operatorname{gr}_{\mathcal{J}} M$. Well, the key is that are given that $M_{N+i} = I^i M_N$ by stability, so fixing some element $x \in M_{N+i}$, we can write
$$x = rx',$$
where $r \in I^i$. If $r \in I^{i+1}$, then $x \in I^{i+1}M_N = M_{i+N+1}$, so $[x]_{M_{i+N+1}} = 0$, and there's nothing more to say. Similarly, if $x' \in M_{N+1}$, then $x \in I^i M_{N+1} = M_{i+N+1}$, so $[x]_{M_{i+N+1}} = 0$, and we are again done. So we may assume that $r \in I^i \setminus I^{i+1}$ and $x' \in M_N \setminus M_{N+1}$. But now
$$\operatorname{in} r \cdot \operatorname{in} x' = [r]_{I^i} \cdot [x']_{M_{N+1}} = [rx']_{M_{i+N+1}}$$
in $\operatorname{gr}_{\mathcal{J}} M$. To finish, we know from the previous point that $\{[x_{Nj}]_{M_{N+1}}\}_{j=1}^m$ will be able to hit $[x']_{M_{N+1}} \in M_N/M_{N+1}$, so now we just need to multiply all the coefficients in the expansion by $\operatorname{in} r$ to finish.

The above casework finishes the proof. ■

Anyways, we are now allowed to define the Hilbert function for modules.

Definition 4.30 (Hilbert function)**.** Fix R a local Noetherian ring where $\mathfrak{m}$ is the maximal ideal with M a finitely generated R-module. Then we define

$$H_M(s) = \dim_{R/\mathfrak{m}} \left(\mathfrak{m}^s M/\mathfrak{m}^{s+1} M\right).$$

Again, $\mathfrak{m}^s M/\mathfrak{m}^{s+1} M$ is an $R/\mathfrak{m}$-vector space because multiplication by any element $\mathfrak{m}$ will zero out the element. To see that it is finite-dimensional, we note that M is Noetherian (because it is finitely generated over the Noetherian ring R), so the submodule $\mathfrak{m}^s M \subseteq M$ is finitely generated, so $\mathfrak{m}^s M/\mathfrak{m}^{s+1} M$ is also finitely generated.

4.1.7 Blow-Up Rings

We are finally ready to state our main result.

Theorem 4.31 (Artin–Rees lemma)**.** Fix R a Noetherian ring and $I \subseteq R$ an ideal with M a finitely generated R-module granted a stable I-filtration $\mathcal{J}$ denoted by

$$M = M_0 \supseteq M_1 \supseteq M_2 \supseteq \cdots.$$

Then given a submodule $M' \subseteq M$, the induced filtration by $M'_k := M_k \cap M'$ is also a stable I-filtration.

For the proof, we will want to introduce the blow-up ring.

Definition 4.32 (Blow-up ring)**.** Fix R a ring and $I \subseteq R$ an ideal. Then we define the *blow-up ring* $\operatorname{B}_I R$ by

$$\operatorname{B}_I R := R \oplus I \oplus I^2 \oplus \cdots.$$

Concretely, think about $\operatorname{B}_I R$ as getting its ring structure from $R[t]$ as "$R[It]$," which also gives us our grading. We have the following checks.

Lemma 4.33. Fix R a ring and $I \subseteq R$ an ideal. The ring $\mathrm{B}_I R$ is an R-algebra and a graded ring (in the natural way).

Proof. Our main check is that $\mathrm{B}_I R$ is a ring, for which we have to define our multiplication. This is defined in the natural way: given $x \in I^s$ and $y \in I^q$, then we consider the product $xy \in I^s I^q = I^{s+q}$. In particular, this gives us a map

$$I^s \times I^q \to I^{s+q}. \tag{$*$}$$

We can check that this map is R-bilinear: if $r_1, r_2 \in R$ with $x_1, x_2 \in I^s$ and $s_1, s_2 \in R$ with $y_1, y_2 \in I^q$, then

$$(r_1x_1 + r_2x_2)(s_1y_1 + s_2y_2) = r_1s_1(x_1y_1) + r_1s_2(x_1y_2) + r_2s_1(x_2y_1) + r_2s_2(x_2y_2),$$

by rearranging in R. However, this is exactly the R-bilinearity check, so we get a map

$$I^s \otimes_R I^q \to I^{s+q} \hookrightarrow \bigoplus_{i\ge 0} I^i$$

by $x \otimes y \mapsto xy$, essentially by the universal property of the tensor product. These stitch together into a map

$$\left(\bigoplus_{s\ge 0} I^s\right) \otimes_R \left(\bigoplus_{q\ge 0} I^q\right) \simeq \bigoplus_{s,q\ge 0} (I^s \otimes_R I^q) \to \bigoplus_{i\ge 0} I^i$$

by $(\sum_s a_s) \otimes \left(\sum_q b_q\right) \mapsto \sum_{s,q} a_s b_q$, essentially using how tensor products play with direct sums. Going backwards, we are thus promised an R-bilinear map

$$\mathrm{B}_I R \times \mathrm{B}_I R \to \mathrm{B}_I R$$

by

$$\left(\sum_s a_s, \sum_q b_q\right) \mapsto \sum_{s,q} a_s b_q,$$

which is exactly our ring multiplication. Notably, we can see that this multiplication commutes because multiplication commutes in R; this associates by association in R; this distributes by the R-bilinearity of the map; and our unit element is $(1, 0, 0, \ldots)$ because $1b_q = b_q$ for each b_q, and all other terms vanish.

For the grading, we merely have to check that $(\mathrm{B}_I R)_s(\mathrm{B}_I R)_q = I^s I^q \subseteq I^{s+q} = (\mathrm{B}_I R)_{s+q}$, which is true by $(*)$. Lastly, we are an R-algebra because $\mathrm{B}_I R$ is an R-module component-wise, and we merely added the ring structure on top. ■

Remark 4.34 (Nir)**.** In fact, if R is Noetherian, then $\mathrm{B}_I R$ is also Noetherian. Indeed, $I \subseteq R$ must be finitely generated, so write $I = (f_1, \ldots, f_n)$. The main claim is that $R[x_1, \ldots, x_n] \twoheadrightarrow \mathrm{B}_I R$ via extending $R \hookrightarrow \mathrm{B}_I R$ by $x_\bullet \mapsto f_\bullet \in I = (\mathrm{B}_I R)_1$.

This comes down to seeing that the component $(\mathrm{B}_I R)_s = I^s$ is generated by products of the form

$$f_1^{\alpha_1} \cdots f_n^{\alpha_n}$$

with $\alpha_1 + \cdots + \alpha_n = s$, but this element is hit by $x_1^{\alpha_1} \cdots x_n^{\alpha_n}$. In fact the grading matches because each x_i goes to a degree-1 element, so $x_1^{\alpha_1} \cdots x_n^{\alpha_n}$ goes to a degree-s element in $(\mathrm{B}_I R)_s$.

To finish, we see $R[x_1, \ldots, x_n]$ is Noetherian by Proposition 4.40, so $\mathrm{B}_I R$ is Noetherian by taking the quotient (e.g., using Proposition 1.40).

Because the associated graded ring was supposed to be "the" way to create a ring out of a filtration, it is reassuring that we can relate the associated graded ring to the blow-up ring.

Lemma 4.35. Fix R a ring and $I \subseteq R$ an ideal. Then $\operatorname{B}_I R / I \operatorname{B}_I R \cong \operatorname{gr}_I R$ as graded rings.

Proof. It is not too difficult to create an isomorphism of R-modules. Indeed, we see that

$$I \operatorname{B}_I R = I\left(\bigoplus_{s\geq 0} I^s\right) = \bigoplus_{s\geq 0} II^s = \bigoplus_{s\geq 0} I^{s+1}$$

by definition of our R-action. In particular, we can compute our quotient as

$$\varphi : \frac{\operatorname{B}_I R}{I \operatorname{B}_I R} = \frac{\bigoplus_{s\geq 0} I^s}{\bigoplus_{s\geq 0} I^{s+1}} \cong \bigoplus_{s\geq 0} \frac{I^s}{I^{s+1}} = \operatorname{gr}_I R.$$

Technically, some care is required on $\cong$, but it amounts to stitching together the short exact sequences

$$0 \to I^{s+1} \to I^s \to I^s/I^{s+1} \to 0$$

into the short exact sequence

$$0 \to \bigoplus_{s\geq 0} I^{s+1} \to \bigoplus_{s\geq 0} I^s \to \bigoplus_{s\geq 0} I^s/I^{s+1} \to 0,$$

which witnesses the desired isomorphism.

It remains to show that the composite φ is an isomorphism of graded rings. Well, we compute

$$\varphi\left(\left[\sum_{s\geq 0} a_s\right] \cdot \left[\sum_{q\geq 0} b_q\right]\right) = \varphi\left(\sum_{s,q\geq 0} [a_s b_q]\right) = \sum_{s,q\geq 0} [a_s b_q]_{I^{s+q+1}}$$

by keeping track of our grading. From the above, we can un-distribute back to $\varphi\left(\left[\sum_s a_s\right]\right)\varphi\left(\left[\sum_q b_q\right]\right)$, which finishes. To see that this isomorphism has degree-0, we note $\varphi([a_s]\cdot[b_q]) = [a_s b_q]_{I^{s+q+1}}$ for $a_s \in I^s$ and $b_q \in I^q$. ■

We briefly discuss the geometric meaning to blowing up.

Exercise 4.36. We interpret blowing up in the case of $R := k[x,y]$ at the "point"/maximal ideal $I = (x,y)$.

Proof. Fix $R := k[x,y]$ and consider $(0,0) \in \mathbb{A}^2(k)$ with associated maximal ideal $I := (x,y) \subseteq R$. In this case, our blow-up ring is

$$\operatorname{B}_I R = R \oplus I \oplus I^2 \oplus \cdots = k[x,y] \oplus (x,y) \oplus \left(x^2, xy, y^2\right) \oplus \cdots.$$

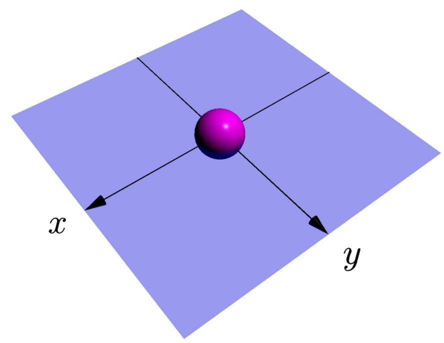
Intuitively, we can think of this as $k[x,y][tx,ty] \subseteq k[x,y][t]$, where we map $I = (x,y) \mapsto (tx,ty)$ to associate the grading. A more hands-free way to rigorize $k[x,y][tx,ty]$ is to imagine the projection

$$k[x,y][u,v] \twoheadrightarrow k[x,y][tx,ty]$$

by taking $u \mapsto tx$ and $v \mapsto ty$. We can verify by hand that $yu - xv$ is in the kernel of this map, and one can show that it generates the kernel, but we will not do this.

Now we proceed with our discussion, in two ways.

- Look at $Z \subseteq \mathbb{A}^2(k) \times \mathbb{P}^1(k)$ to be points (p,ℓ) such that $p \in \ell$. Intuitively, what we have done is to replace the point $(0,0) \in \mathbb{A}^2(k)$ with a copy of $\mathbb{P}^1(k)$, which looks more like a 2-sphere, hence the name "blowing up." This looks like the following.



We can project $Z \twoheadrightarrow \mathbb{A}^2(k)$ in the natural way by $(p, \ell) \mapsto p$. As long as $p \neq 0$, there is exactly one pre-image. But if $p = 0$, then our pre-image contains all the lines in $\mathbb{P}^1(k)$! So we have created some "blowing up" at the origin.

To make our blow-up ring, we compute $A(Z)$. This will be a quotient of $k[x, y][u, v]$, where the x and y come from $\mathbb{A}^2(k)$, and the u and v come from $\mathbb{P}^1(k)$. Now, $((x, y), (u : v)) \in Z$ if and only if $(x, y) \in (u : v)$ if and only if there exists some t such that $(x, y) = t(u, v)$ if and only if $yu - xv = 0$.[2] So we have

$$A(Z) = \frac{(k[x, y])[u, v]}{(yu - xv)},$$

where we can verify that $yu - xv \in k[x, y][u, v]$ is indeed a homogeneous polynomial. But the above is our blow-up ring! So we verify that $A(Z) \cong \mathrm{B}_I\, R$.

- Alternatively, focus on the ring

$$\mathrm{B}_I\, R \cong \frac{k[x, y, u, w]}{(xw - yv)},$$

and think about the right-hand side as the coordinate ring over the variety 2×2 singular matrices embedded into $\mathbb{A}^4(k)$. To make our blowing up appear, we imagine taking the quotient by the action of the matrices

$$\begin{bmatrix} 1 & 0 \\ 0 & \lambda \end{bmatrix}.$$

More explicitly, our action is by

$$\begin{bmatrix} x & u \\ y & v \end{bmatrix} \begin{bmatrix} 1 & 0 \\ 0 & \lambda \end{bmatrix} = \begin{bmatrix} x & \lambda u \\ y & \lambda v \end{bmatrix},$$

which we can see a poor man's way to create $\mathbb{P}^1(\mathbb{C})$ in the second vector. Now, when $(x, y) \neq (0, 0)$, the orbit of (u, v) will make a one-dimensional line. However, at $(x, y) = (0, 0)$, we see that (u, v) can be whatever we want, so modding out by this action recovers all of $\mathbb{P}^1(\mathbb{C})$ (as $(u, v) = (0, 0)$). Visually, this will look like the blowing up we discussed in the previous point.

So we see that, geometrically, blowing up is intended to match the idea of expanding a single point with projective space. ■

4.1.8 Blow-Up Modules

We remark that there is also a notion of the blow-up module.

[2] For this last equivalence, note $(x, y) = t(u, v)$ with $(u, v) \neq 0$ is equivalent to (x, y) and (u, v) being linearly dependent is equivalent to their determinant vanishing.

Definition 4.37 (Blow-up module)**.** Fix R a ring and $I \subseteq R$ an ideal. Further, fix a module M with an I-filtration $\mathcal{J}$ denoted

$$M = M_0 \supseteq M_1 \supseteq M_2 \supseteq \cdots .$$

Then we define the *blow-up module* $\mathrm{B}_I\,\mathcal{J} M$ by

$$\mathrm{B}_I\,M := M_0 \oplus M_1 \oplus M_2 \oplus \cdots .$$

Example 4.38. Fix $M = R$ and $\mathcal{J}$ by the I-stable filtration

$$R \supseteq I \supseteq I^2 \supseteq \cdots .$$

Then $\mathrm{B}_{\mathcal{J}}\,M = \mathrm{B}_I\,R$. For example, $\mathrm{B}_{\mathcal{J}}\,M$ is finitely generated as a $\mathrm{B}_I\,R$-module, for free.

As usual, a priori we only know that $\mathrm{B}_{\mathcal{J}}\,M$ is a large R-module, but in fact it's a graded $\mathrm{B}_I\,R$-module.

Lemma 4.39. Fix R a ring and $I \subseteq R$ an ideal. Further, fix M an R-module and $\mathcal{J}$ an I-filtration denoted by

$$M = M_0 \supseteq M_1 \supseteq M_2 \supseteq \cdots .$$

We check that $\mathrm{B}_{\mathcal{J}}\,M$ is a graded $\mathrm{B}_I\,R$-module.

Proof. As usual, the main point is to define the action on the components $(\mathrm{B}_I\,R)_s = I^s$ and $(\mathrm{B}_{\mathcal{J}}\,M)_q = M_q$. Well, if we have $r \in I^s$ and $x \in M_q$, then because we have an I-filtration, we see $rx \in M_{q+s}$. In fact, this defines an R-bilinear map

$$I^s \times M_q \to M_{s+q}.$$

To see that this is R-bilinear, we pick up $r_1, r_2 \in R$ with $y_1, y_2 \in I^s$ and $s_1, s_2 \in R$ with $x_1, x_2 \in M_q$ so that

$$(r_1y_1 + r_2y_2)(s_1x_1 + s_2x_2) = r_1s_1(y_1x_1) + r_1s_2(y_1x_2) + r_2s_1(y_2x_1) + r_2s_2(y_2x_2)$$

by distributing, which is exactly our R-bilinearity check. We note that, if we can extend this map $I^s \times M_q \to M_{s+q}$ to an R-action of $\mathrm{B}_I\,R$ on $\mathrm{B}_{\mathcal{J}}\,M$, then it will automatically be graded because we will have

$$(\mathrm{B}_I\,R)_s(\mathrm{B}_{\mathcal{J}}\,M)_q = I^sM_q \subseteq M_{s+q} = (\mathrm{B}_{\mathcal{J}}\,M)_{s+q}$$

So it remains to assemble our action. By universal property, we have an R-linear map

$$I^s \otimes_R M_q \to M_{s+q} \hookrightarrow \mathrm{B}_{\mathcal{J}}\,M$$

by $r \otimes x \mapsto rx$. Now, taking the direct sum over s and q, we see we have a map

$$\mathrm{B}_I\,R \otimes_R \mathrm{B}_{\mathcal{J}}\,M = \left(\bigoplus_{s\ge 0} I^s\right) \otimes_R \left(\bigoplus_{q\ge 0} M_q\right) \simeq \bigoplus_{s,q\ge 0} (I^s \otimes_R M_q) \to \mathrm{B}_{\mathcal{J}}\,M$$

by $\left(\sum_s r_s\right) \otimes \left(\sum_q x_q\right) \mapsto \sum_{s,q} r_sx_q$. Thus, by the tensor-hom adjunction, we have an R-module homomorphism

$$\varphi : \mathrm{B}_I\,R \to \mathrm{End}_R(\mathrm{B}_{\mathcal{J}}\,M).$$

It remains to show that φ is a homomorphism of rings. Well, $1 \in \mathrm{B}_I\,R$ is $(1, 0, 0, \ldots)$ gets sent to the action taking

$$\sum_{q\ge 0} x_q \mapsto \sum_{s,q\ge 0} 1_{s=0}x_q = \sum_{q\ge 0} x_q.$$

It remains to show that φ is multiplicative. Well, we compute

$$\varphi\left(\left(\sum_{s\geq 0} r_s\right)\left(\sum_{s'\geq 0} r'_{s'}\right)\right) = \sum_{s,s'} \varphi(r_s r'_{s'})$$

by distributing. Now, we could distribute this back so long as we know that $\varphi(r_s r'_{s'}) = \varphi(r_s)\varphi(r'_{s'})$. Well, picking up some $\sum_{q\geq 0} x_q$, we compute

$$\varphi(r_s)\varphi(r'_{s'})\left(\sum_{q\geq 0} x_q\right) = \sum_{q\geq 0} r_s r'_{s'} x_q = \varphi(r_s r'_{s'})\left(\sum_{q\geq 0} x_q\right),$$

which is what we wanted. ■

Now, the reason we are introducing blow-ups right now is that blowing up turns stability of filtrations into a more comfortable ring-theoretic condition.

Proposition 4.40. Fix R a Noetherian ring and $I \subseteq R$ an ideal with M a finitely generated R-module granted an I-filtration $\mathcal{J}$ denoted by

$$M = M_0 \supseteq M_1 \supseteq M_2 \supseteq \cdots.$$

Then $\operatorname{B}_{\mathcal{J}} M$ is finitely generated as a $\operatorname{B}_I R$-module if and only if $\mathcal{J}$ is I-stable.

Proof. We show the directions independently.

- Suppose that $\operatorname{B}_{\mathcal{J}} M$ is finitely generated. By decomposing the generators into their (finitely many) homogeneous parts, we may assume that all the generators are homogeneous. Explicitly, denote our generators by $x_1, \ldots, x_n$ such that $x_i \in (\operatorname{B}_{\mathcal{J}} M)_{d_i} = M_{d_i}$ for each i.

  Without much better to do, we set $N = \max_i\{d_i\}$ to be the maximum degree of a generator. We claim that $\mathcal{J}$ stabilizes after N.

  Indeed, pick some $q+N > N$, and we need to show $M_{q+N} = I^q M_N$. Certainly $I^q M_N \subseteq M_{q+N}$ because $\mathcal{J}$ is an I-filtartion. In the other direction, pick up some $x \in M_{q+N}$ and embed it into $\operatorname{B}_{\mathcal{J}} M$. But now $\operatorname{B}_{\mathcal{J}} M$ is finitely generated by the x_i, so we may write

  $$x = \sum_{i=1}^n \left(\sum_{s\geq 0} r_{is} x_i\right)$$

  for some elements $\sum_{s\geq 0} r_{is} \in \operatorname{B}_I R$. Now, if we only pay attention to the terms of degree $q+N$, we see that we get the equality

  $$x = \sum_{i=1}^n r_{i,q+N-d_i} x_i.$$

  In particular, we note that $r_{i,q+N-d_i} x_i \in I^{q+N-d_i} M_{d_i} = I^q \cdot I^{N-d_i} M_{d_i} \subseteq I^q M_N$, so the entire sum lives in $I^q M_N$, and we are done.

- Conversely, suppose that $\mathcal{J}$ is I-stable so that $M_{q+N} = I^q M_N$ for some large N and any q. Taking a hint from the above, we choose our generators for $\operatorname{B}_{\mathcal{J}} M$ to be the (embedded) generators of $M_0, \ldots, M_N$, which will work.

  Explicitly, note that M is Noetherian because it is finitely generated over a Noetherian ring, so each of the M_i are also finitely generated. So suppose that we can generate M_i by the elements $\{x_{i1}, \ldots, x_{im_i}\}$. We claim that the (finite!) set

  $$\bigcup_{i=1}^N \{x_{i1}, \ldots, x_{im_i}\}$$

will generate $\mathrm{B}_{\mathcal{J}} M$ as a $\mathrm{B}_I R$-module.

Fixing some element $x \in \mathrm{B}_{\mathcal{J}} M$, we note that it suffices to show that the homogeneous components of x can be generated by out set, so without loss of generality, take x homogeneous with $x \in M_q$ for some q. If $q \le N$, then we simply use the generators of M_q to write

$$x = \sum_{j=1}^{m_q} r_j x_{qj}$$

for some $r_1, \ldots, r_{m_i} \in R$. The above equation lifts to a multiplication of elements $r_j \in R = (\mathrm{B}_I R)_0$ by elements $x_{qj} \in M_q = (\mathrm{B}_{\mathcal{J}} R)_q$. Notably, each product $r_j x_{qj}$ will live in $(\mathrm{B}_I R)_0 (\mathrm{B}_{\mathcal{J}} R)_q = (\mathrm{B}_{\mathcal{J}} R)_q$ by the grading.

Otherwise, $q > N$. Thus, we may write $M_q = I^{q-N} M_N$, so $x = rx'$ with $r \in I^{q-N}$ and $x' \in M_N$. Now, we know that we can generate $M_N = (\mathrm{B}_{\mathcal{J}} M)_N$ from the above argument, so write

$$x' = \sum_{j=1}^{m_N} r_j x'_{Nj}.$$

Multiplying this equation by r pushes $rr_j \in I^{q-N} = (\mathrm{B}_I R)_{q-N}$, so in total we will have components $rr_j x_{Nj} \in I^{q-N} M_N = M_q = (\mathrm{B}_{\mathcal{J}} M)_q$. So the grading here matches, and we can indeed lift this equation into $(\mathrm{B}_{\mathcal{J}} M)_q$, showing that we are able to generate $(\mathrm{B}_{\mathcal{J}} M)_q$.

The above two directions finish the proof. ■

4.1.9 The Artin–Rees Lemma

We are now ready to attack the proof of the Artin–Rees lemma. Recall the statement.

Theorem 4.31 (Artin–Rees lemma)**.** Fix R a Noetherian ring and $I \subseteq R$ an ideal with M a finitely generated R-module granted a stable I-filtration $\mathcal{J}$ denoted by

$$M = M_0 \supseteq M_1 \supseteq M_2 \supseteq \cdots .$$

Then given a submodule $M' \subseteq M$, the induced filtration by $M'_k := M_k \cap M'$ is also a stable I-filtration.

Proof. The idea is to use Proposition 4.40 to turn stability into finite generation. Namely, let $\mathcal{J}'$ be the induced filtration for M', notated by

$$M' = M' \cap M_0 \supseteq M' \cap M_1 \supseteq M' \cap M_2 \supseteq \cdots .$$

Now, because $\mathcal{J}$ is I-stable, Proposition 4.40 implies that $\mathrm{B}_{\mathcal{J}} M$ is finitely generated as a $\mathrm{B}_I R$-module.

But now Remark 4.34 tells us that $\mathrm{B}_I R$ is Noetherian! Thus, $\mathrm{B}_{\mathcal{J}} M$ being finitely generated makes $\mathrm{B}_{\mathcal{J}} M$ Noetherian. So we note the inclusions $M_i \cap M' \hookrightarrow M_i$ glue together to an inclusion

$$\mathrm{B}_{\mathcal{J}'} M' \hookrightarrow \mathrm{B}_{\mathcal{J}} M,$$

so $\mathrm{B}_{\mathcal{J}'} M'$ is a $\mathrm{B}_I R$-submodule,[3] so $\mathrm{B}_{\mathcal{J}'} M'$ is finitely generated. So Proposition 4.40 tells us that $\mathcal{J}'$ is I-stable. ■

Here is a nice application.

[3] Yes, the $\mathrm{B}_I R$-action behaves on restriction, essentially by just looking at it. In fact, the inclusion $\mathrm{B}_{\mathcal{J}'} M' \hookrightarrow \mathrm{B}_{\mathcal{J}} M$ is set-theoretic.

Theorem 4.41 (Krull intersection)**.** Fix R a Noetherian ring with an ideal I and finitely generated R-module M. Further, set

$$M' := \bigcap_{s\geq 0} I^s M.$$

Then there is some $r \in I$ such that $(1-r)M' = 0$.

Proof. The point is to recall we had a lemma to Nakayama's lemma Lemma 3.34, which we will want to use here. In particular, it will suffice to show that $IM' = M'$, which is intuitively pretty clear from the definition of M'.

The trick to rigorize our intuition is to use Theorem 4.31 on $M' \subseteq M$, where we give M the I-stable filtration

$$M \supseteq IM \supseteq I^2 M \supseteq \cdots.$$

In particular, we are told by Theorem 4.31 that the filtration

$$M' \supseteq M' \cap IM \supseteq M' \cap I^2 M \supseteq \cdots$$

will stabilize, so there exists some large N so that

$$M' \cap I^{N+1} M = I\left(M' \cap I^N M\right).$$

But of course, for any q, we have $M' \subseteq I^q M$ by definition of M', so we see that the above tells us $M' = IM'$, finishing. ■

Remark 4.42 (Nir)**.** Here is one reason to believe Theorem 4.41: certainly if we can write $(1-r)M' = 0$ for some $r \in I$, then $M' = rM'$, so $M' = rM' = r^2 M' = \cdots$ inductively. In particular, $M' \subseteq I^q M' \subseteq I^q M$ for any q.

Corollary 4.43. Fix R a Noetherian ring with a proper ideal I. If R is local or a domain, then

$$\bigcap_{s\geq 0} I^s = 0.$$

Proof. Set

$$J := \bigcap_{s \geq 0} I^s.$$

We would like to show that $J = 0$, for which we use Theorem 4.41. We show our two cases separately.

- Take R local. Back in the proof of Theorem 4.41, we showed that $IJ = J$. Now, because I is proper, I is contained in the unique maximal ideal of R, which is the Jacobson radical of R. So Theorem 3.33 tells us that $J = 0$.
- Take R a domain. Using Theorem 4.41 more directly, we are promised $r \in I$ such that $(1-r)J = 0$. Now, $1 \notin I$ because I is proper, so $(1-r) \neq 0$. However, for any $x \in J$, we have $(1-r)x = 0$, so $x = 0$ is forced because R is a domain. Thus, $J = 0$.

The above two cases finish the proof. ■

Remark 4.44. The condition that R is Noetherian is necessary. We will give an example next class.

We close with an exercise.

Exercise 4.45. Fix R a local Noetherian ring and $I \subseteq R$ a proper ideal. If $\operatorname{gr}_I R$ is a domain, then R is a domain.

Proof. The main idea is to show that $\operatorname{in} f = 0$ if and only if $f = 0$ via Corollary 4.43. Indeed, if $f = 0$, then $\operatorname{in} f = 0$ by definition because $f \in I^s$ for all s. Conversely, if $\operatorname{in} f = 0$, then $f \in I^s$ for all s, so

$$f \in \bigcap_{s \geq 0} I^s,$$

so $f = 0$ follows from Corollary 4.43.

We now finish. Suppose that $fg = 0$ in R, and we show $f = 0$ or $g = 0$. By Proposition 4.20, we see that

$$\operatorname{in} f \cdot \operatorname{in} g = \operatorname{in}(fg) = 0,$$

so $\operatorname{in} f = 0$ or $\operatorname{in} g = 0$ because $\operatorname{gr}_I R$ is an integral domain. But by our work above, we see that $\operatorname{in} f = 0$ implies $f = 0$, and $\operatorname{in} g = 0$ implies $g = 0$, so we are done. ■

4.2 March 1

Welcome back everyone. The average and median for the exam was 32/50.

4.2.1 Krull's Intersection Theorem

Last time we showed the following.

Corollary 4.43. Fix R a Noetherian ring with a proper ideal I. If R is local or a domain, then

$$\bigcap_{s \geq 0} I^s = 0.$$

The Noetherian condition is necessary here; consider the following example.

Exercise 4.46. Let R consist of the ring of germs of infinitely differentiable functions $f : \mathbb{R} \to \mathbb{R}$ at 0. Namely, two functions $f, g : \mathbb{R} \to \mathbb{R}$ are equivalent in R if and only if they coincide on an open neighborhood around 0. Then R is local with unique maximal ideal

$$\mathfrak{m} := \{f \in R : f(0) = 0\}.$$

However,

$$\bigcap_{s \geq 0} \mathfrak{m}^s$$

is nonzero.

Proof. We start with the checks on R.

- We describe how to check that R is actually a ring, but we will not do so. To begin, the set of infinitely differentiable functions $C^\infty(\mathbb{R})$ is a ring with addition and multiplicative defined pointwise; e.g., our identity is $f \equiv 1$. Then we define the ideal

  $$I = \{f : f(x) = 0 \text{ for all } x \in U \text{ for some open } U \text{ containing } 0\}.$$

  It is not hard to check that I is an ideal: if $f, g \in I$ and $r, s \in C^\infty(\mathbb{R})$ with $f|_U = 0$ and $g|_V = 0$ where $0 \in U \cap V$, then $(rf + sg)|_{U \cap V} = 0$.

Now, we simply define $R := C^\infty(\mathbb{R})/I$. In particular, $[f]_I = [g]_I$ for $f, g \in C^\infty(\mathbb{R})$ if and only if $(f-g)$ vanishes on some neighborhood U of 0, which is equivalent to f and g agreeing on some neighborhood U of 0.

- We check that R is local with the given maximal ideal $\mathfrak{m}$. For this, we show that all elements outside $\mathfrak{m}$ are units, which will be enough because it will show that any proper ideal (which only contains non-units) is contained in $\mathfrak{m}$.

  Indeed, pick up some $u \notin \mathfrak{m}$ so that $u(0) \neq 1$. Because u is continuous, $u(\mathbb{R} \setminus \{0\})$ is open and contains 0, so there exists an $\varepsilon > 0$ such that u is nonzero on the compact set $[-\varepsilon, \varepsilon]$. Then $1/u$ is an infinitely differentiable function v on $(-\varepsilon, \varepsilon)$, which we can then extend to a function in $C^\infty(\mathbb{R})$.[4] So indeed, uv agrees with the function 1 on $(-\varepsilon, \varepsilon)$, so $uv \equiv 1 \pmod{I}$.

It remains to check that

$$\bigcap_{s \geq 0} \mathfrak{m}^s \neq 0.$$

Indeed, set, for given m,

$$g_m(x) := \begin{cases} e^{-1/x^2}/x^m & x \neq 0, \\ 0 & x = 0. \end{cases}$$

An induction shows that, on $\mathbb{R} \setminus \{0\}$, we have $g_m^{(n)}(x) = p_n(1/x)e^{-1/x^2}$ some $p_n \in \mathbb{Q}[x]$, for any $n \geq 0$. Indeed, it holds for $n = 0$ by taking $p_0(x) = x^m$, and the inductive step merely needs to write

$$g_m^{(n+1)}(x) = \frac{d}{dx} g_m^{(n)}(x) = \frac{d}{dx} p_n(1/x) e^{-1/x^2} = \underbrace{\left(p_n'\left(\frac{1}{x}\right) \cdot -\frac{1}{x^2} + \frac{-2}{x^3} \right)}_{p_{n+1}(1/x)} e^{-1/x^2}.$$

Thus, we can show by induction that $g_m^{(n)}(0) = 0$ for each 0. We get $n = 0$ for free, and otherwise, we compute

$$g_m^{(n+1)}(0) = \lim_{x \to 0} \frac{g_m^{(n)}(x) - g_m^{(n)}(0)}{x} = \lim_{h \to 0} \left(\frac{p_n(1/x)}{x} \cdot e^{-1/x^2} \right) = \lim_{x \to \pm\infty} \frac{x p_n(x)}{e^{-x^2}},$$

which vanishes no matter which $\pm\infty$ we approach. So in total, we see that $g \in C^\infty(\mathbb{R})$, so it will produce a legal germ at 0.

It follows that $e^{-1/x^2}/x^m = g_m(x) \in C^\infty(\mathbb{R})$ for each m. To finish, we see that

$$e^{-1/x^2} = x^m \cdot e^{-1/x^2}/x^m \in \mathfrak{m}^m C^\infty(\mathbb{R}) \subseteq \mathfrak{m}^m$$

for any m, which is what we wanted. ■

Remark 4.47 (Nir). The finite generation is also necessary: the module $M = \mathbb{Q}$ over the integral domain $R = \mathbb{Z}$ has $I = (2) \subseteq \mathbb{Z}$ a proper ideal while $IM = (2)\mathbb{Q} = \mathbb{Q}$ so that $\bigcap_s I^s M = M$. We are essentially detecting a counterexample to Nakayama's lemma here.

4.2.2 Flat Modules

Today we are talking about flatness and Tor. Let's start with flatness; we recall the definition.

Definition 2.45 (Flat). Fix R a ring. Then an R-module M is *flat* if and only if the functor $M \otimes_R -$ is exact.

As we discussed in Remark 2.46, because $M \otimes_R -$ is already left-exact, we merely have to check that $N \hookrightarrow N'$ induces an injection $M \otimes_R N \hookrightarrow M \otimes_R N'$.

We now run through some examples of flat modules.

[4] I think some kind of uniformity condition is needed here to make sure that $1/u$ can be extended as claimed, but I won't bother making this rigorous.

Example 4.48. We showed back in Example 2.48 that R^n is a flat R-module. Essentially this is because $R^n \otimes A \simeq (R \otimes A)^n \simeq M^n$ (functorially), so injections $A \hookrightarrow B$ remain injections $A^n \hookrightarrow B^n$.

Example 4.49. For any multiplicative set $U \subseteq R$, the module $R\left[U^{-1}\right]$ is flat, as we showed in Corollary 2.53. For example, $\mathbb{Q}$ is flat as a $\mathbb{Z}$-module.

Remark 4.50. As a small aside, we note that Proposition 2.52 only says that $R\left[U^{-1}\right] \otimes - : \mathrm{Mod}_R \to \mathrm{Mod}_{R[U^{-1}]}$ takes short exact sequences in Mod_R to short exact sequences in $\mathrm{Mod}_{R[U^{-1}]}$, but this restricts to R-modules just fine (even when $R \to R\left[U^{-1}\right]$ is not injective). To be explicit, given $A \hookrightarrow B$ in Mod_R, the fact that the map

$$A \otimes_R R\left[U^{-1}\right] \to B \otimes_R R\left[U^{-1}\right]$$

is injective does not matter if we are looking in the category $\mathrm{Mod}_{R[U^{-1}]}$ or Mod_R.

And let's see a non-example.

Exercise 4.51. For any positive integer $n > 1$, the module $\mathbb{Z}/n\mathbb{Z}$ is not flat in the category of $\mathbb{Z}$-modules.

Proof. We witness this with a specific short exact sequence. For our purposes, we will take

$$0 \to \mathbb{Z} \stackrel{\times n}{\to} \mathbb{Z} \to \mathbb{Z}/n\mathbb{Z} \to 0.$$

We now claim that the induced sequence

$$0 \to \mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Z}/n\mathbb{Z} \stackrel{\times n}{\to} \mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z} \to 0$$

is not exact. In particular, we need to show that the induced map $\varphi : \mathbb{Z}\otimes_{\mathbb{Z}}\mathbb{Z}/n\mathbb{Z} \stackrel{\times n}{\to} \mathbb{Z}\otimes_{\mathbb{Z}}\mathbb{Z}/n\mathbb{Z}$ is not injective. Well, we note $\mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}/n\mathbb{Z}$ by $1 \otimes [k]_n \mapsto [k]_n$, so we note $1 \otimes [1]_n$ is a nonzero element (it goes to $[1]_n$ under the isomorphism) and that

$$\varphi(1 \otimes [1]_n) = 1 \otimes n[1]_n = 1 \otimes [0]_n$$

is 0 in $\mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Z}/n\mathbb{Z}$. ■

4.2.3 Projective Modules

For our next example of flat modules, we will want to talk about projective modules. Before doing, so we should discuss what it means for a short exact sequence to split.

Definition 4.52 (Splits)**.** Fix a short exact sequence of R-modules

$$0 \to A \to B \stackrel{\pi}{\to} C \to 0.$$

Then we say that this short exact sequence *splits* if and only if there is a "lift" $\varphi : C \to B$ such that $\pi \circ \varphi = \mathrm{id}_C$.

Here are a few equivalent conditions.

Lemma 4.53. Fix a short exact sequence of R-modules.

$$0 \to A \stackrel{\iota}{\to} B \stackrel{\pi}{\to} C \to 0.$$

Then the following are equivalent.

(a) The short exact sequence splits, in the sense of Definition 4.52.

(b) There is an isomorphism $\psi : A \oplus C \to B$ such that the following diagram commutes, where the bottom row has the canonical inclusion and projection.

$$\begin{tikzcd} 0 \arrow[r] & A \arrow[r] \arrow[d, equal] & A \oplus C \arrow[r] \arrow[d, "\psi"] & C \arrow[r] \arrow[d, equal] & 0 \\ 0 \arrow[r] & A \arrow[r, "\iota"] & B \arrow[r, "\pi"] & C \arrow[r] & 0 \end{tikzcd}$$

(c) The function $(\pi \circ -) : \operatorname{Hom}_R(C, B) \to \operatorname{Hom}_R(C, C)$ is surjective.

Proof. We start by showing (a) is equivalent to (b).

- We show that (a) implies (b). Well, we claim that the provided lift $\varphi : C \to B$ such that $\pi \circ \varphi = \operatorname{id}_C$ will create the needed isomorphism by $\psi = \iota \oplus \varphi$. Namely, we have to show that $\iota \oplus \varphi : A \oplus C \to B$ is an isomorphism. Certainly it is an R-module homomorphism, so we need to show that it is a bijection, for which we have the following checks.
  - We show that $\iota \oplus \varphi$ is injective. Well, if $(\iota \oplus \varphi)(a, c) = 0$, then we want to show $(a, c) = (0, 0)$. Well, $\iota(a) + \varphi(c) = 0$, so
  $$0 + c = \pi(\iota(a)) + \pi(\varphi(c)) = \pi(\iota(a) + \varphi(c)) = 0,$$
  so $c = 0$ follows. But then $\iota(a) = 0$, so $a = 0$ by injectivity of ι.
  - We show that $\iota \oplus \varphi$ is surjective. Well, pick up some $b \in B$. Then we set $c := \pi(b)$ so that
  $$\pi(b - \varphi(c)) = \pi(b) - \operatorname{id}_C(c) = 0.$$
  In particular, $b - \varphi(c) \in \ker \pi = \operatorname{im} \iota$ by exactness, so there exists $a \in A$ such that $b - \varphi(c) = \iota(a)$, from which $(\iota \oplus \varphi)(a, c) = b$ follows.

  It remains to show that the diagram

  $$\begin{tikzcd} 0 \arrow[r] & A \arrow[r] \arrow[d, equal] & A \oplus C \arrow[r] \arrow[d, dashed, "\iota\oplus\varphi"] & C \arrow[r] \arrow[d, equal] & 0 \\ 0 \arrow[r] & A \arrow[r, "\iota"] & B \arrow[r, "\pi"] & C \arrow[r] & 0 \end{tikzcd}$$

  commutes. To check that the left square commutes, we go along the top to get $a \mapsto (a, 0) \mapsto \iota(a)$ and go along the bottom to get $a \mapsto a \mapsto \iota(a)$, which match.

  To check that the right square commutes, we go along the top to get $(a, c) \mapsto c \mapsto c$ and go along the bottom to get $(a, c) \mapsto \iota(a) + \varphi(c) \mapsto 0 + c$, which match.

- We show that (b) implies (a). Well, we claim that the composite
  $$\varphi(c) := \psi((0, c))$$
  will work. Indeed, because the right square of the given diagram commutes, we see that
  $$\pi(\varphi(c)) = \pi(\psi((0, c))) = c,$$
  which is what we wanted.

We now show that (a) is equivalent to (c).

- We show that (a) implies (c). For this, we pick up any morphism $f : C \to C$ that we want to hit and observe $(\varphi \circ f) : C \to B$ will have

$$(\pi \circ -)(\varphi \circ f) = (\pi \circ \varphi) \circ f = \mathrm{id}_C \circ f = f,$$

  so we are done.

- We show that (c) implies (a). This is not too bad: because $(\pi \circ -)$ is surjective, it must hit $\mathrm{id}_C : C \to C$, so there is a morphism $\varphi : C \to B$ such that $\pi \circ \varphi = (\pi \circ -)(\varphi) = \mathrm{id}_C$, which is what we wanted.

The above implications finish the proof. ■

And now we get to talk about projective modules.

Definition 4.54 (Projective)**.** An R-module P is *projective* if and only if, for any surjection $\pi : B \twoheadrightarrow C$ and map $\varphi : P \to C$, there exists an induced map $\overline{\varphi} : P \to B$ making the following diagram commute.

$$\begin{tikzcd} & P \arrow[dl, dashed, "\psi"'] \arrow[d, "\varphi"] \\ B \arrow[r, two heads, "\pi"'] & C \end{tikzcd}$$

We might feel scammed that we just spent so much time discussing short exact sequences splitting, and the definition of projective does not use this. However, there are lots of equivalent definitions of projective; here are the ones we care about.

Lemma 4.55. Fix an R-module P. Then the following are equivalent.

(a) P is projective, in the sense of Definition 4.54.

(b) Any short exact sequence of R-modules

$$0 \to A \to B \to P \to 0$$

splits.

(c) There exists an R-module K such that $K \oplus P$ is a free R-module.

(d) The functor $\mathrm{Hom}_R(P, -)$ is exact.

Proof. We take our implications one at a time.

- We show that (a) implies (b). The key is to write the short exact sequence in the following diagram.

$$\begin{tikzcd} & & & P \arrow[dl, dashed, "\varphi"'] \arrow[d, equal] \\ 0 \arrow[r] & A \arrow[r] & B \arrow[r, two heads, "\pi"'] & P \arrow[r] & 0 \end{tikzcd}$$

  In particular, because P is projective, there exists a map $\varphi : P \to M$ such that $\pi \circ \varphi = \mathrm{id}_P$. This is exactly what we need for the short exact sequence to split.

- We show that (b) implies (c). The point is to create a free R-module to surject onto R and then use Lemma 4.53. We outsource this difficulty into the following lemma.

Lemma 4.56. Fix M an R-module. Then there is a free R-module which surjects onto M.

Proof. For each $m \in M$, we have a map $\varphi_m : R \to M$ by sending $\varphi_m : x \mapsto xm$, and this is an R-module homomorphism because, for $r_1, r_2, x_1, x_2 \in R$ we have

$$\varphi_m(r_1x_1 + r_2x_2) = (r_1x_1 + r_2x_2)m = r_1(x_1m) + r_2(x_2m) = r_1\varphi_m(x_1) + r_2\varphi_m(x_2).$$

Now, we can stitch these φ_m together to create a surjection

$$\varphi : \underbrace{\bigoplus_{m \in M} R}_{F} \to M,$$

and we note that φ is now surjective because, for any m_0, we have

$$\varphi\left((1_{m=m_0})_{m\in M}\right) = \sum_{m\in M} \varphi_m(1_{m=m_0}) = \varphi_{m_0}(1) = m_0.$$

Thus, we do indeed have a free module F which surjects onto M. ■

We now finish showing that (b) implies (c). We use Lemma 4.56 to conjure the map $\varphi : F \twoheadrightarrow M$ where F is a free R-mdule and then create the short exact sequence

$$0 \to \ker \varphi \to F \xrightarrow{\varphi} M \to 0.$$

Now, by definition of M, this short exact sequence splits, so by Lemma 4.53, we have an isomorphism $F \cong (\ker \varphi) \oplus M$, which is what we wanted.

- We show that (c) implies (d). The main point is that (d) is not too hard to verify for free modules, so we will start by reducing to the free case. Fix our R-modules K and F so that F is free and $F \cong K \oplus P$; name this isomorphism $\psi : F \to K \oplus P$. Now, given a short exact sequence

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

we need to show that the sequence

$$0 \to \operatorname{Hom}_R(P, A) \to \operatorname{Hom}_R(P, B) \to \operatorname{Hom}_R(P, C) \to 0$$

is exact. Well, we know that $\operatorname{Hom}_R(P, -)$ is always left-exact, so it remains to show that the map $\operatorname{Hom}_R(P, B) \to \operatorname{Hom}_R(P, C)$ is surjective. To be explicit, we name the map $B \to C$ by $\pi : B \to C$ so that we are showing

$$(\pi \circ -) : \operatorname{Hom}_R(P, B) \to \operatorname{Hom}_R(P, C)$$

is surjective.

For this, pick up a morphism $f : P \to C$ that we want to hit. We now reduce to the free case. By gluing this together with the zero morphism $0 : K \to C$, we get an induced map $f : P \oplus K \to C$, which induces a map $f\varphi : F \to C$. Now that we are mapping from a free module, we can lift to $P \to B$ with ease: suppose $F = R^\lambda$ is free indexed by $\alpha \in \lambda$, so we see that we can find elements $\{b_\alpha\}_{\alpha\in\lambda} \subseteq B$ such that

$$\pi(b_\alpha) = (f\varphi)(\alpha)$$

because π is surjective. Now, we can define a map $\overline{f} : F \to B$ by $\alpha \mapsto b_\alpha$ because F is free, which satisfies

$$\pi \circ \overline{f} = f\varphi$$

by checking $(\pi \circ \overline{f})(\alpha) = \pi(b_\alpha) = (f\varphi)(\alpha)$ on each $\alpha \in \lambda$.

To finish, $\overline{f} : F \to B$ induces a map $\overline{f}\varphi^{-1} : P \oplus K \to B$, which restricts to a map $\overline{f}\varphi^{-1}\iota : P \to K$ by $p \mapsto (p, 0) \mapsto \overline{f}(\varphi^{-1}(p, 0))$. We now check that $\overline{f}\varphi^{-1}\iota$ actually satisfies the desired property: we see

$$\pi \circ (\overline{f} \circ \varphi^{-1} \circ \iota) = f \circ \varphi \circ \varphi^{-1} \circ \iota = f \circ \mathrm{id}_{P\oplus K} \circ \iota_P = f \circ \mathrm{id}_P = f,$$

so we are done.

- We show that (d) implies (a). This is definition-chasing. Suppose that we have a surjection $\pi : B \twoheadrightarrow C$ and a map $\varphi : P \to C$ that we want to lift. Well, there is a short exact sequence

$$0 \to \ker \pi \to B \xrightarrow{\pi} C \to 0,$$

which upon applying the exact functor $\operatorname{Hom}_R(P, -)$ gives tells us that

$$(\pi \circ -) : \operatorname{Hom}_R(P, C) \to \operatorname{Hom}_R(P, B)$$

is surjective, which is (c). In particular, there is a map $\overline{\varphi} : P \to C$ such that $\pi \circ \overline{\varphi} = \varphi$, which is what we wanted. ■

Remark 4.57 (Nir). Even though being projective has many definitions, some more concrete than others, I have chosen Definition 4.54 to begin with because it will be the most useful in homological algebra, which is where we are going next.

Because I just can't resist, here is a more geometric view of projective modules, which was not covered in class.

Proposition 4.58. Fix M a finitely presented R-module. Then M is projective if and only if $M_\mathfrak{p}$ is a free $R_\mathfrak{p}$ for all primes $\mathfrak{p} \subseteq R$. In other words, M is projective if and only if M is locally free.

Proof. We take our directions separately.

- Suppose M is a finitely generated projective R-module. Thus, we have a projection $R^n \twoheadrightarrow M$, so Lemma 4.55 grants us an isomorphism $K \oplus M \cong R^n$ for some R-module K. Localizing at some prime $\mathfrak{p}$, we get

$$K_\mathfrak{p} \oplus M_\mathfrak{p} \cong R_\mathfrak{p}^n.$$

So now we see that the localized module $M_\mathfrak{p}$ is still a finitely generated projective $R_\mathfrak{p}$-module by Lemma 4.55, but now $R_\mathfrak{p}$ is local with maximal ideal $\mathfrak{p}_\mathfrak{p}$.

The main idea, now, is to extract out our dimension via Corollary 3.36: note that we have an isomorphism

$$(K_\mathfrak{p}/\mathfrak{p}_\mathfrak{p}K_\mathfrak{p}) \oplus (M_\mathfrak{p}/\mathfrak{p}_\mathfrak{p}M_\mathfrak{p}) \cong (R_\mathfrak{p}/\mathfrak{p}_\mathfrak{p}) \otimes_{R_\mathfrak{p}} (K_\mathfrak{p} \oplus M_\mathfrak{p}) \cong (R_\mathfrak{p}/\mathfrak{p}_\mathfrak{p}) \otimes_{R_\mathfrak{P}} R_\mathfrak{p}^n \cong (R_\mathfrak{p}/\mathfrak{p}_\mathfrak{p}R_\mathfrak{p})^n$$

by repeatedly using Proposition 2.96. Now, everything involved now has the $\mathfrak{p}_\mathfrak{p}$-action vanished, so the above exhibits an isomorphism of $R_\mathfrak{p}/\mathfrak{p}_\mathfrak{p}$-vector spaces. In particular,

$$\dim_{R_\mathfrak{p}/\mathfrak{p}_\mathfrak{p}}(K_\mathfrak{p}/\mathfrak{p}_\mathfrak{p}K_\mathfrak{p}) + \dim_{M_\mathfrak{p}/\mathfrak{p}_\mathfrak{p}}(M_\mathfrak{p}/\mathfrak{p}_\mathfrak{p}M_\mathfrak{p}) = n,$$

so we provide these with bases $\{\overline{k_1}, \ldots, \overline{k_a}\}$ and $\{\overline{m_1}, \ldots, \overline{m_b}\}$ with $a + b = n$. By Corollary 3.36, these bases extend to surjections $R_\mathfrak{p}^a \twoheadrightarrow K_\mathfrak{p}$ and $R_\mathfrak{p}^b \twoheadrightarrow M_\mathfrak{p}$ so that we have a big surjection

$$R_\mathfrak{p}^n = R_\mathfrak{p}^a \oplus R_\mathfrak{p}^b \twoheadrightarrow K_\mathfrak{p} \oplus M_\mathfrak{p} \cong R_\mathfrak{p}^n.$$

But now Proposition 3.25 now tells us that this is an isomorphism! In particular, the map $R_\mathfrak{p}^b \twoheadrightarrow M_\mathfrak{p}$ may have no kernel, so it is an isomorphism, and we conclude that $M_\mathfrak{p}$ is free.

- Suppose M is a finitely presented R-module such that $M_\mathfrak{p}$ is a free $R_\mathfrak{p}$-module for each prime $\mathfrak{p} \subseteq R$. The key is to use Remark 2.87. Indeed, suppose that we have any short exact sequence

$$0 \to A \to B \to M \to 0,$$

and by Lemma 4.55, it suffices to show that this short exact sequence splits. Well, by Remark 2.87, this short exact sequence splits if and only if

$$0 \to A_\mathfrak{p} \to B_\mathfrak{p} \to M_\mathfrak{p} \to 0$$

splits for all prime ideals $\mathfrak{p}$. But now $M_\mathfrak{p}$ is free and in particular projective (e.g., use (c) of Lemma 4.55), so the short exact sequence splits by (b) of Lemma 4.55. So we are done. ■

Anyways, here is, roughly, why we introduced projective modules now.

Proposition 4.59. Projective modules are flat.

Proof. The main point is to use (c) of Lemma 4.55 to reduce to the free case, which we already know. Indeed, fix P a projective R-module. By (c) of Lemma 4.55, we are promised an R-module K such that $K \oplus P$ is free.

Now, by Remark 2.46, it suffices to pick up an inclusion $\iota : A \hookrightarrow B$ and show that the induced maps $\iota_P : A \otimes_R P \to B \otimes_R P$ is also injective. As promised, we will reduce to the free case. Indeed, we see that, for an R-module M, we have

$$\psi_M : M \otimes_R (K \oplus P) \simeq (M \otimes_R K) \oplus (M \otimes_R P)$$

by $\psi_M : m \otimes (k,p) \mapsto (m \otimes k, m \otimes p)$. In particular, we pick up the induced map $\iota_K : A \otimes_R K \to B \otimes_R K$ and $\iota_F : A \otimes_R (K \oplus P) \to B \otimes_R (K \oplus P)$ and note that the following diagram commutes.

$$\begin{tikzcd} A \otimes_R (K \oplus P) \arrow[r, "\psi_A"] \arrow[d, "\iota_F"] & (A \otimes_R K) \oplus (A \otimes_R P) \arrow[d, "\iota_K \oplus \iota_P"] \\ B \otimes_R (K \oplus P) \arrow[r, "\psi_B"'] & (B \otimes_R K) \oplus (B \otimes_R P) \end{tikzcd} \qquad (*)$$

Tracking our generating elements, along the top we have $a \otimes (k,p) \mapsto (a \otimes k, a \otimes p) \mapsto (\iota a \otimes k, \iota a \otimes p)$, and along the bottom we have $a \otimes (k,p) \mapsto \iota a \otimes (k,p) \mapsto (\iota a \otimes k, \iota a \otimes p)$, which matches.

To finish, suppose that we have an element $x \in A \otimes_R P$ in the kernel of ι_P. Then $(0,x) \in \ker \iota_K \oplus \iota_P$, so because the diagram in $(*)$ commutes, we see that

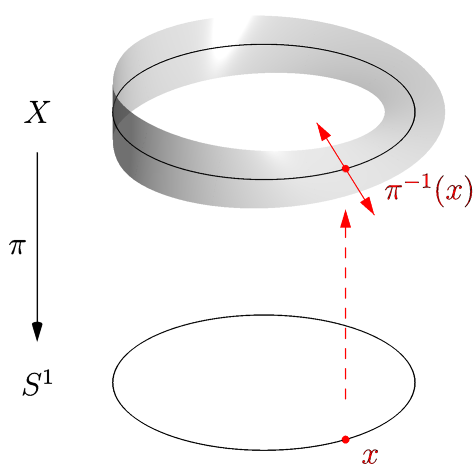
$$\iota_F\left(\psi_A^{-1}(0,x)\right) = \psi_B^{-1}\big((\iota_K \oplus \iota_P)(0,x)\big) = 0.$$

But now F is surely projective by Example 2.48, so ι_F is injective, so $\psi_A^{-1}(0,x) = 0$, so $(0,x) = 0$, so $x = 0$. Thus, ι_P does indeed have trivial kernel. ■

4.2.4 Flatness for Geometers

In algebraic geometry, we are interested in families of affine varieties, which consists of a base B and a morphism $\varphi : X \to B$; in particular, we get an affine variety "parameterized" by the elements of our B by taking the fiber $\varphi^{-1}(b)$ for each $b \in B$.

For example, here is the standard image of a Möbius strip X as a family of affine lines over S^1.



In particular, the "data" of this family really just consists of the morphism $\pi : X \to S^1$.

As usual, the algebraic story will reverse, so a family in the algebraic world should consist of the data

$$(- \circ \varphi) : A(B) \to A(X).$$

In particular, such a map $A(B) \to A(X)$ is exactly the data of $A(X)$ being an $A(B)$-algebra. To make our notions more general, we set $S := A(X)$ an $R := A(B)$-algebra by $\varphi : R \to S$.

Keeping track of our geometry, we would like to talk about how to move fibers into our algebraic world. We start by fixing a point $p \in B$, whose coordinate ring is $R/\mathfrak{m}$, where $\mathfrak{m}$ is some maximal ideal. Moving up to S, we note that if we want a function $f : X \to k$ to vanish on $\varphi^{-1}(p)$, then "morally" it should look like it factors through φ and take the form $f\varphi$ for some $f \in \mathfrak{m}$. In other words, we should modulo out by the ideal generated by

$$(- \circ \varphi)(\mathfrak{m}),$$

which is $\mathfrak{m}S$, so the coordinate ring of $\varphi^{-1}(p)$ will be

$$S/\mathfrak{m}S.$$

To generalize this past maximal ideals, we write[5] $S/\mathfrak{m}S \simeq (R/\mathfrak{m}) \otimes_R S$, so for more general primes $\mathfrak{p} \subseteq R$, our coordinate ring of the fiber over $\mathfrak{p}$ will be

$$(R/\mathfrak{p}) \otimes_R S.$$

In a family, we would like the fibers to be well-behaved. One way to keep track of well-behaved families of "algebras" (which, as above, consists of the data of a single ring homomorphism $R \to S$) is via the flatness condition.

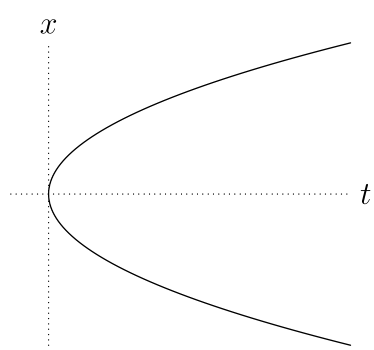
Definition 4.60 (Flat)**.** An R-algebra S is *flat* if and only if S is flat as an R-module.

On the geometric side, flatness (roughly speaking) means that the fiber $(R/\mathfrak{p}) \otimes_R S$ varies continuously as the point $\mathfrak{p}$ moves.

Let's see some examples. We will take our base to be $B := \mathbb{A}^1(k)$ the affine line over a characteristic-0 algebraically closed field k, which gives that $R := k[t]$.

Exercise 4.61. We consider the flatness of $S := R[x]/\left(x^2 - t\right)$ geometrically and algebraically.

Proof. Our family looks like the following.



Now, for a given $a \in k$, the coordinate ring of our fiber over a will be

$$\frac{S}{(t-a)S} = \frac{k[x,t]/\left(x^2-t\right)}{(t-a)k[x,t]/\left(x^2-t\right)} \cong \frac{k[x,t]}{(x^2-t, t-a)} \cong \frac{k[x]}{(x^2-a)},$$

where we have applied evaluation at $t = a$ in the last isomorphism.

We are now ready to compute the fiber. We have two cases.

- Take $a = 0$. Then we get $k[x]/\left(x^2\right)$, which is a two-dimensional k-algebra generated by $\{1, x\}$. For example, we can use Proposition 3.44 for this.

[5] For example, we are using Proposition 2.96 to get an isomorphism of R-modules, but the multiplication also matches: we have $\psi : [s]_{\mathfrak{m}S} \mapsto [1]_{\mathfrak{m}} \otimes s$, so $\psi([s] \cdot [t]) = \psi([st]) = [1] \otimes st = ([1] \otimes s)([1] \otimes t) = \psi([s])\psi([t])$.

- Take $a \neq 0$. Then we get $x^2 - a$ has a root β with $\beta \neq 0$, so $\beta \neq -\beta$ are distinct roots of $x^2 - a$. So the polynomials $(x-\beta)$ and $(x+\beta)$ are coprime (any common divisor would have to divide $(x+\beta)-(x-\beta) = 2\beta \in k^\times$), so the Chinese remainder theorem implies

$$\frac{k[x]}{(x^2-a)} \cong \frac{k[x]}{(x-\beta)} \oplus \frac{k[x]}{(x+\beta)}.$$

  Now, each term on the right-hand side is isomorphic to k by the evaluation morphism $k[x]/(x-\gamma) \to k$ by $x \mapsto \gamma$. So our fiber is isomorphic to k^2. Geometrically, the coordinate ring of a point is simply k, so our fiber looks like two points, as we expect.

Even though the fiber has a bit of hiccup at $a = 0$, its dimension is still uniform (namely, the coordinate ring is generated by two elements), so our fibers appear "continuous."

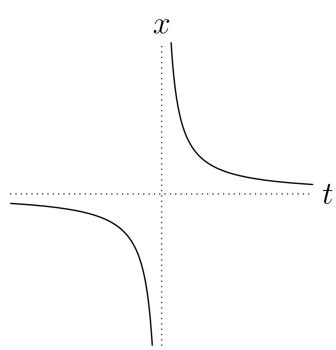
So we have geometric reason to expect S to be flat. Algebraically, we note from Proposition 3.44 that

$$S = \frac{R[t]}{(x^2-t)}$$

is a free R-module and therefore flat by Example 2.48. ■

Exercise 4.62. We consider the flatness of $S := R[x]/(xt-1)$ geometrically and algebraically.

Proof. Our family looks like the following.



We now split our computation of the coordinate ring of the fiber over some fixed $a \in k$ into two cases.

- If $a = 0$, then we are computing $S/(t)S$, but we notice that $t \in S$ is a unit because $xt = 1$ in S, so $S/(t)S$ is simply 0. This corresponds to the fact that we have an empty variety as the fiber over 0.

- If $a \neq 0$, then we directly compute

$$\frac{S}{(t-a)S} = \frac{k[x,t]/(xt-1)}{(t-a)k[x,t]/(xt-1)} \cong \frac{k[x,t]}{(xt-1,t-a)} \cong \frac{k[x]}{(ax-1)},$$

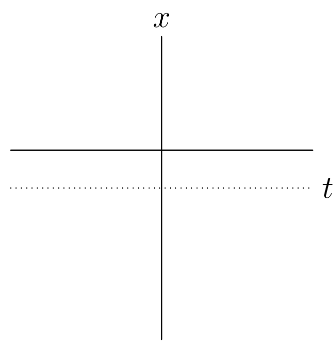
  where we have applied evaluation at $t = a$ in the last isomorphism. Now, the point is that $(ax-1) = (x-1/a)$ because $a \in k^\times$, so $S/(t-a)S \cong k$ by applying the isomorphism $k[x]/(x-1/a) \to k$ by $x \mapsto 1/a$.

  In particular, the coordinate ring being k corresponds to the fact that we have a single point in our fiber.

From the above casework, we see that our fibers vary continuously except for a "singularity" at $a = 0$, which is still legal, so we have some reason to believe that S is flat. And indeed, $S = R[x]/(xt-1) \cong R\left[t^{-1}\right]$ as we showed on the homework, so S is a localization of R, so S is flat as an R-module. ■

Exercise 4.63. We consider the non-flatness of $S := R[x]/(tx - t)$ geometrically and algebraically.

Proof. Our family looks like the following.



We now compute the coordinate ring of the fiber over a fixed point $a \in k$. Generally speaking, we find that

$$\frac{S}{(t-a)S} = \frac{k[x,t]/(tx-t)}{(t-a)k[x,t]/(tx-t)} \cong \frac{k[x,t]}{(tx-t,t-a)} \cong \frac{k[x]}{(ax-a)}.$$

To finish, we do casework on a.

- Take $a = 0$ so that we have
$$\frac{S}{(t)S} \cong \frac{k[x]}{(0)} = k[x].$$
In particular, our coordinate ring being $k[x]$ corresponds to this fiber being a full line.
- Take $a \neq 0$. Then we have
$$\frac{S}{(t-a)S} \cong \frac{k[x]}{(ax-a)}.$$
But now, $(ax - a) = (a)(x-1) = (x-1)$ because $a \in k^\times$. So, applying evaluation at $x = 1$, we see that $S/(t-a)S \cong k$, which corresponds to our coordinate ring consisting of a single point.

Now, the above situation feels and looks significantly less continuous: we added a full line of dimension at $a = 0$.

And indeed, we can verify that S is not flat as an R-module. We have the following result.

Lemma 4.64. Fix R a ring $a \in R$ a non-zero-divisor. Further, if M is a flat R-module, then $am = 0$ implies $m = 0$ for $m \in M$.

Proof. The key is to use the flatness condition on the short exact sequence

$$0 \to R \stackrel{\times a}{\to} R \to R/(a) \to 0.$$

We quickly check that $R \stackrel{\times a}{\to} R$ is indeed injective because it has trivial kernel: if $ar = 0$, then $r = 0$ by construction of a.

So now, upon tensoring with M, we get an embedding

$$\iota : R \otimes_R M \stackrel{\times a}{\hookrightarrow} R \otimes_R M$$

induced by $R \stackrel{\times a}{\hookrightarrow} R$. In particular, using the isomorphism $R \otimes_R M \cong M$ by $r \otimes m \mapsto rm$, we see that $am = 0$ implies that $a \otimes m = 0$ implies that

$$\iota(1 \otimes m) = a \otimes m = 0.$$

Thus, $1 \otimes m \in \ker \iota$, so $1 \otimes m = 0$ is forced, so by pushing through $R \otimes_R M \cong M$ again, we see that $m = 1m = 0$. This is what we wanted. ■

Now, using the above lemma, we note that $t(x-1) = tx - t = 0$ in S while $t \in k[t] = R$ is not a zero-divisor and $x - 1 \neq 0$, so S is not flat. Technically, some argument is required to verify that $x - 1 \neq 0$, but we can see this because $S/(t)S \cong k[x]$ computed above takes $x \mapsto x$, so x is transcendental over k, so $x \neq 1$. ■

4.2.5 Complexes and Homology

We will want to talk about Tor in our discussion of flatness, so we will introduce the necessary homological algebra.

In homological algebra, there are dual discussions of homology and cohomology, but we will choose to focus on homology because that is where Tor arises from, though we will make occasionally comments about how the cohomological story works.

Quote 4.65. The difference between homology and cohomology is that homology indexes like H_i, and cohomology indexes like H^i.

The purpose of homological algebra is to create derived functors, which we will talk about tomorrow. Derived functors, roughly speaking, are a useful way to start with a short exact sequence and get out a long exact sequence. However, we will want to be able to talk about long sequences which are a little less than exact, so we have the following definition.

Definition 4.66 (Chain complex)**.** Fix a ring R with the trivial grading. An R-*complex* (C, ∂) is a $\mathbb{Z}$-graded module $C := \oplus_{i\in\mathbb{Z}} C_i$ (i.e., $RC_i \subseteq C_i$) that is equipped with a (graded) morphism $\partial \in \operatorname{End}_R(C)$ such that $\partial^2 = 0$.

- If $\deg \partial = -1$ (i.e., $\partial|_{C_i} : C_i \to C_{i-1}$), we will call this an R-chain complex.
- If $\deg \partial = +1$ (i.e., $\partial|_{C_i} : C_i \to C_{i+1}$), we will call this an R-cochain complex.

As much as possible, we will omit the ambient ring R and say "(co)chain complex."

One often views a chain complex C as some large chain which looks like

$$\cdots \overset{\partial}{\to} C_2 \overset{\partial}{\to} C_1 \overset{\partial}{\to} C_0 \overset{\partial}{\to} C_{-1} \overset{\partial}{\to} \cdots.$$

For bookkeeping reasons, we might define $\partial_i := \partial|_{C_i} : C_i \to C_{i-1}$ to be more specific about our domain. Dually, a cochain complex can be viewed as a large chain

$$\cdots \overset{\partial}{\to} C_{-1} \overset{\partial}{\to} C^0 \overset{\partial}{\to} C^1 \overset{\partial}{\to} C^2 \overset{\partial}{\to} \cdots.$$

Again, we can index our arrows as $\partial^i := \partial|_{C^i} : C^i \to C^{i-1}$.

Remark 4.67 (Nir)**.** Given a cochain complex $(D^\bullet, \partial^\bullet)$, we can set $C_i := D^{-i}$ to make a chain complex. Formally, $\partial^i : D^i \to D^{i+1}$ becomes $\partial_{-i} : C_{-i} \to C_{-i-1}$, giving our chain complex. Pictorially, we are applying the following process.

$$\begin{tikzcd}
\cdots \arrow[r, "\partial^{-2}"] & D^{-1} \arrow[r, "\partial^{-1}"] \arrow[d, equal] & D^0 \arrow[r, "\partial^0"] \arrow[d, equal] & D^1 \arrow[r, "\partial^1"] \arrow[d, equal] & \cdots \\
\cdots \arrow[r, "\partial^2"'] & C_1 \arrow[r, "\partial^1"'] & C_0 \arrow[r, "\partial^0"'] & C_{-1} \arrow[r, "\partial^{-1}"'] & \cdots
\end{tikzcd}$$

Warning 4.68. In light of Remark 4.67, we will stop talking about cochain complexes, except to say that they have analogous definitions and results by adding in the prefix co- everywhere and flipping the arrows as described in Remark 4.67.

With our chain complexes in place, we can define homology.

Definition 4.69 (Homology). Given a chain complex (C, ∂), we define the *homology module* as

$$H_i(C) \coloneqq \ker \partial_i / \operatorname{im} \partial_{i+1}.$$

Remark 4.70. We quickly check that these modules are well-defined. For a chain complex (C, ∂), we see that $\partial^2 = 0$ implies that $\partial_i \partial_{i+1} : C_{i+1} \to C_{i-1}$ is the zero morphism, so

$$\operatorname{im} \partial_{i+1} \subseteq \ker \partial_i,$$

making our quotient well-defined.

Remark 4.71 (Nir). To remember this notation, note that we always want $\ker \partial_i \subseteq C_i$, so $H_i(C)$ is represented by elements of C_i.

4.2.6 Chain Morphisms

We have just defined an algebraic object (the chain complex), so because this is algebra, we will want to define their morphisms.

Definition 4.72 (Chain morphism). Given chain complexes (A, ∂^A) and (B, ∂^B), we define a *chain morphism* φ as a degree-0 morphism $\varphi : A \to B$ such that $\partial^B \circ \varphi = \varphi \circ \partial^A$.

As usual, we can look at chain morphisms $\varphi : (A, \partial^A) \to (B, \partial^B)$ on the level of component modules as well: for each index $i \in \mathbb{Z}$, we can restrict φ to a morphism $\varphi_i : A_i \to B_i$ such that the following diagram commutes.

$$\begin{tikzcd} A_i \arrow[r, "\partial_i^A"] \arrow[d, "\varphi_i"'] & A_{i-1} \arrow[d, "\varphi_{i-1}"] \\ B_i \arrow[r, "\partial_i^B"'] & B_{i-1} \end{tikzcd}$$

Before continuing, we check that composition of chain morphisms gives another chain morphism.

Lemma 4.73. Fix chain morphisms $\varphi : (A, \partial^A) \to (B, \partial^B)$ and $\psi : (B, \partial^B) \to (C, \partial^C)$. Then $\psi \circ \varphi : (A, \partial^A) \to (C, \partial^C)$ is a chain morphism.

Proof. Because φ and ψ are both degree-0 graded morphisms, we see $\psi \circ \varphi$ is a degree-0 graded morphism; explicitly, for any index i, we have $\varphi(A_i) \subseteq B_i$ and $\psi(B_i) \subseteq C_i$ gives $(\psi \circ \varphi)(A_i) \subseteq C_i$.

Additionally, we note that

$$(\psi \circ \varphi) \circ \partial^A = \psi \circ \varphi \circ \partial^A = \psi \circ \partial^B \circ \varphi = \partial^C \circ \psi \circ \varphi = \partial^C \circ (\psi \circ \varphi),$$

so we see that $\psi \circ \varphi : (A, \partial^A) \to (C, \partial^C)$ is indeed a chain morphism. ■

Also, R-linear combination of chain morphisms gives another chain morphism.

Lemma 4.74. Fix elements $r, s \in R$ and chain morphisms $\varphi, \psi : (A, \partial^A) \to (B, \partial^B)$. Then $r\varphi + s\psi$ is also a chain morphism.

Proof. For any index i, we do indeed have $\varphi(A_i), \psi(A_i) \subseteq B_i$, so

$$(r\varphi + s\psi)(A_i) = r \cdot \varphi(A_i) + s \cdot \psi(A_i) \subseteq rB_i + sB_i \subseteq B_i.$$

Additionally, for any $a \in A$, we can check that

$$\left((r\varphi + s\psi) \circ \partial^A\right)(a) = r\left(\varphi\partial^A\right)(A) + s\left(\psi\partial^A\right)(a) = r\left(\partial^B\varphi\right)(a) + s\left(\partial^B\psi\right)(a) = \left(\partial^B \circ (r\varphi + s\psi)\right)(a),$$

finishing. ■

Now, the commutativity condition $\partial^B\varphi = \varphi\partial^A$ is essentially in place to ensure that chain morphisms give rise to natural morphisms of homology modules.

Lemma 4.75. Fix a chain morphism $\varphi : \left(A, \partial^A\right) \to \left(B, \partial^B\right)$ and an index $i \in \mathbb{Z}$. Then there is a map

$$H_i(\varphi) : H_i(A) \to H_i(B)$$

induced as $H_i(\varphi) : [a]_{\operatorname{im}\partial^A_{i+1}} \mapsto [\varphi_i a]_{\operatorname{im}\partial^B_{i+1}}$. In fact, φ_i induces maps $\ker\partial^A_i \to \ker\partial^B_i$ and $\operatorname{im}\partial^A_{i+1} \to \operatorname{im}\partial^B_{i+1}$ by restriction.

Proof. By construction of the chain morphism, the following diagram commutes.

$$\begin{tikzcd}
A_{i+1} \arrow[r, "\partial^A_{i+1}"] \arrow[d, "\varphi_{i+1}"'] & A_i \arrow[r, "\partial^A_i"] \arrow[d, "\varphi_i"] & A_{i-1} \arrow[d, "\varphi_{i-1}"] \\
B_{i+1} \arrow[r, "\partial^B_{i+1}"'] & B_i \arrow[r, "\partial^B_i"'] & B_{i-1}
\end{tikzcd}$$

Now, for each element $a \in \ker\partial^A_i$, we see that $\partial^B_i(\varphi_a) = \varphi_i\left(\partial^A_i a\right) = \varphi(0) = 0$, so φ_i restricts to a map

$$\varphi_i : \ker\partial^A_i \to \ker\partial^B_i.$$

Continuing, if we pick up some $\partial^A_{i+1}a \in \operatorname{im}\partial^A_{i+1} \subseteq \ker\partial^A_i$ (see Remark 4.70), then $\varphi_i\left(\partial^A_{i+1}a\right) = \partial^B_{i+1}(\varphi_i a)$, so φ_i again restricts to a map

$$\varphi_i : \operatorname{im}\partial^A_{i+1} \to \operatorname{im}\partial^B_{i+1}.$$

Thus, we have shown the last sentence of the claim. Continuing, φ_i induces a map $\ker\partial^A_i \to \ker\partial^B_i \twoheadrightarrow \ker\partial^B_i / \operatorname{im}\partial^B_{i+1}$, from which we can induce our desired map

$$H_i(\varphi) : H_i(A) \to H_i(B)$$

by sending $[a] \mapsto [\varphi_i a]$, as needed. ■

In fact, so far we have discussed how homology produces an R-module from a chain, and we have also discussed how to get a morphism of homology from a morphism of chains. Thus, we have all the data for a functor from chains to R-modules by homology, and we only have to run the following checks.

Lemma 4.76. Fix an index $i \in \mathbb{Z}$. The mapping H_i taking chains (C, ∂) to $H_i(C)$ and morphisms $\varphi : \left(A, \partial^A\right) \to \left(B, \partial^B\right)$ to $H_i(\varphi)$ is in fact a functor. Namely, we have the following.

- Identity: $H_i(\mathrm{id}_C) = \mathrm{id}_{H_i(C)}$ for any chain complex (C, ∂).
- Composition: $H_i(\psi \circ \varphi) = H_i(\psi) \circ H_i(\varphi)$ for any morphisms $\varphi : \left(A, \partial^A\right) \to \left(B, \partial^B\right)$ and $\psi : \left(B, \partial^B\right) \to \left(C, \partial^C\right)$.

Proof. We take our checks one at a time.

- Fix a chain complex (C,∂). Here, $\mathrm{id}_C : (C,\partial) \to (C,\partial)$ is given by $\mathrm{id}_C : C \to C$, which is a chain morphism $\partial\,\mathrm{id}_C = \partial = \mathrm{id}_C\,\partial$. Then, by definition in Lemma 4.75, we see that

$$H_i(\mathrm{id}_C)\left([c]_{\mathrm{im}\,\partial_{i+1}}\right) \coloneqq [\mathrm{id}_C\, c]_{\mathrm{im}\,\partial_{i+1}} = [c]_{\mathrm{im}\,\partial_{i+1}},$$

so $H_i(\mathrm{id}_C) = \mathrm{id}_{H_i(C)}$.

- Fix chain morphisms $\varphi : (A,\partial^A) \to (B,\partial^B)$ and $\psi : (B,\partial^B) \to (C,\partial^C)$. Then we see that $\psi\circ\varphi : (A,\partial^A) \to (C,\partial^C)$ is a chain morphism by Lemma 4.73. Now, using the definition in Lemma 4.75, we see

$$H_i(\psi\circ\varphi)\big([a]_{\mathrm{im}\,\partial^A_{i+1}}\big) = [\psi_i\varphi_i a]_{\mathrm{im}\,\partial^A_{i+1}} = H_i(\psi)\big([\varphi_i a]_{\mathrm{im}\,\partial^A_{i+1}}\big) = H_i(\psi)H_i(\varphi)\big([a]_{\mathrm{im}\,\partial^A_{i+1}}\big),$$

so we do indeed have $H_i(\psi\circ\varphi) = H_i(\psi)\circ H_i(\varphi)$. ■

In fact, H_i is an amazing functor: it also preserves the structure of our Hom sets.

Lemma 4.77. Fix an index $i \in \mathbb{Z}$. Then, elements of our ambient ring $r,s \in R$ and chain morphisms $\varphi,\psi : (A,\partial^A) \to (B,\partial^B)$, we have

$$H_i(r\varphi + s\psi) = rH_i(\varphi) + sH_i(\psi).$$

Proof. Note that $r\varphi + s\psi : (A,\partial^A) \to (B,\partial^B)$ is indeed a chain morphism by Lemma 4.74. Now, we pick up some $[a]_{\mathrm{im}\,\partial^A_{i+1}} \in H_i(A)$ and check via Lemma 4.75 that

$$\begin{aligned} H_i(r\varphi+s\psi)\big([a]_{\mathrm{im}\,\partial^A_{i+1}}\big) &= [r\varphi_i a + s\psi_i a]_{\mathrm{im}\,\partial^A_{i+1}} \\ &= r[\varphi_i a]_{\mathrm{im}\,\partial^A_{i+1}} + s[\psi_i a]_{\mathrm{im}\,\partial^A_{i+1}} \\ &= rH_i(\varphi)\big([a]_{\mathrm{im}\,\partial^A_{i+1}}\big) + rH_i(\psi)\big([a]_{\mathrm{im}\,\partial^A_{i+1}}\big) \\ &= \big(rH_i(\varphi) + sH_i(\psi)\big)\big([a]_{\mathrm{im}\,\partial^A_{i+1}}\big), \end{aligned}$$

so $H_i(r\varphi+s\psi) = rH_i(\varphi) + sH_i(\psi)$ follows. ■

4.2.7 Chain Homotopy

We defined our chain morphisms to give rise to maps of homology modules. Now, sometimes different chain morphisms will give rise to the same map of homology modules, so we will want a way to keep track of this back in the world of chain morphisms. This gives the following definition.

Definition 4.78 (Chain homotopy)**.** Two chain morphisms $\varphi,\psi : (A,\partial^A) \to (B,\partial^B)$ are *homotopically equivalent* if and only if there exists an R-module homomorphism $h : A \to B$ of degree 1 (i.e., $h|_{A_i} : A_i \to B_{i+1}$) such that $\varphi - \psi = h\partial_A + \partial_B h$. In this case, we will write $\varphi \sim \psi$ and call h a *chain homotopy*.

On the level of component modules, the image is as follows. As a warning, this diagram does not commute.

$$\begin{tikzcd} \cdots \arrow[r] & A_2 \arrow[r] \arrow[d] & A_1 \arrow[r] \arrow[d] \arrow[dl, dashed, "h_1"'] & A_0 \arrow[r] \arrow[d] \arrow[dl, dashed, "h_0"'] & \cdots \\ \cdots \arrow[r] & B_2 \arrow[r] & B_1 \arrow[r] & B_0 \arrow[r] & \cdots \end{tikzcd}$$

In particular, we can break up $h : A \to B$ into individual morphisms $h_i : A_i \to B_{i+1}$ such that $\varphi_i - \psi_i = h_{i-1}\partial^A_i + \partial^B_{i+1}h_i$.

Before continuing, we run some checks on homotopy equivalence.

Lemma 4.79. Homotopy equivalence of morphisms $\varphi : (A, \partial^A) \to (B, \partial^B)$ is an equivalence relation.

Proof. We have the following checks. All of our chain morphisms will be $(A, \partial^A) \to (B, \partial^B)$, so we will omit this information in our discussion.

- Reflexive: fix a chain morphism φ, and we show $\varphi \sim \varphi$. Well, take $h = 0$, which is indeed a degree-1 map ($h(A_i) = \{0\} \subseteq B_{i+1}$), and
$$\varphi - \varphi = 0 = 0 \cdot \partial_A + \partial_B \cdot 0.$$
- Symmetric: fix homotopically equivalent chain morphisms $\varphi \sim \psi$ so that we are given a degree-1 map $h : A \to B$ such that $\varphi - \psi = h\partial_A + \partial_B A$. We want to show $\psi \sim \varphi$, for which we take $-h : A \to B$. Note $-h$ is a degree-1 map because $(-h)(A_i) = -h(A_i) \subseteq -B_{i+1} = B_{i+1}$ for any index i. Further, we see
$$\psi - \varphi = -(\varphi - \psi) = -(h\partial_A + \partial_B h) = (-h)\partial_A + \partial_B(-h)$$
after rearranging, so we are done.
- Transitive: fix chain morphisms α, β, γ so that $\alpha \sim \beta$ and $\beta \sim \gamma$. So we are promised a chain homotopies a and b so that
$$\alpha - \beta = a\partial_A + \partial_B a \qquad \text{and} \qquad \beta - \gamma = b\partial_A + \partial_B b,$$
from which we find
$$\alpha - \gamma = (a + b)\partial_A + \partial_B(a + b)$$
by adding. To finish, we check that $a + b$ is a degree-1 morphism, for which we note $(a + b)(A_i) = a(A_i) + b(A_i) \subseteq B_i + B_i = B_i$ for any index i. ■

Lemma 4.80. Fix elements $r, s \in R$ and chain morphisms $\varphi, \varphi', \psi, \psi' : (A, \partial^A) \to (B, \partial^B)$. If $\varphi \sim \varphi'$ and $\psi \sim \psi'$, then
$$r\varphi + s\psi \sim r\varphi' + s\psi'.$$

Proof. We are promised chain homotopies a and b witnessing $\varphi \sim \varphi'$ and $\psi \sim \psi'$, respectively. Now, we compute that
$$\begin{aligned}(r\varphi + s\psi) - (r\varphi' + s\psi') &= r(\varphi - \varphi') + s(\psi - \psi') \\ &= r\left(a\partial^A + \partial^B a\right) + s\left(b\partial^A + \partial^B b\right) \\ &= (ra + sb)\partial^A + \partial^B(ra + sb).\end{aligned}$$
So we will have that $ra + sb$ witnesses $r\varphi + s\psi \sim r\varphi' + s\psi'$ as soon as we know that $ra + sb$ is degree-1, for which we note $(ra + sb)(A_i) = ra(A_i) + sb(A_i) \subseteq rB_{i+1} + sB_{i+1} \subseteq B_{i+1}$ for any index i. ■

With those annoying checks out of the way, we show the main point of introducing chain homotopy.

Proposition 4.81. Fix homotopically equivalent chain morphisms $\varphi, \psi : (A, \partial^A) \to (B, \partial^B)$. Then, for any index i, we have $H_i(\varphi) = H_i(\psi)$.

Proof. Fix $\gamma := \varphi - \psi$, for which we note $\varphi \sim \psi$ implies $\gamma = (\varphi - \psi) \sim (\psi - \psi) = 0$ by Lemma 4.80. We claim that $H_i(\gamma) = 0$, which will be enough because it will show by Lemma 4.77 that
$$H_i(\varphi) - H_i(\psi) = H_i(\varphi - \psi) = H_i(\gamma) = 0,$$
thus finishing.

So it remains to show $\gamma \sim 0$ implies $H(\gamma) = 0$. To start, we are promised a chain homotopy h such that

$$\gamma = \gamma - 0 = h\partial^A - \partial^B h.$$

Now, pick up any element $[a]_{\operatorname{im}\partial_{i+1}^A} \in H_i(A)$ so that we want to show $\gamma\left([a]_{\operatorname{im}\partial_{i+1}^A}\right) = 0 \in H_i(B)$. Well, we compute

$$H_i(\gamma)\left([a]_{\operatorname{im}\partial_{i+1}^A}\right) = [\gamma a]_{\operatorname{im}\partial_{i+1}^B},$$

from which we note $a \in \ker \partial_i^A$ implies

$$\gamma(a) = \left(h_{i-1}\partial_i^A + \partial_{i+1}^B h_i\right)(a) = h_{i-1}(0) + \partial_{i+1}^B(h_i a) \in \operatorname{im}\partial_{i+1}^B,$$

so we do indeed have $H_i(\gamma)\left([a]_{\operatorname{im}\partial_{i+1}^A}\right) = [0]_{\operatorname{im}\partial_{i+1}^B}$, finishing. ■

4.2.8 The Long Exact Sequence

To close out class, we discuss the long exact sequence. The statement is as follows.

Theorem 4.82. Fix

$$0 \to A \stackrel{\varphi}{\to} B \stackrel{\psi}{\to} C \to 0$$

a short exact sequence of chain complexes. Then there is a long exact sequence of homology

$$\cdots \to H_i(A) \stackrel{H_i(\varphi)}{\to} H_i(B) \stackrel{H_i(\psi)}{\to} H_i(C) \stackrel{\delta_i}{\to} H_{i-1}(A) \to \cdots,$$

for some connecting morphisms δ_i.

This is a particularly slick application of the Snake lemma, which is as follows.

Lemma 4.83 (Snake). Fix a "snake" (commutative) diagram as follows.

$$\begin{tikzcd} & A \arrow[r, "f"] \arrow[d, "a"] & B \arrow[r, "g"] \arrow[d, "b"] & C \arrow[r] \arrow[d, "c"] & 0 \\ 0 \arrow[r] & A' \arrow[r, "f'"] & B' \arrow[r, "g'"] & C' & \end{tikzcd}$$

The following are true.

(a) There is an exact sequence

$$\ker a \stackrel{f}{\to} \ker b \stackrel{g}{\to} \ker c \stackrel{\delta}{\to} \operatorname{coker} a \stackrel{f'}{\to} \operatorname{coker} b \stackrel{g'}{\to} \operatorname{coker} c,$$

where $\ker x \stackrel{h}{\to} \ker y$ is restriction, δ is the connecting morphism, and $\operatorname{coker} x \stackrel{h'}{\to} \operatorname{coker} y$ is induced by h' by modding out.

(b) If f is injective, then $\ker a \stackrel{f}{\to} \ker b$ is injective.

(c) If g' is surjective, then $\operatorname{coker} b \stackrel{g'}{\to} \operatorname{coker} c$ is surjective.

Proof. The point is to prove (a), and we will show (b) and (c) in the process. We will show that each of the maps are well-defined for (a), but we will not do the exactness checks because they should not be read. Indeed, readers are encouraged to not read this proof at all (except, perhaps, for the definition of δ) and attempt a proof on their own.

- We construct δ. In short, we define
$$\delta := (f')^{-1} \circ b \circ g^{-1}.$$
In more words, fix some $z \in \ker c$. Then we use the surjectivity of g to pull z back and find $y \in B$ such that $g(y) = z$. From there, we push y forwards to $b(y)$, from which we note
$$g'(b(y)) = (g' \circ b)(y) = (c \circ g)(y) = c(g(y)) = c(z) = 0$$
because $z \in \ker c$. Thus, $b(y) \in \ker g'$, but $\ker g' = \operatorname{im} f'$ by exactness, so we can pull back $b(y) \in \operatorname{im} f'$ to some $x' \in A'$ such that $f'(x') = b(y)$. In particular, x' is unique given $b(y)$ because f' is injective by exactness.

  The above does not describe a well-defined map $\ker c \to A'$ because pulling $z \in C$ back yo $y \in B$ with $g(y) = z$ is unique. However, we can fix this: if we pick up $y_1, y_2 \in B$ such that $g(y_1) = g(y_2) = z$, then $g(y_1 - y_2) = z - z = 0$, so
$$y_1 - y_2 \in \ker g = \operatorname{im} f$$
by exactness. So find some $x \in A$ such that $f(x) = y_1 - y_2$. Then, when we pull $b(y_1)$ and $b(y_2)$ back along f' to x_1' and x_2' respectively, we see that
$$f'(x_1' - x_2') = f'(x_1') - f'(x_2') = b(y_1) - b(y_2) = b(y_1 - y_2) = (bf)(x) = (f'a)(x) = f'(a(x)),$$
so $x_1' - x_2' = a(x) \in \operatorname{im} a$ by injectivity of f'. Thus, x_1' and x_2' do live in the same coset in $\operatorname{coker} a$, so we have a well-defined map $\delta : \ker c \to \operatorname{coker} a$.

- To construct the maps $\ker x \xrightarrow{h} \ker y$ by restriction, we fix the following square to focus on.
$$\begin{tikzcd} X \arrow[r, "h"] \arrow[d, "x"'] & Y \arrow[d, "y"] \\ X' \arrow[r, "h'"'] & Y' \end{tikzcd} \tag{$*$}$$
(Notably, we are applying this to the square with $\{A, B, A', B'\}$ and the square with $\{B, C, B', C'\}$.) We need to show that h restricted to $\ker x$ outputs into $\ker y$. Well, any $a \in \ker x$ will have
$$y(h(a)) = (y \circ h)(a) = (h' \circ x)(a) = h'(x(a)) = 0$$
by the commutativity of ($*$). Thus, we have an induced map $h : \ker x \to \ker y$ by restriction.

  To close, we note that we can show (b) without tears: the map $\ker a \xrightarrow{f} \ker b$ is f on restriction, so this map is injective for free when f is injective. Indeed, $f(x) = f(y)$ for $x, y \in \ker a$ implies $x = y$ because f is injective.

- To construct the maps $\ker x \xrightarrow{h'} \ker y$ by restriction, we fix the same square ($*$); again, we are applying this to the square with $\{A, B, A', B'\}$ and the square with $\{B, C, B', C'\}$.

  We need to induce a map $\operatorname{coker} x \to \operatorname{coker} y$. The main point is to show that h' sends $\operatorname{im} x$ to $\operatorname{im} y$. Indeed, for any $x(a) \in \operatorname{im} x$, we see that
$$h'(x(a)) = (h' \circ x)(a) = (y \circ h)(a) = y(h(a)) \in \operatorname{im} y$$
by the commutativity of ($*$). Thus, we have an induced map $h' : \operatorname{im} x \to \operatorname{im} y$ by restriction. In particular, we can take the composite
$$X' \xrightarrow{h'} Y' \twoheadrightarrow Y'/\operatorname{im} y = \operatorname{coker} y$$
and mod out by $\operatorname{im} x$ in the front because $h'(\operatorname{im} x) \subseteq \operatorname{im} y$. So this is exactly our map $\operatorname{coker} x \to \operatorname{coker} y$; explicitly, we are sending $[x'] \mapsto [h'(x')]$.

  To close, we note that we can show (c) without tears: the map $\operatorname{coker} b \xrightarrow{g'} \operatorname{coker} c$ is g' on modding out, so this map is surjective for free when g' is surjective. Indeed, for any $[c'] \in \operatorname{coker} c$, there is $b' \in B'$ with $g'(b') = c'$, so $[c'] = [g'(b')]$ lives in the image of the induced map of g'.

So far we have constructed the maps in the exact sequence for (a) and showed (b) and (c). As stated above, we will omit the exactness checks for (a). ■

We now proceed with the proof of Theorem 4.82.

Proof of Theorem 4.82. The main idea is to use Lemma 4.83 to induce an exact sequence as follows.

$$\begin{tikzcd} H_i(A) \arrow[r, "H_i(\varphi)"] & H_i(B) \arrow[r, "H_i(\psi)"] & H_i(C) \arrow[dll, "\delta_i"] \\ H_{i-1}(A) \arrow[r, "H_{i-1}(\varphi)"'] & H_{i-1}(B) \arrow[r, "H_{i-1}(\psi)"'] & H_{i-1}(C) \end{tikzcd} \tag{1}$$

As such, we want to create a snake diagram where the terms $H_i(X) = \ker \partial_i^X / \operatorname{im} \partial_{i+1}^X$ appear as kernels and the terms $H_{i-1}(X) = \ker \partial_{i-1}^X / \operatorname{im} \partial_i^X$ appear as cokernels. With this in mind, we draw the following diagram.

$$\begin{tikzcd} & A_i/\operatorname{im}\partial_{i+1}^A \arrow[r, "\varphi_i"] \arrow[d, "\partial_i^A"'] & B_i/\operatorname{im}\partial_{i+1}^B \arrow[r, "\psi_i"] \arrow[d, "\partial_i^B"] & C_i/\operatorname{im}\partial_{i+1}^C \arrow[r] \arrow[d, "\partial_i^C"] & 0 \\ 0 \arrow[r] & \ker\partial_{i-1}^A \arrow[r, "\varphi_{i-1}"'] & \ker\partial_{i-1}^B \arrow[r, "\psi_{i-1}"'] & \ker\partial_{i-1}^C & \end{tikzcd} \tag{2}$$

We have the following remarks on (2).

- As discussed in Lemma 4.75, we see that φ_i (respectively, ψ_i) maps $\operatorname{im}\partial_{i+1}^A$ (respectively, ∂_{i+1}^B) to $\operatorname{im}\partial_{i+1}^B$ (respectively, $\operatorname{im}\partial_{i+1}^C$), so we have induced maps $\varphi_i : A_i/\operatorname{im}\partial_{i+1}^A \to B_i/\operatorname{im}\partial_{i+1}^B$ and $\psi_i : B_i/\operatorname{im}\partial_{i+1}^B \to C_i/\operatorname{im}\partial_{i+1}^C$. These are our maps along the top.

  Similarly, Lemma 4.75 tells us that we have restriction maps $\varphi_{i-1} : \ker\partial_{i-1}^A \to \ker\partial_{i-1}^B$ and $\psi_{i-1} : \ker\partial_{i-1}^B \to \ker\partial_{i-1}^C$. These are our maps along the bottom.

- The vertical maps $\partial_i^X : X_i/\operatorname{im}\partial_{i-1}^X \to \ker\partial_i^X$ are well-defined because $\left(\partial^X\right)^2 = 0$ implies

$$\partial_{i-1}^X\partial_i^X = 0 \qquad \text{and} \qquad \partial_i^X\partial_{i+1}^X = 0,$$

  so $\partial_i^X : X_i \to X_{i-1}$ maps into the kernel of ∂_{i-1}^X (by the first equality above) and contains $\operatorname{im}\partial_{i+1}^X$ in its kernel (by the second equality above), so we get to induce a map $\partial_i^X : X_i/\operatorname{im}\partial_{i-1}^X \to \ker\partial_i^X$.

- We check that the diagram commutes. It will suffice to show that the square

$$\begin{tikzcd} A_i/\operatorname{im}\partial_{i+1}^A \arrow[r, "\varphi_i"] \arrow[d, "\partial_i^A"'] & B_i/\operatorname{im}\partial_{i+1}^B \arrow[d, "\partial_i^B"] \\ \ker\partial_{i-1}^A \arrow[r, "\varphi_{i-1}"'] & \ker\partial_{i-1}^B \end{tikzcd}$$

  commutes for any chain morphism $\varphi : \left(A, \partial^A\right) \to \left(B, \partial^B\right)$ and then apply this to both squares in the diagram. Well, along the top, we have $[a]$ goes to $[\varphi_i a]$ goes to $\partial_i^B\varphi_i(a)$; along the bottom, we have $[a]$ goes to $\partial_i^A a$ goes to $\varphi_{i-1}\partial_i^A a$. These outputs are equal because φ is a chain morphism.

We will show that (2) has exact rows as an application of Lemma 4.83. Assuming this for a moment, we note that applying Lemma 4.83 directly to (2): note $\ker\partial_i^X$ consists of the cosets of $[x] = X_i/\operatorname{im}\partial_{i+1}^X$ such that $x \in \ker\partial_i^X$, which is simply $\ker\partial_i^X/\operatorname{im}\partial_{i+1}^X = H_i(X)$. Similarly, $\operatorname{coker}\partial_i^X$ is $\ker\partial_{i-1}^X$ modded out by the image of $X_i/\operatorname{im}\partial_{i+1}^X$, which is just the image of X_i, so we have $\operatorname{coker}\partial_i^X = \ker\partial_{i-1}^X/\operatorname{im}\partial_i^X$. Thus, Lemma 4.83 gives us an exact sequence as follows.

$$\begin{tikzcd} H_i(A) \arrow[r, "\varphi_i"] & H_i(B) \arrow[r, "\psi_i"] & H_i(C) \arrow[dll, "\delta_i"] \\ H_{i-1}(A) \arrow[r, "\varphi_{i-1}"'] & H_{i-1}(B) \arrow[r, "\psi_{i-1}"'] & H_{i-1}(C) \end{tikzcd}$$

Very quickly, we note that φ_i along the top sends $[a] \in A_i/\operatorname{im}\partial_{i+1}^A$ to $[\varphi_i a] = H_i(\varphi)([a])$, so this map is $H_i(\varphi)$; in the same way, ψ_i along the top is $H_i(\psi)$. Further, φ_{i-1} along the bottom sends $[a] \in \ker\partial_{i-1}^A/\operatorname{im}\partial_i^A$ to $[\varphi_{i-1}a] = H_{i-1}(\varphi)[a]$; in the same way, ψ_{i-1} along the bottom is $H_{i-1}(\psi)$. Thus, we have exhibited (1); superimposing the shifts of (1) gives the desired long exact sequence.

It remains to show that (2) has exact rows. After shifting indices in the top and bottom rows together and noting $X_i/\operatorname{im}\partial_{i+1}^X = \operatorname{coker}\partial_{i+1}^X$, it suffices to show that the sequence

$$0 \to \ker\partial_i^A \stackrel{\varphi_i}{\to} \ker\partial_i^B \stackrel{\psi_i}{\to} \ker\partial_i^C \stackrel{\delta}{\to} \operatorname{coker}\partial_i^A \stackrel{\varphi_i}{\to} \operatorname{coker}\partial_i^B \stackrel{\psi_i}{\to} \operatorname{coker}\partial_i^C \to 0$$

is exact, for some connecting morphism δ. (The exactness of left half gives exactness of the bottom row of (2), and the exactness of the right half gives exactness of the top row of (2).) Notably, the maps between kernels are by restriction, and the maps between cokernels are induced. Well, looking at Lemma 4.83, we draw the following diagram.

$$\begin{tikzcd}
0 \arrow[r] & A_i \arrow[r, "\varphi_i"] \arrow[d, "\partial_i^A"'] & B_i \arrow[r, "\psi_i"] \arrow[d, "\partial_i^B"] & C_i \arrow[r] \arrow[d, "\partial_i^C"] & 0 \\
0 \arrow[r] & A_{i+1} \arrow[r, "\varphi_{i+1}"'] & B_{i+1} \arrow[r, "\psi_{i+1}"'] & C_{i+1} \arrow[r] & 0
\end{tikzcd}$$

The diagram commutes and is exact because we are supposed to start with a short exact sequences of complexes. Thus, Lemma 4.83 gives us a short exact sequence

$$0 \to \ker\partial_i^A \stackrel{\varphi_i}{\to} \ker\partial_i^B \stackrel{\psi_i}{\to} \ker\partial_i^C \stackrel{\delta}{\to} \operatorname{coker}\partial_i^A \stackrel{\varphi_i}{\to} \operatorname{coker}\partial_i^B \stackrel{\psi_i}{\to} \operatorname{coker}\partial_i^C \to 0,$$

which is exactly what we need; note that the maps between kernels are by restriction and the maps between cokernels are induced, so we did provide exactness of the correct sequence of morphisms. (In particular, we get the 0s on the ends of the above exact sequence by (b) and (c) of Lemma 4.83.) ■

4.3 March 3

Welcome back everybody.

4.3.1 Projective Resolutions

Today we will discuss homological methods to determine flatness. As mentioned last class, we will want to introduce the functor Tor, so we want to be able to talk about left-derived functors.

We will make left-derived functors out of projective resolutions, so that is where we will start.

Definition 4.84 (Resolution)**.** Given an R-module M a *resolution of M* is a chain complex (P, ∂) such that

$$P_i = 0 \qquad \text{for } i < 0.$$

Additionally, we require an augmentation map $\varepsilon : P_0 \twoheadrightarrow M$ so that

$$\cdots \stackrel{\partial_3}{\to} P_2 \stackrel{\partial_2}{\to} P_1 \stackrel{\partial_1}{\to} P_0 \stackrel{\varepsilon}{\to} M \to 0$$

is an exact sequence. We call the above complex the *augmented resolution*, and we notate it by $P \to M$.

Remark 4.85. Alternatively, we can just look at the complex

$$\cdots \overset{\partial_3}{\to} P_2 \overset{\partial_2}{\to} P_1 \overset{\partial_1}{\to} P_0 \overset{\partial_0}{\to} 0$$

and ask to be exact at all terms except at P_0, where we require $H_0(P) = \ker \partial_0 / \operatorname{im} \partial_1 = M$. In particular, we note $\ker \partial_0 = P_0$ because $\partial_0 : P_0 \to 0$, so ∂_0 induces a surjection $P \twoheadrightarrow M$ with kernel $\operatorname{im} \partial_1$. So we can insert M to make an exact sequence

$$\cdots \overset{\partial_3}{\to} P_2 \overset{\partial_2}{\to} P_1 \overset{\partial_1}{\to} P_0 \overset{\partial_0}{\to} M \to 0.$$

Definition 4.86 (Projective, free resolutions)**.** Fix an R-module M with a resolution (P, ∂).

- The resolution is *projective* if and only if P_i is projective for $i \geq 0$.
- The resolution is *free* if any only if P_i is free over $i \geq 0$.

Remark 4.87. Because free modules are projective (see Lemma 4.55 part (c), for example), it follows that a free resolution is a projective resolution.

To start, we give every module a projective resolution.

Lemma 4.88. Every R-module M has a free resolution and therefore a projective resolution.

Proof. We build the augmented resolution $P \to M$, which we callously call P (so that $P_{-1} = M$). The point is to use Lemma 4.56. We produce our injective resolution inductively. To start our resolution (P, ∂), we start as required with

$$P_i = \begin{cases} M & i = -1, \\ 0 & i < -1, \end{cases}$$

and $\partial_i = 0$ for $i \leq -1$. We now claim that, for any $n \in \mathbb{N}$, we can construct projective modules $\{P_i\}_{i=0}^n$ with maps $\partial_i : P_i \to P_{i-1}$ such that

$$P_n \overset{\partial_n}{\to} P_{n-1} \overset{\partial_{n-1}}{\to} \cdots \overset{\partial_2}{\to} P_1 \overset{\partial_1}{\to} P_0 \overset{\partial_0}{\to} M \to 0$$

is an exact sequence. This induction will finish the proof.[6]

For $n = 0$, we use Lemma 4.56 to find a free module P_0 which surjects onto M as $\partial_0 : P_0 \twoheadrightarrow M$. Thus,

$$P_0 \overset{\partial_0}{\to} M \to 0$$

is exact at M because the kernel of $0 : M \to 0$ is all of M, which is precisely the image of $\partial_0 : P_0 \twoheadrightarrow M$.

For the inductive step, we begin with our exact sequence

$$P_n \overset{\partial_n}{\to} P_{n-1} \overset{\partial_{n-1}}{\to} \cdots \overset{\partial_2}{\to} P_1 \overset{\partial_1}{\to} P_0 \overset{\partial_0}{\to} M \to 0$$

and extend it by P_{n+1}. Indeed, by Lemma 4.56, we can find a free module P_{n+1} with a surjection $\partial_{n+1} : P_{n+1} \twoheadrightarrow \ker \partial_n$. Tacking this on the front, we have the sequence

$$P_{n+1} \overset{\partial_{n+1}}{\to} P_n \overset{\partial_n}{\to} P_{n-1} \overset{\partial_{n-1}}{\to} \cdots \overset{\partial_2}{\to} P_1 \overset{\partial_1}{\to} P_0 \overset{\partial_0}{\to} M \to 0.$$

[6] Technically, one might want to use something like Zorn's lemma to actually go get the projective resolution with infinitely many terms, but we won't do this here.

It remains to show that this sequence is exact. Well, by the inductive hypothesis, we already have exactness at everyone in $\{P_{n-1}, P_{n-2}, \ldots, P_1, P_0, M\}$. It remains to show exactness at P_n. Well, by construction of ∂_{n+1}, we see that

$$\operatorname{im} \partial_{n+1} = \ker \partial_n,$$

which is exactly the exactness condition at P_n. ■

Remark 4.89 (Nir). There is a complaint that Lemma 4.56 products huge free modules to project. However, if R is Noetherian and M is finitely generated, then we can choose a resolution of free and finitely generated modules.

To see this, we proceed inductively: M is finitely generated, so we can choose P_0 to be free of finite rank surjecting onto M. Then, for the inductive step, P_n is free of finite rank, and $\ker \partial_n \subseteq P_n$ is a submodule of the Noetherian module P_n, so $\ker \partial_n$ is finitely generated, so we can surject onto it with a free module P_{n+1} of finite rank.

Example 4.90. Fix $R := k[x]/\left(x^2\right)$. Then k is an R-module, where the x acts by 0: we can induce a map $k[x] \to k$ by lifting $\mathrm{id}_k : k \to k$ by $x \mapsto 0$, and then we can mod out $k[x]$ by $x^2 \mapsto 0$, which gives us our map $\pi : R \to k$. Note $ax + b \in \ker \pi$ if and only if $bx = x(ax+b) = 0$, so $\ker \pi = kx$.

To start our projective resolution, we note we have a surjection

$$R \xrightarrow{\pi} k \to 0$$

with kernel kx; in particular, π is surjective because π lifts $\mathrm{id}_k : k \to k$. But now, we see that $\ker \pi = kx \cong k$ by $ax \mapsto a$, so we can project onto this kernel from R by $ax + b \mapsto b \mapsto bx = x(ax+b)$. Thus, employing the algorithm in Lemma 4.88, we can create a free resolution

$$\cdots \xrightarrow{x} R \xrightarrow{x} R \xrightarrow{x} R \to k \to 0.$$

4.3.2 Creating Chain Morphisms

Warning 4.91 (Nir). The proofs in the next two subsections were written for augmented resolutions and then edited later to accommodate the correct definition of a projective resolution. There might be typos and are many elided details in this transition.

One complaint is that our proof of Lemma 4.88 did not produce a unique projective resolution. However, projective resolutions are unique in the following way.

Lemma 4.92. Suppose that $P := \overline{P} \to M$ and $Q := \overline{Q} \to M$ are augmented projective resolutions for an R-module M. Then there are chain morphisms $\alpha : P \to Q$ and $\beta : Q \to B$ such that $\alpha\beta \sim \mathrm{id}_Q$ and $\beta\alpha \sim \mathrm{id}_P$.

For this, it will be convenient to talk about how to induce chain morphisms for projective resolutions.

Lemma 4.93. Suppose that $P := \overline{P} \to M$ and $Q := \overline{Q} \to N$ are projective resolutions for the R-modules M and N, respectively. Then an R-module homomorphism $\varphi : M \to N$ can be extended to a chain morphism $\varphi : P \to Q$.

Proof. The point is to use the fact our modules are projective to extend the morphism $\varphi_{-1} : P_{-1} \to Q_{-1}$

backwards. In particular, for $i < -1$, we set $\varphi_i = 0$ so that the following diagram commutes for any $i \leq -1$.

$$\begin{tikzcd} P_i \arrow[r, "\partial_i^P"] \arrow[d, "\varphi_i"'] & P_{i-1} \arrow[d, "\varphi_{i-1}"] \\ Q_i \arrow[r, "\partial_i^Q"'] & Q_{i-1} \end{tikzcd}$$

Namely, the top and bottom arrows are both 0s, so the diagram commutes for free.

Because we have φ_i for $i \leq -1$, it suffices exhibit the φ_i for $i \geq 0$ inductively, assuming that we have φ_{i-1}; this will finish by muttering something about Zorn's lemma. Namely, we need to induce φ_i to make the following diagram commute.

$$\begin{tikzcd} P_i \arrow[r, "\partial_i^P"] \arrow[d, dashed, "\varphi_i"'] & P_{i-1} \arrow[r, "\partial_{i-1}^P"] \arrow[d, "\varphi_{i-1}"] & P_{i-2} \arrow[d, "\varphi_{i-2}"] \\ Q_i \arrow[r, "\partial_i^Q"'] & Q_{i-1} \arrow[r, "\partial_{i-1}^Q"'] & Q_{i-2} \end{tikzcd}$$

We would like the fact that P_i is projective in order to induce this arrow, but ∂_i^Q is not a surjection. However, ∂_i^Q does surject onto $\operatorname{im} \partial_i^Q = \ker \partial_{i-1}^Q$ (by exactness), so we would like $\varphi_{i-1} \circ \partial_i^P$ to map into this kernel. Well, we can use the commutativity of the right square to write

$$\partial_{i-1}^Q \circ \varphi_{i-1} \circ \partial_i^P = \varphi_{i-2} \circ \partial_{i-1}^P \circ \partial_i^P = \varphi_{i-2} \circ 0 = 0,$$

so $\operatorname{im}(\varphi_{i-1} \circ \partial_i^P) \subseteq \ker \partial_{i-1}^Q = \operatorname{im} \partial_i^Q$. Thus, the following diagram is well-defined.

$$\begin{tikzcd} P_i \arrow[d, dashed, "\varphi_i"'] \arrow[dr, "\varphi_{i-1} \circ \partial_i^P"] & \\ Q_i \arrow[r, two heads, "\partial_i^Q"'] & \operatorname{im} \partial_i^Q \end{tikzcd}$$

So, because P_i is projective, we are promised an induced morphism $\varphi_i : P_i \to Q_i$ such that $\partial_i^Q \circ \varphi_i = \varphi_{i-1} \circ \partial_i^P$, which is what we wanted. ■

Now, these induced chain morphisms do not look unique either (namely, the arrow provided by the projective condition need not be unique), but they are unique in the following sense.

> **Lemma 4.94.** Suppose that $P := \overline{P} \to M$ and $Q := \overline{Q} \to N$ are augmented projective resolutions for the R-modules M and N, respectively. Further, fix two chain morphisms $\alpha, \beta : P \to Q$ such that $\alpha_{-1} = \beta_{-1}$; i.e., the restrictions of α and β to $M \to N$ are equal. Then α and β are homotopic.

Proof. By Lemma 4.80, it suffices to show that $\alpha - \beta \sim 0$, so set $\varphi := \alpha - \beta$. In particular, we know that $\varphi_{-1} = \alpha_{-1} - \beta_{-1} = 0$, and we would like to extend this to $\varphi \sim 0$.

Unsurprisingly, we construct our chain homotopy h to witness $\varphi \sim 0$ inductively; i.e., we want $\varphi_i = h_{i-1}\partial_i^P + \partial_{i+1}^Q h_i$ for each i. To start off, we set $h_i = 0$ for $i \leq -1$ because this is a morphism $h_i : P_i \to Q_{i+1}$, which must be the zero morphism anyways. Observe that $i \leq -1$ will then have

$$\varphi_i = 0 = h_{i-1}\partial_i^P + \partial_{i+1}^Q h_i$$

because everything involved is 0. For the inductive step, we have $i \geq 0$ and are trying to induce the arrow h_i in the following diagram which does not commute.

$$\begin{tikzcd} & P_i \arrow[r, "\partial_i^P"] \arrow[dl, dashed, "h_i"'] \arrow[d, dashed, "\varphi_i"] & P_{i-1} \arrow[dl, "h_{i-1}"] \\ Q_{i+1} \arrow[r, "\partial_{i+1}^Q"'] & Q_i & \end{tikzcd}$$

As usual, we would like to induce h_i using the fact that P_i is projective. The main point is to show that $\varphi_i - h_{i-1}\partial_i^P$ maps into $\operatorname{im}\partial_{i+1}^Q = \ker\partial_i^Q$. Well, because $\varphi_{i-1} = h_{i-2}\partial_{i-1}^P + \partial_i^Q h_{i-1}$ already, we compute

$$\begin{aligned}\partial_i^Q\left(\varphi_i - h_{i-1}\partial_i^P\right) &= \partial_i^Q\varphi_i - \partial_i^Q h_{i-1}\partial_i^P \\ &= \partial_i^Q\varphi_i - \left(\varphi_{i-1} - h_{i-2}\partial_{i-1}^P\right)\partial_i^P \\ &= \left(\partial_i^Q\varphi_i - \varphi_{i-1}\partial_i^P\right) + h_{i-2}\partial_{i-1}^P\partial_i^P.\end{aligned}$$

The left term here is zero because φ is a chain morphism; the right term is zero by exactness of P. Thus, $\operatorname{im}\left(\varphi_i - h_{i-1}\partial_i^P\right) \subseteq \ker\partial_i^Q = \operatorname{im}\partial_{i+1}^Q$, so the following diagram makes sense.

$$\begin{tikzcd} & P_i \arrow[dl, dashed, "h_i"'] \arrow[d, "\varphi_i - h_{i-1}\partial_i^P"] \\ Q_{i+1} \arrow[r, two heads, "\partial_{i+1}^Q"'] & \operatorname{im}\partial_{i+1}^Q \end{tikzcd}$$

In particular, the fact that P_i is projective grants us a morphism h_i such that

$$\partial_{i+1}^Q h_i = \varphi_i - h_{i-1}\partial_i^P,$$

which is what we wanted. ■

We are now ready to prove Lemma 4.92.

Proof of Lemma 4.92. To start, we use Lemma 4.93 to construct chain morphisms $\alpha : P \to Q$ and $\beta : Q \to P$ such that $\alpha_{-1} = \beta_{-1} = \mathrm{id}_M$.

By symmetry, it suffices to show that $\alpha\beta \sim \mathrm{id}_Q$. Well, $\alpha\beta : Q \to Q$ is a chain morphism such that

$$(\alpha\beta)_{-1} = \alpha_{-1}\beta_{-1} = \mathrm{id}_M\,\mathrm{id}_M = \mathrm{id}_M,$$

and $\mathrm{id}_Q : Q \to Q$ is also a chain morphism such that $(\mathrm{id}_Q)_{-1} = \mathrm{id}_M$. This finishes by Lemma 4.94. ■

4.3.3 The Horseshoe Lemma

Arguably, the "main point" of homology is to introduce the amazing long exact sequence in Theorem 4.82. To apply this story to projective resolutions, we will need a way to create a short exact sequence of projective resolutions.

Proposition 4.95 (Horseshoe lemma)**.** Fix a short exact sequence of R-modules named

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

Further, suppose we have augmented projections resolutions $P' = \overline{P'} \to M'$ and $P'' := \overline{P''} \to M''$ for M' and M'', respectively. Then we can form an augmented projective resolution $P := \overline{P} \to M$ for M such that

$$0 \to P' \to P \to P'' \to 0$$

is a split short exact sequence of complexes.

Proof. This is a little technical. Let our short exact sequence of R-modules be

$$0 \to M' \xrightarrow{\iota} M \xrightarrow{\pi} M'' \to 0,$$

and name our projective resolutions (P', ∂') and (P'', ∂'') for M' and M''. To ground ourselves, we'll say from the outset that

$$P_i := \begin{cases} M & i = -1, \\ P_i' \oplus P_i'' & i \neq -1. \end{cases}$$

Further, we set $\iota_i : P'_i \to P_i$ be ι at $i = -1$ and the canonical inclusion otherwise; similarly, set $\pi_i : P_i \to P''_i$ be π at $i = -1$ and the canonical projection otherwise. Thus, $\operatorname{im} \iota_i = \ker \pi_i$ for all i, by construction. As such,

$$0 \to P' \to P \to P'' \to 0$$

will be a short exact sequence of complexes as soon as we exhibit the needed map $\partial : P \to P$. We have two constraints.

- To make (P, ∂) a valid projective resolution, we require $\operatorname{im} \partial_i = \ker \partial_{i-1}$ for each i.
- To make ι and π valid chain morphisms, we need $\partial'_i \iota_{i-1} = \iota_i \partial_i$ and $\partial_i \pi_{i-1} = \pi_i \partial''_i$ for each $i \le -1$.

Of course, we will set $\partial_i = 0$ for $i \le -1$ because $P_{i+1} = 0$ here, which gives $\operatorname{im} \partial_i = \ker \partial_{i-1}$ as well as $\partial'_i \iota_{i-1} = \iota_i \partial_i$ and $\partial_i \pi_{i-1} = \pi_i \partial''_i$ for each $i \le -1$.

From here, it should not be a surprise that we will inductively construct ∂_i for $i \ge 0$. In particular, we want to exhibit ∂_i in the following diagram.

$$\begin{tikzcd} 0 \arrow[r] & P'_{i-1} \arrow[r, "\iota_{i-1}"] & P_{i-1} \arrow[r, "\pi_{i-1}"] & P''_{i-1} \arrow[r] & 0 \\ 0 \arrow[r] & P'_i \arrow[u, "\partial'_i"] \arrow[r, "\iota_i"'] & P'_i \oplus P''_i \arrow[u, dashed, "\partial_i"'] \arrow[r, "\pi_i"'] & P''_i \arrow[u, "\partial''_i"'] \arrow[r] & 0 \end{tikzcd} \tag{1}$$

Well, we have a map $f_i : P'_i \to P_{i-1}$ by $f_i := \iota_{i-1} \partial'_i$. To get a map $P''_i \to P_{i-1}$, we use the fact that P''_i is projective: $\pi_{i-1} : P_{i-1} \twoheadrightarrow P''_{i-1}$ is a surjection, so we can pull $\partial''_{i-1} : P_{i-1} \to P''_{i-1}$ backwards to a map $f'_i : P''_i \to P_{i-1}$ such that $\pi_{i-1} f'_i = \partial''_{i-1}$. We acknowledge that we have some freedom in our choice of f'_i, which we will restrict later.

From here, we set

$$\partial_i := f_i \oplus f'_i.$$

We now run our checks on ∂_i. Note that $\iota_{i-1} \partial'_i = f_i = \partial_i \iota_i$. Further, note that $\pi_{i-1} f_i = \pi_{i-1} \iota_{i-1} \partial'_i = 0$ by the exactness of the top row, so

$$\pi_{i-1} \partial_i = \pi_{i-1}(f_i \oplus f'_i) = (\pi_{i-1} f_i) \oplus (\pi_{i-1} f'_i) = 0 \oplus \partial''_{i-1} = \partial''_{i-1} \pi_i.$$

So we have made ι and π into valid chain morphisms.

It remains to show that (P, ∂) is a complex which is exact everywhere; i.e., we need $\operatorname{im} \partial_i = \ker \partial_{i-1}$. The trick is to claim that we can construct such a ∂_i with the additional constraint that

$$0 \to \ker \partial'_i \overset{\iota_i}{\to} \ker \partial_i \overset{\pi_i}{\to} \ker \partial''_i \to 0.$$

We show this claim by induction.

When $i = 0$, we simply use the above construction for ∂_i. Then (1) is a morphism of short exact sequences, so Lemma 4.83 gives us the exact sequence

$$0 \to \ker \partial'_0 \to \ker \partial_0 \to \ker \partial''_0 \to \operatorname{coker} \partial'_0 \to \operatorname{coker} \partial_0 \to \operatorname{coker} \partial''_0 \to 0.$$

But now we see that $\partial'_0 : P'_0 \to M'$ and $\partial''_0 : P''_0 \to M''$ are both surjective, so $\operatorname{coker} \partial'_0 = 0$ and $\operatorname{coker} \partial''_0 = 0$. Thus, the above sequence forces $\operatorname{coker} \partial_0 = 0$, so $\operatorname{im} \partial_0 = M = \ker \partial_{-1}$. Additionally, we do indeed get our short exact sequence

$$0 \to \ker \partial'_0 \to \ker \partial_0 \to \ker \partial''_0 \to 0.$$

Now, when $i > 0$, induction grants us a short exact sequence

$$0 \to \ker \partial'_{i-1} \overset{\iota_{i-1}}{\to} \ker \partial_{i-1} \overset{\pi_{i-1}}{\to} \ker \partial''_{i-1} \to 0.$$

By exactness of P' and P'', we see that $\operatorname{im} \partial'_i = \ker \partial'_{i-1}$ and $\operatorname{im} \partial''_i = \ker \partial''_{i-1}$, so we can rewrite (1) as follows.

$$\begin{tikzcd} 0 \arrow[r] & P'_i \arrow[d, "\partial'_i"'] \arrow[r, "\iota_i"] & P'_i \oplus P''_i \arrow[d, dashed, "\partial_i"] \arrow[r, "\pi_i"] & P''_i \arrow[d, "\partial''_i"] \arrow[r] & 0 \\ 0 \arrow[r] & \ker \partial'_{i-1} \arrow[r, "\iota_{i-1}"'] & \ker \partial'_{i-1} \arrow[r, "\pi_{i-1}"'] & \ker \partial''_{i-1} \arrow[r] & 0 \end{tikzcd} \tag{2}$$

Notably, we have chosen to replace P_{i-1} with $\ker \partial_{i-1}$! So now, redoing the construction of ∂_i with $\ker \partial_{i-1}$ as the codomain, we get a map $\partial_i : P_i \to \ker \partial_{i-1}$ such that the above diagram commutes. Running Lemma 4.83 on (2), we get the exact sequence

$$0 \to \ker \partial_i' \to \ker \partial_i \to \ker \partial_i'' \to \operatorname{coker} \partial_i' \to \operatorname{coker} \partial_i \to \operatorname{coker} \partial_i'' \to 0.$$

Once more, exactness of P' and P'' promises $\operatorname{coker} \partial_i' = \operatorname{coker} \partial_i'' = 0$, so $\operatorname{coker} \partial_i = 0$ in (2), meaning that $\operatorname{im} \partial_i = \ker \partial_{i-1}$, as needed. Additionally, we do indeed get

$$0 \to \ker \partial_i' \to \ker \partial_i \to \ker \partial_i'' \to 0,$$

which finishes the induction. ■

4.3.4 Left-Derived Functors

We are now ready to talk about left-derived functors. The functor Tor will fall out of this theory, but we will continue with the generality for a little while longer. For left-derived functors, we need to start with an additive right-exact functor Φ.

Definition 4.96 (Additive)**.** A functor $\Phi : \operatorname{Mod}_R \to \operatorname{Mod}_S$ is *additive* if and only if, for any R-modules M and N, the induced map

$$\Phi : \operatorname{Hom}_R(M, N) \to \operatorname{Hom}_R(\Phi M, \Phi N)$$

is a homomorphism of abelian groups.

Definition 4.97 (Right exact)**.** A functor $\Phi : \operatorname{Mod}_R \to \operatorname{Mod}_S$ is *right-exact* if and only if Φ sends right-exact sequences to right-exact sequences.

Example 4.98. In the discussion that follows, keeping $\Phi := - \otimes_R M$ in mind is not a bad idea; this will be the only example that we care about because it will give Tor. To be explicit, we already know that Φ is right-exact, and it is additive by simply checking: $\varphi, \psi : A \to B$ give

$$(\varphi \otimes M + \psi \otimes M)(a \otimes m) = \varphi(a) \otimes m + \psi(a) \otimes m = (\varphi + \psi)(a) \otimes m = ((\varphi + \psi) \otimes M)(a \otimes m).$$

Here's a reason why we want the additive condition.

Lemma 4.99. Additive functors Φ preserve the zero object.

Proof. Note that an additive functor Φ must preserve the zero morphism, but when 0 is our zero object, this is our identity. So

$$\Phi \operatorname{id}_0 = \operatorname{id}_{\Phi 0}$$

must still be a zero morphism, so $\Phi 0$ is the zero object. ■

Here is a better reason.

Lemma 4.100. Additive functors Φ preserves split short exact sequences.

Proof. The idea is to turn being a split short exact sequence into some system of equations which Φ will then preserve. By the proof of Lemma 4.53, the short exact sequence

$$0 \to A \xrightarrow{\iota} B \xrightarrow{\pi} C \to 0$$

splitting implies that we have an isomorphism $\iota \oplus \varphi : A \oplus C \to B$ such that $\pi\varphi = \mathrm{id}_C$. In addition, we see that this gives an arrow $B \cong A \oplus C \to A$ which we name ψ such that $\psi\iota = \mathrm{id}_A$. Notably, $\psi\varphi = 0$ because

$$\psi(\iota \oplus \varphi)(\iota \oplus \varphi)^{-1}\varphi(c) = \psi(\iota \oplus \varphi)(0, c) = 0$$

because $\psi(\iota \oplus \varphi)$ projects onto the A-coordiante. It follows

$$\iota\psi + \varphi\pi = \mathrm{id}_B$$

because multiplying by the invertible morphism $\iota \oplus \varphi$ on the right gives $(\iota \oplus 0) + (0 \oplus \varphi) = (\iota \oplus \varphi)$, which is true.

Now, applying Φ everywhere, we get the sequence of maps

$$0 \to \Phi A \overset{\Phi\iota}{\to} \Phi B \overset{\Phi\pi}{\to} \Phi C \to 0,$$

which we would like to show is a split short exact sequence. We see $(\Phi\psi)(\Phi\iota) = \mathrm{id}_{\Phi A}$, so $\Phi\iota$ is injective. Also, $(\Phi\pi)(\Phi\varphi) = \mathrm{id}_{\Phi C}$, so $\Phi\pi$ is surjective. Further, we have

$$(\Phi\iota)(\Phi\psi) + (\Phi\varphi)(\Phi\pi) = \mathrm{id}_{\Phi B} \qquad (*)$$

because Φ is additive (!).

So to finish, we need to show that $\ker \Phi\pi = \operatorname{im} \Phi\iota$ from which $(\Phi\pi)(\Phi\varphi) = \mathrm{id}_{\Phi C}$ will show that our short exact sequence splits.

- If $b \in \ker \Phi\pi$, then
$$(\Phi\iota)((\Phi\psi)b) = b$$
by $(*)$, so $b \in \operatorname{im} \Phi\iota$.
- We see $(\Phi\pi)(\Phi\iota) = \Phi(\pi\iota) = \Phi 0 = 0$ because Φ is additive, so $\operatorname{im} \Phi\iota \subseteq \ker \Phi\pi$.

These checks finish. ■

And here are our left-derived functors.

Definition 4.101 (Left-derived functor)**.** Fix an additive right-exact functor $\Phi : \mathrm{Mod}_R \to \mathrm{Mod}_S$ (where R and S are rings) and $i \in \mathbb{N}$ an index. Then, for any R-module M, we build a projective resolution P for M by

$$\cdots \to P_2 \to P_1 \to P_0 \to M \to 0.$$

Applying Φ gives us another complex

$$\cdots \to \Phi P_2 \to \Phi P_1 \to \Phi P_0 \to \Phi M \to 0.$$

Then we define the *left-derived functor* $L_i\Phi : \mathrm{Mod}_R \to \mathrm{Mod}_S$ by $L_i\Phi(M) := H_i(\Phi P)$.

We quickly check that ΦP does indeed properly as a complex.

Lemma 4.102. Fix a functor $\Phi : \mathrm{Mod}_R \to \mathrm{Mod}_S$.

- If (P, ∂) is a complex, then $(\Phi P, \Phi\partial)$ is also a complex.
- If $\alpha : (P, \partial^P) \to (Q, \partial^Q)$ is a chain morphism, then $\Phi\alpha : (\Phi P, \partial^{\Phi P}) \to (\Phi Q, \partial^{\Phi Q})$ is also a chain morphism.

Proof. We do our checks separately.

- Expanding out, we see that Φ applied to the complex P produces the complex

$$\cdots \to \Phi P_2 \overset{\Phi\partial_2}{\to} \Phi P_1 \overset{\Phi\partial_1}{\to} \Phi P_0 \overset{\Phi\partial_0}{\to} \cdots .$$

  We can use this labeling to properly make ΦP into a graded module, but we won't bother because this is a formalization of the above sequence anyways. To check that this is a complex, we pick up any index $i \in \mathbb{N}$ and note

$$(\Phi\partial_{i+1})(\Phi\partial_i) = \Phi(\partial_{i+1}\partial_i) = \Phi 0 = 0$$

  by functoriality of Φ.

- On applying Φ to α, here is the diagram we need to commute.

$$\begin{tikzcd}
\cdots \arrow[r] & \Phi P_{i-1} \arrow[r, "\Phi\partial^P_{i-1}"] \arrow[d, "\Phi\alpha_{i-1}"'] & \Phi P_i \arrow[r, "\Phi\partial^P_i"] \arrow[d, "\Phi\alpha_i"] & \Phi P_{i+1} \arrow[r] \arrow[d, "\Phi\alpha_{i+1}"] & \cdots \\
\cdots \arrow[r] & \Phi Q_{i-1} \arrow[r, "\Phi\partial^Q_{i-1}"'] & \Phi Q_i \arrow[r, "\Phi\partial^Q_{i+1}"'] & \Phi Q_{i+1} \arrow[r] & \cdots
\end{tikzcd}$$

  In particular, for $\Phi\alpha$ to be a chain morphism, we note that $\alpha\partial^P = \partial^Q\alpha$ because α is a chain morphism, so

$$(\Phi\alpha)\partial^{\Phi P} = (\Phi\alpha)\left(\Phi\partial^P\right) = \Phi\left(\alpha\partial^P\right) = \Phi\left(\partial^Q\alpha\right) = \left(\Phi\partial^Q\right)(\Phi\alpha) = \partial^{\Phi Q}(\Phi\alpha)$$

  by repeatedly using the functoriality of Φ. This finishes. ■

Remark 4.103. A few more checks would show that Φ induces a functor from the category of complexes over R to the category of complexes over S.

However, the bigger concern with Definition 4.101 is that it looks like it depends on our choice of projective resolution for M. Thankfully, Lemma 4.94 assures us that it does not.

Lemma 4.104. Fix an additive right-exact functor $\Phi : \mathrm{Mod}_R \to \mathrm{Mod}_S$. Then the left-derived functor $L_i\Phi$ is well-defined, up to isomorphism. Namely, $L_i\Phi(M)$ does not depend on the chosen projective resolution of M.

Proof. Pick up two augmented projective resolutions for M denoted $P := \overline{P} \to M$ and $Q := \overline{Q} \to M$. The main point is to use Lemma 4.92 to induce isomorphisms of the homology modules of ΦP and ΦQ. Writing this all out takes some words.

By Lemma 4.92, we are promised chain morphisms $\alpha : P \to Q$ and $\beta : Q \to P$ such that

$$\beta\alpha \sim \mathrm{id}_P \qquad \text{and} \qquad \alpha\beta \sim \mathrm{id}_Q .$$

Namely, there is a degree-1 morphisms $g : P \to P$ and $h : Q \to Q$ such that

$$\alpha\alpha - \mathrm{id}_P = h\partial^Q + \partial^Q h \qquad \text{and} \qquad \alpha\beta - \mathrm{id}_Q = g\partial^P + \partial^P g.$$

Applying Φ, functoriality and additivity tells us that

$$(\Phi\beta)(\Phi\alpha) - \mathrm{id}_{\Phi P} = (\Phi h)\partial^{\Phi P} + \partial^{\Phi P}(\Phi h) \qquad \text{and} \qquad (\Phi\alpha)(\Phi\beta) - \mathrm{id}_{\Phi Q} = (\Phi g)\partial^{\Phi Q} + \partial^{\Phi Q}(\Phi g).$$

In particular, the differentials of ΦP and Φ^Q are $\Phi\partial^P$ and $\Phi\partial^Q$, respectively, and $\Phi\alpha$ and $\Phi\beta$ are chain morphisms by Lemma 4.102. It follows that

$$(\Phi\beta)(\Phi\alpha) \sim \mathrm{id}_{\Phi P} \qquad \text{and} \qquad (\Phi\alpha)(\Phi\beta) \sim \mathrm{id}_{\Phi Q} .$$

Now, Lemma 4.75 promises us induced morphisms $H_i(\Phi\alpha) : (\Phi P)_i \to (\Phi Q)_i$ and $H_i(\Phi\beta) : (\Phi Q)_i \to (\Phi P)_i$, from which Lemma 4.76 gives

$$H_i(\Phi\beta)H_i(\Phi\alpha) = H_i(\Phi(\beta\alpha)) \stackrel{*}{=} H_i(\mathrm{id}_{\Phi Q}) = \mathrm{id}_{H_i(\Phi Q)},$$

where we have used Proposition 4.81 in $\stackrel{*}{=}$. Similarly,

$$H_i(\Phi\alpha)H_i(\Phi\beta) = H_i(\Phi(\alpha\beta)) = H_i(\mathrm{id}_{\Phi P}) = \mathrm{id}_{H_i(\Phi P)},$$

where we have again used Proposition 4.81 in $\stackrel{*}{=}$. Thus, $H_i(\Phi\alpha) : H_i(\Phi P) \to H_i(\Phi Q)$ is an isomorphism with inverse $H_i(\Phi\beta)$.

Now, $L_i\Phi(M) = H_i(\Phi P)$ at all indices except $i = 0$ (recall that P is the augmented projective resolution), so we so far know that $L_i\Phi(M)$ is well-defined away from $i = 0$. To fix this, we pick up the following lemma.

Lemma 4.105. Fix $\Phi : \mathrm{Mod}_R \to \mathrm{Mod}_S$ a right-exact functor. We have that $L_0\Phi(M) \cong \Phi M$.

Proof. For the first time, we use the fact that Φ is right-exact. Give M any projective resolution (P, ∂) so that our resolution starts as the exact sequence

$$P_1 \stackrel{\partial_1}{\to} P_0 \stackrel{\varepsilon}{\to} M \to 0.$$

Because Φ is right-exact, we get an exact sequence

$$\Phi P_1 \stackrel{\Phi\partial_1}{\to} \Phi P_0 \stackrel{\Phi\varepsilon}{\to} \Phi M \to 0.$$

Thus, $\Phi\varepsilon$ induces an isomorphism

$$\Phi M \cong \frac{\Phi P_0}{\operatorname{im} \Phi\partial_1} = \frac{\ker \Phi\partial_0}{\operatorname{im} \Phi\partial_1} = H_0(\Phi P) = L_0\Phi(M),$$

which is what we wanted. ■

Remark 4.106 (Nir). The above lemma is why the definition of a projective resolution does not take $P_{-1} = M$ automatically.

It follows that $L_0\Phi(M)$ is in fact well-defined as ΦM. This finishes. ■

Notation 4.107. Because $L_i\Phi$ is only well-defined up to isomorphism, we will simply define $L_0\Phi(M) := \Phi M$, for psychological reasons.

4.3.5 Properties of Left-Derived Functors

We take a moment to list some nice properties of left-derived functors. To start off these are actually functors.

Lemma 4.108. Fix an additive right-exact functor $\Phi : \mathrm{Mod}_R \to \mathrm{Mod}_S$ and an R-module homomorphism $\varphi : M \to N$. Given any index $i \in \mathbb{N}$, we can exhibit an S-module morphism $L_i\Phi(\varphi) : L_i\Phi(M) \to L_i(\Phi N)$ satisfying the following functoriality conditions.

- For R-modules A, B, C with morphisms $\alpha : A \to B$ and $\beta : B \to C$, we have $L_i\Phi(\beta)L_i(\alpha) = L_i\Phi(\beta\alpha)$.
- For an R-module M, we have $L_i\Phi(\mathrm{id}_M) = \mathrm{id}_{L_i\Phi(M)}$.

Proof. We simply plug into Lemma 4.76. Fix an R-module homomorphism $\varphi : M \to N$, and we give M and N the projective resolutions $\left(P, \partial^P\right)$ and $\left(Q, \partial^Q\right)$, respectively. Note that Lemma 4.93 then grants us an extension of $\varphi : M \to N$ to a full chain morphism $\varphi : P \to Q$. Pushing through Lemma 4.102 grants us a chain morphism $\Phi\varphi : \Phi P \to \Phi Q$, from which Lemma 4.75 turns into a morphism

$$H_i(\Phi\varphi) : H_i(\Phi P) \to H_i(\Phi Q).$$

As such, we set $L_i\Phi(\varphi) := H_i(\Phi\varphi)$.

Checking through the above construction, we see that all steps are well-defined except for extending the morphism $\varphi : M \to N$ to a chain morphism $\varphi : P \to Q$. However, this is okay: if $\alpha, \beta : P \to Q$ are chain morphisms extending φ so that $\alpha_{-1} = \beta_{-1} = \varphi$, Lemma 4.94 implies

$$\alpha \sim \beta.$$

So Proposition 4.81 tells us $H_i(\Phi\alpha) = H_i(\Phi\beta)$, so our induced morphism $L_i\Phi(\varphi)$ is well-defined.

We now run our functoriality checks.

- We work in the context of the statement. As discussed above, extend $\alpha : A \to B$ and $\beta : B \to C$ to any chain morphism of projective resolutions. From Lemma 4.76, we see that

$$L_i\Phi(\beta)L_i\Phi(\alpha) = H_i(\Phi\beta)H_i(\Phi\alpha) = H_i(\Phi\beta \circ \Phi\alpha) = H_i(\Phi(\beta\alpha)) = L_i\Phi(\beta\alpha),$$

  where we have also used the functoriality of Φ.

- Fix our module M with projective resolution (P, ∂). Note that id_M can be extended to the chain morphism $\mathrm{id}_P :\to P$, from which Lemma 4.76 tells us that

$$L_i\Phi(\mathrm{id}_M) = H_i(\Phi\,\mathrm{id}_P) = H_i(\mathrm{id}_{\Phi P}) = \mathrm{id}_{H_i(\Phi P)} = \mathrm{id}_{L_i\Phi(M)},$$

  where we have again used the functoriality of Φ.

The above checks finish. ■

Example 4.109. Fix an additive right-exact functor $\Phi : \mathrm{Mod}_R \to \mathrm{Mod}_S$. Then, given an R-module homomorphism $\varphi : M \to N$, we see

$$L_0\Phi(\varphi) = H_0(\Phi\varphi),$$

which is simply $\Phi\varphi$ after tracking $L_i\Phi(M) \cong M$ and $L_i\Phi(N) \cong N$ through with Lemma 4.75.

Remark 4.110 (Nir)**.** Now that we have a functor, we remark that Lemma 4.105 is natural in M: if $\varphi : M \to N$ is an R-module homomorphism, then we claim that the following diagram commutes.

$$\begin{tikzcd} L_0\Phi(M) \arrow[r, "L_0\Phi(\varphi)"] \arrow[d, equal] & L_0\Phi(N) \arrow[d, equal] \\ \Phi M \arrow[r, "\Phi\varphi"'] & \Phi N \end{tikzcd}$$

Indeed, along the top we take $x \in L_0\Phi(M)$ to $H_0(\Phi\varphi)(x) = (\Phi\varphi)(x)$, which is the same as what we get along the bottom.

Here is another computation.

Lemma 4.111. Fix an additive right-exact functor $\Phi : \mathrm{Mod}_R \to \mathrm{Mod}_S$. Then, if P is a projective R-module, then $L_i\Phi(R) = 0$ for $i > 0$.

Proof. We build our projective resolution by hand. Note that the sequence

$$0 \to P \to P \to 0$$

is exact, so we set

$$P_i := \begin{cases} P & i = 0, \\ 0 & i \neq 0, \end{cases}$$

with $\partial = 0$. This makes $\partial^2 = 0$, so (P, ∂) is a complex. Further, we set $\varepsilon = \mathrm{id}_P$ (note $P_0 = P$), so the sequence

$$\cdots \xrightarrow{0} P_2 \xrightarrow{0} P_1 \xrightarrow{0} P_0 \overset{\varepsilon}{=} P \to 0$$

is exact. Indeed, we are exact at each $P_i = 0$ for $i > 0$ because both the kernel and images are 0. We are exact at P_0 because the kernel of the map $\mathrm{id}_P : P_0 \to P$ is 0; we are exact at P because the kernel of the map $P \to 0$ is equal to P, which is the image of $\varepsilon = \mathrm{id}_P$. Thus, P is indeed a projective resolution of P.

Now, we apply Φ, which gives the complex

$$\cdots \to \Phi P_2 \to \Phi P_1 \to \Phi P_0 \to 0.$$

In particular, note that $\Phi 0 = 0$ by Lemma 4.99, so for $i > 0$, we can compute

$$H_i(P \otimes_R N) = \frac{\ker \partial_i}{\operatorname{im} \partial_{i+1}} = \frac{0}{\operatorname{im} \partial_{i+1}} = 0$$

because $\ker \partial_i \subseteq \Phi P_i = \Phi 0 = 0$ for $i > 0$. The result follows ■

Lastly, here is the main result of left-derived functors.

Proposition 4.112. Fix an additive right-exact functor $\Phi : \mathrm{Mod}_R \to \mathrm{Mod}_S$. Suppose

$$0 \to M' \xrightarrow{\iota} M \xrightarrow{\pi} M'' \to 0$$

an exact sequence of R-modules. Then there is a long exact sequence of left-derived functors, given by

$$\begin{tikzcd} \cdots \arrow[r] & L_i\Phi(M') \arrow[r, "L_i\Phi(\iota)"] & L_i\Phi(M) \arrow[r, "L_i\Phi(\pi)"] & L_i\Phi(M'') \arrow[dll, "\delta_i"'] \\ & L_{i-1}\Phi(M') \arrow[r, "L_{i-1}\Phi(\iota)"'] & L_{i-1}\Phi(M) \arrow[r, "L_{i-1}\Phi(\pi)"'] & L_{i-1}\Phi(M'') \arrow[r] & \cdots \end{tikzcd}$$

Proof. Choose any augmented projective resolutions $P' := \overline{P'} \to M'$ and $P'' := \overline{P''} \to M''$ for M' and M''. Then Proposition 4.95 promises us a third augmented projective resolution $P := \overline{P} \to M$ so that we have a short exact sequence

$$0 \to P' \to P \to P'' \to 0$$

of augmented projective resolutions. By deleting everything at index -1 (i.e., replacing this row with 0s across), we obtain a split short exact sequence

$$0 \to \overline{P'} \to \overline{P} \to \overline{P''} \to 0$$

of projective resolutions. Now, because Φ is additive, this will induce a short exact sequence of complexes

$$0 \to \Phi\overline{P'} \to \Phi\overline{P} \to \Phi\overline{P''} \to 0$$

by Lemma 4.100. From here, Theorem 4.82 grants us a long exact sequence as follows.

$$\begin{tikzcd} \cdots \arrow[r] & H_i(\Phi P') \arrow[r, "H_i(\Phi\iota)"] & H_i(\Phi P) \arrow[r, "H_i(\Phi\pi)"] & H_i(\Phi P'') \arrow[dll, "\delta_i"'] \\ & H_i(\Phi P') \arrow[r, "H_{i-1}(\Phi\iota)"'] & H_i(\Phi P) \arrow[r, "H_{i-1}(\Phi\pi)"'] & H_i(\Phi P'') \arrow[r] & \cdots \end{tikzcd}$$

Plugging into the definitions of the functor $L_i\Phi$ finishes. ■

Remark 4.113. The fact that we have extended our short exact sequence

$$\cdots \to \Phi M' \to \Phi M \to \Phi M'' \to M' \to M \to M'' \to 0$$

to the "left" is why these are called left-derived functors.

4.3.6 Uniqueness of Left-Derived Functors

We close our discussion of left-derived functors with a uniqueness result, which we will only sketch. This was not covered in class. We start with a remark.

Remark 4.114. In fact, the δ_i from Proposition 4.112 are natural in the short exact sequence, in the sense that a morphism of short exact sequences labeled

$$\begin{tikzcd} 0 \arrow[r] & M' \arrow[r] \arrow[d, "\varphi'"'] & M \arrow[r] \arrow[d, "\varphi"] & M'' \arrow[r] \arrow[d, "\varphi''"] & 0 \\ 0 \arrow[r] & N' \arrow[r] & N \arrow[r] & N'' \arrow[r] & 0 \end{tikzcd}$$

gives rise to a commutative diagram as follows.

$$\begin{tikzcd} L_i\Phi(M'') \arrow[r, "\delta_i"] \arrow[d, "L_i\Phi(\varphi'')"'] & L_{i-1}\Phi(M') \arrow[d, "L_{i-1}\Phi(\varphi')"] \\ L_i\Phi(N'') \arrow[r, "\delta_i"'] & L_{i-1}\Phi(N'') \end{tikzcd}$$

Checking this commutativity is a matter of unraveling all the definitions; we will not do it here.

In fact, the above properties uniquely determine the functors $L_i\Phi$, in the following sense.

Theorem 4.115. Fix an additive right-exact functor $\Phi : \operatorname{Mod}_R \to \operatorname{Mod}_S$. Then, up to natural isomorphism, there is exactly one family of functors $\{L_i\Phi\}_{i\in\mathbb{N}}$ taking $\operatorname{Mod}_R \to \operatorname{Mod}_S$ satisfying the following.

(a) We have $L_0\Phi$ is naturally isomorphic to Φ.

(b) We have $L_i\Phi(F) = 0$ for any free R-module F and $i > 0$.

(c) For any short exact sequence
$$0 \to M' \stackrel{\iota}{\to} M \stackrel{\pi}{\to} M''$$
of R-modules, there is a long exact sequence
$$\cdots \to L_i\Phi(M') \stackrel{L_i\Phi(\iota)}{\to} L_i\Phi(M) \stackrel{L_i\Phi(\pi)}{\to} L_i\Phi(M'') \stackrel{\delta_i}{\to} L_{i-1}\Phi(M') \stackrel{L_{i-1}\Phi(\iota)}{\to} \cdots$$
such that the δ_i are natural in the short exact sequence.

Proof. We will be brief. We employ dimension-shifting, inducting on i. The fact that $L_0\Phi$ is unique follows from (a).

Now take $i > 0$ and suppose that we have uniquely determined the functor $L_{i-1}\Phi$ up to natural isomorphism. We now pick up any R-module M, and we show that $L_i\Phi$ is unique up to natural isomorphism. Well, by Lemma 4.56, there is a free R-module F and surjection $\pi : F \twoheadrightarrow M$. Setting $K := \ker \pi$, we have a short exact sequence

$$0 \to K \stackrel{\iota}{\to} F \stackrel{\pi}{\to} M \to 0.$$

Using (c), we thus have the exact sequence

$$L_i\Phi(F) \to L_i\Phi(M) \stackrel{\delta_i}{\to} L_{i-1}\Phi(K) \stackrel{L_{i-1}\Phi(\iota)}{\to} L_{i-1}\Phi(F).$$

Because $i > 0$, we see that $L_i\Phi(F) = 0$ by (b), so δ_i is injective. In particular, $L_i\Phi(M)$ is isomorphic to the kernel of $L_{i-1}\Phi(\iota)$. This isomorphism is natural because the δ_i is natural and $L_{i-1}\Phi$ is determined up to natural isomorphism. We will not say more. ■

Remark 4.116. There is an analogous theory for right-derived functors for left-exact functors by simply flipping all the arrows. For example, instead of using projective resolutions, we use injective resolutions. The only technicality is showing that all modules can be embedded into an injective module, which is not easy. We will not say more.

4.3.7 The Functor Tor

After all of our hard work, we are able to define the functor Tor.

Definition 4.117 (Tor)**.** Fix an R-module N. Then the functor $-\otimes_R N : \operatorname{Mod}_R \to \operatorname{Mod}_R$ is an additive right-exact functor, so we define $\operatorname{Tor}_i^R(M,N) := L_i(-\otimes_R N)(M)$.

In practice, what happens is that we take a projective resolution P of M written as

$$\cdots \stackrel{\partial_2}{\to} P_1 \stackrel{\partial_1}{\to} P_0 \stackrel{\partial_0}{\to} 0.$$

Then we apply the functor $-\otimes_R N$ to get

$$\cdots \stackrel{\partial_2\otimes N}{\to} P_1 \otimes_R N \stackrel{\partial_1\otimes N}{\to} P_0 \otimes_R N \stackrel{\partial_0\otimes N}{\to} 0,$$

and $\operatorname{Tor}_i^R(M,N)$ will be the ith homology module of this complex.

Example 4.118. Lemma 4.105 implies that $\operatorname{Tor}_0^R(M,N) = L_0(-\otimes_R N)(M) = M \otimes_R N$.

Remark 4.119. We note that

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

which is symmetric. It is more generally true that $\operatorname{Tor}_i^R(M,N) \simeq \operatorname{Tor}_i^R(N,M)$ for any index $i \in \mathbb{N}$, but we will not use this.

The proof of the above symmetry requires more effort than I would like to exert, but we can give a small case, which is all we will need (and gives a taste of the general case).

Lemma 4.120. Fix two R-modules M and N. Then

$$\operatorname{Tor}_1^R(M,N) \cong \operatorname{Tor}_1^R(N,M).$$

Proof. We will be brief. Fix (augmented) projective resolutions for M and N named (P, ∂^P) and (Q, ∂^Q)

with augmentation maps $P \overset{\varepsilon_M}{M}$ and $Q \overset{\varepsilon_N}{N}$, respectively. The point is to draw the following big diagram.

$$\begin{tikzcd}
 & P_1 \otimes_R Q_0 \arrow[r, "P_1 \otimes \varepsilon_N"] \arrow[d, "\partial_1^P \otimes Q_0"] & P_1 \otimes_R N \arrow[r] \arrow[d, "\partial_1^P \otimes N"] & 0 \\
P_0 \otimes_R Q_1 \arrow[r, "P_0 \otimes \partial_1^Q"] \arrow[d, "\varepsilon_M \otimes Q_1"] & P_0 \otimes_R Q_0 \arrow[r, "P_0 \otimes \varepsilon_N"] \arrow[d, "\varepsilon_M \otimes Q_0"] & P_0 \otimes_R N \arrow[r] \arrow[d, "\varepsilon_M \otimes N"] & 0 \\
M \otimes_R Q_1 \arrow[r, "M \otimes \partial_1^Q"] \arrow[d] & M \otimes_R Q_0 \arrow[r, "M \otimes \varepsilon_N"] \arrow[d] & M \otimes_R N \arrow[r] \arrow[d] & 0 \\
0 & 0 & 0 &
\end{tikzcd}$$

The diagram commutes because $\otimes_R$ is functorial in its entries. Now,

$$\operatorname{Tor}_1^R(M,N) = \frac{\ker(P_0 \otimes N \to M \otimes N)}{\operatorname{im}(P_1 \otimes N \to P_0 \otimes N)} \qquad \text{and} \qquad \operatorname{Tor}_1^R(N,M) = \frac{\ker(M \otimes Q_0 \to M \otimes N)}{\operatorname{im}(M \otimes Q_1 \to M \otimes Q_0)}.$$

As such, we can show that we have a morphism $\operatorname{Tor}_1^R(M,N) \to \operatorname{Tor}_1^R(N,M)$ as

$$(P_0 \otimes \varepsilon_N)(\varepsilon_M \otimes Q_0)^{-1}.$$

This has an inverse morphism defined in the analogous way, so we have an isomorphism. This finishes. ■

Let's continue collecting properties.

Lemma 4.121. Fix an R-module N. Then $\operatorname{Tor}_i^R(-,N)$ is a functor.

Proof. We defined $\operatorname{Tor}_i^R(-,N) = L_i(- \otimes_R N)(-)$, so we are done by Lemma 4.108. ■

Arguably, the following is the "main result" and the reason we've been keeping track of our long exact sequences.

Theorem 4.122. Fix an R-module N If we have a short exact sequence

$$0 \to M' \overset{\iota}{\to} M \overset{\pi}{\to} M'' \to 0,$$

of R-modules, then we have a long exact sequence of Tor, as follows.

$$\begin{tikzcd}
\cdots \arrow[r] & \operatorname{Tor}_i^R(M',N) \arrow[r, "\operatorname{Tor}_i^R(\iota,N)"] & \operatorname{Tor}_i^R(M,N) \arrow[r, "\operatorname{Tor}_i^R(\pi,N)"] & \operatorname{Tor}_i^R(M'',N) \arrow[dll, "\delta_i"'] & \\
 & \operatorname{Tor}_{i-1}^R(M',N) \arrow[r, "\operatorname{Tor}_{i-1}^R(\iota,N)"'] & \operatorname{Tor}_{i-1}^R(M,N) \arrow[r, "\operatorname{Tor}_{i-1}^R(\pi,N)"'] & \operatorname{Tor}_{i-1}^R(M'',N) \arrow[r] & \cdots
\end{tikzcd}$$

Proof. By definition $\operatorname{Tor}_i^R(-,N) := L_i(- \otimes_R N)(-)$, so this is an application of Proposition 4.112. ■

Here are some more basic computations.

Lemma 4.123. If P is a projective R-module, then $\operatorname{Tor}_i^R(P,N) \cong 0$ for all $i > 0$.

Proof. As usual, this follows from plugging in $L_i(- \otimes_R N)(-)$ into Lemma 4.111. ■

Remark 4.124. In fact, if F is a flat module, then $\operatorname{Tor}_i^R(M,F) \cong 0 \cong \operatorname{Tor}_i^R(F,M)$ for all $i > 0$. We will show this shortly.

Remark 4.125. In fact, the above properties more or less characterize Tor, as usual by plugging into the associated result for left-derived functors, namely Theorem 4.115.

4.3.8 Properties of Tor

We continue our fact-collection beyond what immediately falls out of the theory of left-derived functors. For example, Tor is reasonably small.

Lemma 4.126. Fix a Noetherian ring R and finitely generated R-modules M and N. Then, for any index $i \in \mathbb{N}$, the module $\operatorname{Tor}_i^R(M,N)$ is finitely generated.

Proof. The point is to use Remark 4.89. Before continuing, we pick up the following lemma.

Lemma 4.127. Suppose that A and B are finitely generated R-modules. Then $A \otimes_R N$ is also a finitely generated R-module.

Proof. By hypothesis, we are granted $m, n \in \mathbb{N}$ and surjections $\varphi : R^m \twoheadrightarrow A$ and $\psi : R^n \twoheadrightarrow N$. Because tensoring is right-exact and in particular preserves surjections, we see that $\psi : R^n \twoheadrightarrow N$ induces a surjection

$$M \otimes_R R^n \twoheadrightarrow M \otimes_R N$$

by applying $M \otimes_R -$. Further, $\varphi : R^m \twoheadrightarrow M$ induces a surjection

$$R^m \otimes_R R^n \twoheadrightarrow M \otimes_R R^n$$

by applying $- \otimes_R R^n$. But now, we see that

$$R^m \otimes_R R^n \cong (R \otimes_R R^n)^m \cong ((R \otimes_R R)^n)^m \cong R^{nm}$$

is a free R-module of finite rank which can surject onto $M \otimes_R R^n$ and then onto $M \otimes_R N$. ■

Now, Remark 4.89 promises us a free and therefore projective resolution for M notated

$$\cdots \to P_2 \to P_1 \to P_0 \to 0$$

such that all the $P_\bullet$ are finitely generated. Applying $- \otimes_R N$ gives us the complex

$$\cdots \overset{\partial_3 \otimes N}{\to} P_2 \otimes_R N \overset{\partial_2 \otimes N}{\to} P_1 \otimes_R N \overset{\partial_1 \otimes N}{\to} P_0 \otimes_R N \overset{\partial_0 \otimes N}{\to} 0,$$

where each term is finitely generated by the above lemma. Thus, for our fixed index i, we see that $\ker(\partial_i \otimes N)$ is finitely generated (for example, use the fact that finitely generated modules over a Noetherian), so

$$\operatorname{Tor}_i^R(M,N) = \ker(\partial_i \otimes N) / \operatorname{im}(\partial_{i+1} \otimes N)$$

is finitely generated as well, so we are done. ■

We also have a notion of base change, for flat algebras.

Lemma 4.128. Fix a flat R-algebra S as well as R-modules M and N. Then

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

Proof. The point is to build our projective resolution for $S \otimes_R M$ by hand. We need S to be flat in order to preserve homology and exactness. To be explicit, we use Lemma 4.88 to give M a free resolution so that the sequence

$$\cdots \to F_2 \stackrel{\partial_2}{\to} F_1 \stackrel{\partial_1}{\to} F_0 \stackrel{\varepsilon}{\to} M \to 0$$

is an exact sequence. The key trick is that applying $S \otimes_R -$ to this sequence gives the complex

$$\cdots \to S \otimes_R F_2 \stackrel{S\otimes\partial_2}{\to} S \otimes_R F_1 \stackrel{S\otimes\partial_1}{\to} S \otimes_R F_0 \stackrel{\varepsilon}{\to} S \otimes_R M \to 0. \qquad (*)$$

Note that this complex is exact everywhere; more generally, we have the following lemma.

Lemma 4.129. Fix a complex (A,∂) of R-modules and $\Phi : \operatorname{Mod}_R \to \operatorname{Mod}_S$ an exact functor. Then $H_i(\Phi A) \cong \Phi H_i(A)$.

Proof. Because Φ is exact, we note that Φ preserves kernels and cokernels: a morphism $\varphi : A \to B$ gives the exact sequence

$$0 \to \ker\varphi \to A \stackrel{\varphi}{\to} B,$$

which upon applying Φ to will show that $\Phi\ker\varphi \subseteq \Phi A$ is the kernel of the morphism $\Phi\varphi$. Similarly, we have the short exact sequence

$$A \stackrel{\varphi}{\to} B \to \operatorname{coker}\varphi \to 0,$$

so applying Φ will give the short exact sequence

$$\Phi A \stackrel{\Phi\varphi}{\to} \Phi B \to \Phi\operatorname{coker}\varphi \to 0,$$

from which $\Phi\operatorname{coker}\varphi = \operatorname{coker}\Phi\varphi$.[7]

To finish, we note that $H_i(A)$ is the kernel of the map

$$\partial_i : \operatorname{coker}\partial_{i+1} \to A_{i-1}.$$

Thus, $\Phi H_i(A)$ is the kernel of the map

$$\Phi\partial_i : \Phi\operatorname{coker}\partial_{i+1} \to \Phi A_{i-1},$$

but because we know $\Phi\operatorname{coker}\partial_{i+1} = \operatorname{coker}\Phi\partial_{i+1}$, we see that this kernel is also $H_i(\Phi A)$. ■

Lemma 4.130. Fix an exact complex of R-modules (A,∂). Then, given an exact functor $\Phi : \operatorname{Mod}_R \to \operatorname{Mod}_S$, the complex

$$\cdots \to \Phi A_2 \to \Phi A_1 \to \Phi A_0 \to \cdots$$

is an exact complex of S-modules.

Proof. That we have a complex of S-modueles is because Φ is a functor $\operatorname{Mod}_R \to \operatorname{Mod}_S$. Then we simply note that the above lemma tells us that

$$H_i(\Phi A) = \Phi H_i(A) = \Phi 0 = 0,$$

where the last equality is by Lemma 4.99. Thus, ΦA is exact everywhere, finishing. ■

[7] We are being intentionally sloppy about these objects being literally equal instead of naturally isomorphic or something because I don't want to write out the naturality squares we have to check.

Thus, $(*)$ shows that

$$\cdots \to S\otimes_R F_2 \stackrel{S\otimes\partial_2}{\to} S\otimes_R F_1 \stackrel{S\otimes\partial_1}{\to} S\otimes_R F_0 \stackrel{S\otimes\varepsilon}{\to} S\otimes_R M \to 0$$

is a(n augmented) resolution for $S\otimes_R M$. In fact, because $S\otimes_R R^{\oplus X}\cong (S\otimes_R)^{\oplus X}\cong S^{\oplus X}$ is a free S-module for any free R-module $R^{\oplus X}$, we conclude that we in fact have a free resolution for $S\otimes_R M$.

For our homology computation, we will also want to create the module $S\otimes_R \operatorname{Tor}_i^R(M,N)$ as a homology module. Well, $S\otimes_R -$ is an exact functor, so we note that

$$S\otimes_R H_i(F_\bullet\otimes_R N)\cong H_i(S\otimes_R (F_\bullet\otimes_R N)).$$

However, by Proposition 2.101, we see that $S\otimes_R (F_\bullet\otimes_R N)\cong (S\otimes_R F_\bullet)\otimes_S (S\otimes_R N)$, and in fact this isomorphism is functorial (which we can track through via Remark 2.102), so it follows

$$H_i(S\otimes_R (F_\bullet\otimes_R N))\cong H_i((S\otimes_R F_\bullet)\otimes_S (S\otimes_R N)).$$

So to finish, we note that this last homology comes from the complex that we get after applying $-\otimes_S (S\otimes_R N)$ to the projective resolution for $S\otimes_R M$. In particular, it is $\operatorname{Tor}_i^S(S\otimes_R M, S\otimes_R N)$, so we are done. ■

We close with an example computation for Tor.

Exercise 4.131. Fix $a\in R$ an element which is not a zero-divisor. Further, fix M an R-module. Then we compute $\operatorname{Tor}_i^R(R/(a),M)$ as

$$\operatorname{Tor}_i^R(R/(a),M)\cong\begin{cases} M/aM & i=0,\\ \{m\in M: am=0\} & i=1,\\ 0 & i\ge 2.\end{cases}$$

Proof. The main point is to construct a projective resolution for $R/(a)$. Namely, we claim that the sequence

$$\cdots\to 0\to 0\to R\stackrel{a}{\to} R\to R/(a)\to 0$$

is exact and therefore provides an augmented resolution for $R/(a)$. We have the following checks.

- We are exact at all 0s for free.
- Exactness at the first R follows because the map $R\stackrel{a}{\to} R$ is injective. This is because a is not a zero-divisor: if $x\in R$ is in the kernel, then $ax=0$, so $x=0$. Thus, the kernel is indeed trivial.
- Exactness at the second R is because $x\in R$ goes to 0 under $R\twoheadrightarrow R/(a)$ if and only if $x\in(a)$ if and only if there exists $y\in R$ such that $x=ay$.
- Lastly, we are exact at $R/(a)$ because the map $R\twoheadrightarrow R/(a)$ is surjective.

Now, tensoring our projective resolution M, we get the complex

$$\cdots\to 0\to 0\to R\otimes_R M\stackrel{a}{\to} R\otimes_R M\to 0.$$

Tracking the isomorphism $R\otimes_R M\cong M$ through, we see that $R\otimes_R M\stackrel{a}{\to} R\otimes_R M$ becomes $m\mapsto 1\otimes m\mapsto a\otimes m\mapsto am$, which is $M\stackrel{a}{\to} M$. So our complex is

$$\cdots\to 0\to 0\to M\stackrel{a}{\to} M\to 0.$$

We now run our homology computation. For $i>2$, we see that we have $\operatorname{Tor}_i^R(M,N)=0$ immediately. It remains to compute $i=0$ and $i=1$.

- We see $\operatorname{Tor}_0^R(R/(a),M)$ is the kernel of $M\to 0$ (which is all of M) modded out by the image of $M\stackrel{a}{\to} M$ (which is aM). So we have M/aM here.

- We see $\operatorname{Tor}_1^R(R/(a), M)$ is the kernel of $M \xrightarrow{a} M$ modded out by the image of $0 \to M$ (which is 0). So we have $\{m \in M : am = 0\}$ in this case.

The above computation finishes. ■

Remark 4.132 (Nir)**.** The fact that $\operatorname{Tor}_1^R(R/(a), M) = \{m \in M : am = 0\}$ is the a-torsion of M explains the name Tor: we are detecting torsion.

4.3.9 Flatness via Tor

Here is our main result for today.

Theorem 4.133. Fix an R-module M. The following are equivalent.

(a) M is flat.

(b) $\operatorname{Tor}_1^R(N, M) = 0$ for any R-module N.

(c) $\operatorname{Tor}_i^R(N, M) = 0$ for any R-module N and index $i > 0$.

Proof. We show our implications one at a time; we start by showing that (a) and (b) are equivalent.

- We show that (a) implies (b). Fix any R-module N. Then Lemma 4.56 gives us some free module F with a projection $\pi : F \twoheadrightarrow N$, and we build the short exact sequence

$$0 \to K \xrightarrow{\iota} F \xrightarrow{\pi} N \to 0$$

where $K := \ker \pi$. Applying Theorem 4.122, we get the exact sequence

$$\operatorname{Tor}_1^R(F, M) \to \operatorname{Tor}_1^R(N, M) \to \operatorname{Tor}_0^R(K, M) \to \operatorname{Tor}_0^R(F, M).$$

However, $\operatorname{Tor}_1^R(F, M) = 0$ by Lemma 4.123, so upon plugging into Remark 4.110, we can set up the following diagram.

$$\begin{tikzcd}
0 \arrow[r] & \operatorname{Tor}_1^R(N, M) \arrow[r] \arrow[d, dashed] & \operatorname{Tor}_0^R(K, M) \arrow[r] \arrow[d, equal] & \operatorname{Tor}_0^R(F, M) \arrow[d, equal] \\
0 \arrow[r] & \ker(\iota \otimes M) \arrow[r] & K \otimes_R M \arrow[r, "\iota\otimes M"'] & F \otimes_R M
\end{tikzcd}$$

Here, the top row is exact by our discussion of the Tor exact sequence, and the bottom row is exact by how kernels work. The right square commutes by Remark 4.110, so we have an induced isomorphism $\operatorname{Tor}_1^R(N, M) \cong \ker(\iota \otimes M)$. So to finish, we note that M is flat, so $\iota \otimes M$ is injective, so $\operatorname{Tor}_1^R(N, M) \cong \ker(\iota \otimes M) = 0$.

- We show that (b) implies (a). Suppose that we have a short exact sequence

$$0 \to N' \xrightarrow{\iota} N \xrightarrow{\pi} N'' \to 0.$$

Using Theorem 4.122, this gives an exact sequence

$$\operatorname{Tor}_1^R(N'', M) \to \operatorname{Tor}_0^R(N', M) \to \operatorname{Tor}_0^R(N, M) \to \operatorname{Tor}(N'', M) \to 0.$$

But by hypothesis, $\operatorname{Tor}_1^R(N'', M) = 0$, so plugging into Remark 4.110 gives us the short exact sequence

$$0 \to N' \otimes_R M \xrightarrow{\iota\otimes M} N \otimes_R M \xrightarrow{\pi\otimes M} N'' \otimes_R M \to 0,$$

which is what we wanted.

Lastly, we deal with (c).

- Note that (c) implies (b) by setting $i = 1$.
- We show that (a) implies (c). For this, we build a projective resolution for N as

$$\cdots \to P_2 \to P_1 \to P_0 \to 0.$$

Because M is flat, we know that $- \otimes_R M$ is an exact functor, so Lemma 4.129 promises us that

$$\cdots \to P_2 \otimes_R M \to P_1 \otimes_R M \to P_0 \otimes_R M \to 0$$

will have the same homology modules. That is, we see that

$$\operatorname{Tor}_i^R(N, M) = H_i(P \otimes_R M) = H_i(P) \otimes_R M,$$

so in particular $i > 0$ will have $H_i(P) \otimes_M R = 0 \otimes_R M = 0$. This finishes.

The above implications finish the proof. ■

We can even go in the other direction of having vanishing Tor.

Theorem 4.134. Fix an R-module M. The following are equivalent.

(a) M is flat.

(b) $\operatorname{Tor}_1^R(M, N) = 0$ for any R-module N.

(c) $\operatorname{Tor}_i^R(M, N) = 0$ for any R-module N and index $i > 0$.

Proof. By Theorem 4.133, we see that (a) is equivalent to $\operatorname{Tor}_1^R(N, M) = 0$ for any R-module N, but by Lemma 4.120, $\operatorname{Tor}_1^R(M, N) \cong \operatorname{Tor}_1^R(N, M)$ for any R-module N, so (a) is in fact equivalent to (b).

It remains to deal with (c). Of course, (c) implies (b) by setting $i = 1$, so the hard part is in getting a reverse implication to (c). We claim that (a) implies (c). For this, we have the following lemma.

Lemma 4.135. Fix a short exact sequence

$$0 \to K \to F \to M \to 0$$

of R-modules such that both F and M are flat. Then K is also flat.

Proof. Label our short exact sequence as

$$0 \to K \xrightarrow{\iota} F \xrightarrow{\pi} M \to 0.$$

By Remark 2.46, it suffices to pick up an embedding $\varphi : A \hookrightarrow B$ and show that $\varphi \otimes K : A \otimes_R K \to B \otimes_R K$ is also injective. For this, we draw the following diagram.

$$\begin{tikzcd}
A \otimes_R K \arrow[r, "A\otimes\iota"] \arrow[d, dashed, "\varphi\otimes K"] & A \otimes_R F \arrow[d, dashed, "\varphi\otimes F"] \\
B \otimes_R K \arrow[r, "B\otimes\iota"'] & B \otimes_R F
\end{tikzcd}$$

Quickly, the diagram commutes: along the top we take $a \otimes k$ to $a \otimes \iota k$ to $\varphi a \otimes \iota k$; along the bottom we take $a \otimes k$ to $\varphi a \otimes k$ to $\varphi a \otimes \iota k$, which is the same.

We need to show that the left arrow is injective; we will show this by showing that all the other arrows are injective.

- Note that $\varphi \otimes F$ is injective because F is flat.
- For the horizontal arrows, we let $X \in \{A, B\}$ and note that Theorem 4.122 gives us an exact sequence

$$\operatorname{Tor}_1^R(M, X) \to \operatorname{Tor}_0^R(K, X) \to \operatorname{Tor}_0^R(F, X).$$

  We already know that M being flat forces $\operatorname{Tor}_1^R(M, X) = 0$, so the map $\operatorname{Tor}_0^R(K, X) \to \operatorname{Tor}_0^R(F, X)$ is injective. Further, by Remark 4.110, we see that this map is exactly $X \otimes \iota : X \otimes_R K \to X \otimes_R F$ (after noting that $\otimes$ commutes), which is now also injective.

Thus, we see that all the arrows in our diagram are injective except for $\varphi \otimes K$. To conclude that $\varphi \otimes K$ is injective, we note that any element of its kernel will also live in the kernel of the diagonal map

$$(B \otimes \iota)(\varphi \otimes K) = \varphi \otimes \iota = (\varphi \otimes K)(A \otimes \iota),$$

but the right-hand map is the composite of injective maps and is therefore injective. Thus, the kernel of $\varphi \otimes K$ is trivial. ■

We will now show that (a) implies (c) by dimension-shifting. In particular, we claim that all free modules M have $\operatorname{Tor}_i^R(M, N) = 0$ for any R-module N and index $i \geq 1$ by induction on i; for $i = 1$, this is the implication of (a) implies (b).

For the inductive step, we fix $i > 1$ and note that Lemma 4.56 gives us a free module F with a projection $\pi : F \twoheadrightarrow M$. Setting $K := \ker \pi$, we have a short exact sequence

$$0 \to K \to F \xrightarrow{\pi} M \to 0.$$

Now, M is flat by hypothesis, and F is flat because it is free (e.g., Example 2.48), so K is flat by Lemma 4.135. In particular, the inductive hypothesis tells us that $\operatorname{Tor}_{i-1}^R(K, N) = 0$, so we use Theorem 4.122 to get an exact sequence

$$\operatorname{Tor}_i^R(F, N) \to \operatorname{Tor}_i^R(M, N) \to \operatorname{Tor}_{i-1}^R(K, N).$$

We just remarked that $\operatorname{Tor}_{i-1}^R(K, N) = 0$, and $\operatorname{Tor}_i^R(F, N) = 0$ because F is free, using Lemma 4.123. Thus, exactness forces $\operatorname{Tor}_i^R(M, N) = 0$. This finishes. ■

Here is an example of testing Tor_1.

> **Lemma 4.136.** Fix a ring R a ring, an ideal $I \subseteq R$, and an R-module M. We show that $\operatorname{Tor}_1^R(R/I, M)$ vanishes if and only if the (natural) map $I \otimes_R M \to M$ is injective.

Proof. The point is to begin with the short exact sequence

$$0 \to I \xrightarrow{\iota} R \to R/I \to 0.$$

Writing the long exact sequence for $\operatorname{Tor}_\bullet^R(M, -)$ (via Theorem 4.122), we get

$$\underbrace{\operatorname{Tor}_1^R(R, M)}_{0} \to \operatorname{Tor}_1^R(R/I, M) \to \underbrace{\operatorname{Tor}_0^R(I, M)}_{I \otimes_R M} \to \underbrace{\operatorname{Tor}_0^R(R, M)}_{R \otimes_R M}.$$

By Lemma 4.123, we see that $\operatorname{Tor}_1^R(R, M) = 0$. Then using Remark 4.110, we can build the following diagram.

$$\begin{tikzcd} 0 \arrow[r] & \operatorname{Tor}_1^R(R/I, M) \arrow[r] \arrow[d, dashed] & \operatorname{Tor}_0^R(I, M) \arrow[r] \arrow[d, equal] & \operatorname{Tor}_0^R(R, M) \arrow[d, equal] \\ 0 \arrow[r] & \ker(\iota \otimes M) \arrow[r] & I \otimes_R M \arrow[r, "\iota \otimes M"'] & R \otimes_R M \end{tikzcd}$$

We know that the right square commutes by Remark 4.110, and the rows are exact as discussed. It follows that we have an induced isomorphism $\operatorname{Tor}_1^R(R/I, M) \cong \ker(\iota \otimes M)$. Further, because $R \otimes_R M \cong M$, we can append this isomorphism (which is notably injective) to $\iota \otimes M$ without changing the kernel, so in fact $\operatorname{Tor}_1^R(R/I, M)$ is isomorphic to the kernel of the natural map

$$I \otimes_R M \to M.$$

Thus, $\operatorname{Tor}_1^R(R/I, M) = 0$ if and only if the map $I \otimes_R M \to M$ is injective. ■

To use this, we have the following result.

Theorem 4.137. An R-module M is flat if and only if $\operatorname{Tor}_1^R(R/I, M) = 0$ for all finitely generated ideals $I \subseteq R$. Equivalently, $\operatorname{Tor}_1^R(R/I, M) = 0$ if and only if the natural map $I \otimes_R M \to M$ is injective.

Proof. We will prove this next class. ■

4.4 March 8

We will finish up homological algebra today by talking more about flatness. We will then shift over to talk about completions.

4.4.1 A Criterion for Flatness

Let's review the following result.

Theorem 4.137. An R-module M is flat if and only if $\operatorname{Tor}_1^R(R/I, M) = 0$ for all finitely generated ideals $I \subseteq R$. Equivalently, $\operatorname{Tor}_1^R(R/I, M) = 0$ if and only if the natural map $I \otimes_R M \to M$ is injective.

Proof. The second statement follows from Lemma 4.136, so the real content is in the first statement. Of course, if M is flat, then any finitely generated R-ideal I makes R/I into an R-module, so $\operatorname{Tor}_1^R(R/I, M) = 0$ by Theorem 4.133.

Thus, we want to show that, if $\operatorname{Tor}_1^R(R/I, M) = 0$ for any finitely generated R-ideal I, then M is flat. We proceed with the following steps. The main point is to use the fact that tensor products use only finite sums.

1. We show $\operatorname{Tor}_1^R(R/I, M) = 0$ for all R-ideals I. By Lemma 4.136, this is equivalent to showing that $I \otimes_R M \to M$ is injective for all R-ideals I. For this, we proceed by contraposition: we claim that if we can find some R-ideal I such that $I \otimes_R M \to M$ has nontrivial kernel, then we can find a finitely generated I such that $I \otimes_R M \to M$ has nontrivial kernel, which is enough by Lemma 4.136.

   Well, if we have a nontrivial element x of the kernel of $\varphi : I \otimes M \to_R M$, then we can write

   $$x = \sum_{i=1}^n x_i \otimes m_i$$

   for some $x_1, \ldots, x_n \in I$ and $m_1, \ldots, m_i \in M$. In particular, we are told that

   $$\varphi(x) = \sum_{i=1}^n x_i m_i = 0$$

   even though $x \neq 0$.

   Now, we set $I' := (x_1, \ldots, x_n)$ and consider the natural map $\varphi' : I' \otimes_R M \to M$; we claim that φ' has nontrivial kernel, which will finish because I' is a finitely generated ideal. Well, we still have

   $$\varphi'\left(\sum_{i=1}^n x_i \otimes m_i\right) = \sum_{i=1}^n x_i m_i = 0,$$

so this element $x' := \sum_i x_i \otimes m_i \in I' \otimes_R M$ still lives in the kernel. But x was nonzero in $I \otimes_R M$, so it will remain nonzero in this restriction: namely, the map $I' \hookrightarrow I$ induces a map $I' \otimes_R M \to I \otimes_R M$ by $r \otimes m \mapsto r \otimes m$, through which we see that

$$x' \mapsto \sum_{i=1}^n x_i \otimes m_i = x.$$

So if $x' = 0$, then $x = 0$, which is false, so we instead see that x' is indeed a nontrivial element of our kernel.

2. We next claim that $\operatorname{Tor}_1^R(N, M) = 0$ for any finitely generated R-module N. We proceed by induction on the number of generators for N. If we use zero generators, then $N = 0$, so $\operatorname{Tor}_1^R(N, M) = \operatorname{Tor}_1^R(0, M) = 0$ by Lemma 4.123.

   Otherwise, suppose that all R-modules generated by n elements have vanishing $\operatorname{Tor}_1^R(-, M)$. Now, we set any R-module $N = (x_1, \ldots, x_{n+1})$ generated by $n+1$ elements, and we fix

   $$N' := (x_1, \ldots, x_n) \subseteq N$$

   to be generated by N' elements. Then any element of N/N' can be written as

   $$\sum_{i=1}^{n+1} r_i x_i + N' = r_{n+1}x_{n+1} + \underbrace{\sum_{i=1}^{n} r_i x_i}_{\in N'} + N' = r_{n+1}x_{n+1},$$

   so N/N' is generated by $x_{n+1} + N'$. In particular, there is a surjection $R \twoheadrightarrow N/N'$ by $1 \mapsto x_{n+1} + N'$, so letting I be the kernel of this map, we have an isomorphism $R/I \cong N/N'$.

   Now, consider the short exact sequence

   $$0 \to N' \to N \to N/N' \to 0.$$

   Applying Theorem 4.122, we get an exact sequence

   $$\operatorname{Tor}_1^R(N', M) \to \operatorname{Tor}_1^R(N, M) \to \operatorname{Tor}_1^R(N/N', M).$$

   To finish, note $\operatorname{Tor}_1^R(N', M) = 0$ by the inductive hypothesis and $\operatorname{Tor}_1^R(N/N', M) = \operatorname{Tor}_1^R(R/I, M) = 0$ by the step above, so $\operatorname{Tor}_1^R(N, M) = 0$ follows by exactness.

3. We claim that, if A and B are finitely generated R-modules equipped with an embedding $\iota : A \hookrightarrow B$, then the induced map

   $$\iota \otimes M : A \otimes_R M \to B \otimes_R M$$

   is still injective.

   The point is that $\operatorname{Tor}_1^R(B/\iota A, M) = 0$. Indeed, because B is finitely generated, there is an integer b with a surjection $R^b \twoheadrightarrow B \twoheadrightarrow B/\iota A$, so $B/\iota A$ is finitely generated, so $\operatorname{Tor}_1^R(B/\iota A, M) = 0$ follows from the previous part.

   But now, we see that we have a short exact sequence

   $$0 \to A \xrightarrow{\iota} B \to B/\iota A \to 0,$$

   which by Theorem 4.122 gives us an exact sequence

   $$\operatorname{Tor}_1^R(B/\iota A, M) \to \operatorname{Tor}_0^R(A, M) \to \operatorname{Tor}_0^R(B, M).$$

   Thus, $\operatorname{Tor}_1^R(B/\iota A, M) = 0$ forces $\operatorname{Tor}_0^R(A, M) \to \operatorname{Tor}_0^R(B, M)$ to be injective, but Remark 4.110 tells us that this map is $\iota \otimes M : A \otimes_R M \to B \otimes_R M$. So we are done.

4. Lastly, we show that M is flat, given the previous step. By Remark 2.46, it suffices to show that any embedding $\iota : A \hookrightarrow B$ induces an injective map $\iota \otimes M : A \otimes_R M \to B \otimes_R M$, so the content is in reducing this condition to the finitely generated case, which is the previous step.

   Well, we proceed by contraposition: suppose that M is not flat so that Remark 2.46 promises us an embedding of R-modules $\iota : A \hookrightarrow B$ such that $\iota \otimes M$ is not injective. This means that we have a nonzero element $x \in A \otimes_R M$, of the form
$$x \coloneqq \sum_{i=1}^{n} a_i \otimes m_i$$
   such that
$$\sum_{i=1}^{n} \iota a_i \otimes m_i = (\iota \otimes M)(x) = 0.$$
   Well, we set $A' \coloneqq (a_1, \ldots, a_n)$ and $B' \coloneqq (\iota a_1, \ldots, \iota a_n)$, which are now both finitely generated. Notably, ι will restrict to a map $\iota' A' \to B'$, where $\operatorname{im} \iota' \subseteq B'$ because any element $\sum_i r_i a_i$ of A' has
$$\iota'\left(\sum_{i=1}^{n} r_i a_i\right) = \sum_{i=1}^{n} r_i \iota'(a_i) \in (\iota a_1, \ldots, \iota a_n) = B'.$$
   We now claim that $\iota' \otimes M$ has nontrivial kernel, which will finish because A' and B' are finitely generated. Namely, consider the element
$$x' \coloneqq \sum_{i=1}^{n} a_i \otimes m_i \in A' \otimes_R M.$$
   Note that $x' \in \ker(\iota' \otimes M)$ because
$$\iota'(x') = \sum_{i=1}^{n} \iota' a_i \otimes m_i = \sum_{i=1}^{n} \iota a_i \otimes m_i = \iota(x) = 0.$$
   Further, we note that $A' \subseteq A$ and $B' \subseteq B$ induces a map $A' \otimes_R B' \to A \otimes_R B$ by $a \otimes b \mapsto a \otimes b$ (i.e., by restricting the identity), upon which the element x' goes to
$$x' = \sum_{i=1}^{n} a_i \otimes m_i \mapsto \sum_{i=1}^{n} a_i \otimes m_i = x,$$
   so $x \neq 0$ forces $x' \neq 0$. So we see that x' is the nontrivial element of our kernel. This finishes. ■

Let's see some examples.

Exercise 4.138. Set $R \coloneqq k[x]/\left(x^2\right)$. We show that an R-module M is flat if and only if
$$M/xM \stackrel{\times x}{\to} M$$
is an isomorphism.

Proof. We use Theorem 4.137. The main point is to classify the possible ideals of R. In particular, we see that any element $a + bx \in R$ such that $a \neq 0$ is a unit because
$$(a+bx) \cdot (a-bx) \cdot a^{-2} = \left(a^2 - b^2x^2\right) \cdot a^{-2} = a^2 \cdot a^{-2} = 1.$$
Thus, everything outside the set $\{bx : b \in k\} = (x)$ is a unit R is local with maximal ideal (x). However, all nonzero elements of (x) generate (x): if $bx \neq 0$, then $b \neq 0$, so $bx \cdot b^{-1} = x$, so
$$(bx) \supseteq (x) \supseteq (bx),$$
giving $(x) = (bx)$. Thus, if we have any proper ideal I, we see that either $I = (0)$ or $I = (x)$.

Thus, our only ideals to check for Theorem 4.137 are (0) and (x) and R.

- For $I = (0)$, we are asking if the natural map
$$(0) \otimes_R M \to M$$
is injective, but $0 \otimes_R M$ is generated by elements of the form $0 \otimes m = 0$, so $(0) \otimes_R M = 0$. Thus, this map is injective for free.
- For $I = R$, we are asking if the natural map
$$R \otimes_R M \to M$$
is injective, but this map is the isomorphism $R \otimes_R M \cong M$ by $r \otimes m \mapsto rm$. Thus, this map is still injective.
- It remains to deal with (x). The main point is that there is an isomorphism $R/(x) \to (x)$, induced by sending $a \mapsto ax$. As such, we see that $(x) \otimes_R M \to M$ is injective if and only if
$$M/xM \cong R/(x) \otimes_R M \overset{\times x}{\cong} (x) \otimes_R M \to M$$
is injective.

Synthesizing, we see that Theorem 4.137 really only has to worry about the last case, so M is flat if and only if
$$M/xM \overset{\times x}{\to} M$$
is injective (from the last case), which is what we wanted. ■

Remark 4.139 (Serganova)**.** In fact, we can show that any R-module M can be written as $M_0 \oplus F$ where $M_0 \cong \ker(x)/\operatorname{im}(x)$ and F is free.

Exercise 4.140. Fix R a principal ideal domain. Then an R-module M is flat if and only if M is torsion-free.

Proof. If M is flat, then M is torsion-free by Lemma 4.64: any non-zero-divisor $a \in R$ must have $am = 0$ imply $m = 0$.

For the reverse direction, we use Theorem 4.137. Suppose that M is torsion-free. Now, we can choose any ideal $I \subseteq R$ to be $I = (a)$ for some $a \in R$ because R is a principal ideal domain. We have two cases.

- If $a = 0$, then we are looking at the natural map
$$0 \otimes_R M \to M.$$
However, $0 \otimes_R M$ is generated by elements of the form $0 \otimes m = 0$, so $0 \otimes_R M = 0$, so this map is the zero map and therefore injective automatically.
- If $a \neq 0$, then because R is a domain, a is a non-zero-divisor. In particular, Exercise 4.131 tells us that
$$\operatorname{Tor}_1^R(R/(a), M) = \{m \in M : am = 0\},$$
but the right-hand side is 0 because M is torsion-free. This finishes this check.

So we see that all cases satisfied the needed conclusion of Theorem 4.137, so M is indeed flat. ■

Example 4.141. If a $\mathbb{Z}$-module M is finitely generated and torsion free, then M must actually be free by the classification of finitely generated abelian groups. Also, $\mathbb{Q}$ is torsion free and hence flat.

4.4.2 Flatness Locally

We note the following.

Lemma 4.142. Fix R a ring and $\mathfrak{p}$ a prime. If M is a flat R-module, then $M_\mathfrak{p}$ is a flat $R_\mathfrak{p}$-module.

Proof. The main point is that $M_\mathfrak{p} \cong R_\mathfrak{p} \otimes_R M$, where M is a flat R-module. Namely, we will show that $R_\mathfrak{p} \otimes M$ is a flat $R_\mathfrak{p}$-module. By Remark 2.46, it suffices to pick up any inclusion $\iota : A \to B$ if $R_\mathfrak{p}$ and show that the induced map

$$\iota \otimes (R_\mathfrak{p} \otimes M) : A \otimes_{R_\mathfrak{p}} (R_\mathfrak{p} \otimes M) \to B \otimes_{R_\mathfrak{p}} (R_\mathfrak{p} \otimes M).$$

Indeed, the key is showing that the following diagram commutes.

$$\begin{tikzcd} (A \otimes_{R_\mathfrak{p}} R_\mathfrak{p}) \otimes_R M \arrow[r, "(\iota\otimes R_\mathfrak{p})\otimes M"] \arrow[d] & (B \otimes_{R_\mathfrak{p}} R_\mathfrak{p}) \otimes_R M \arrow[d] \\ A \otimes_{R_\mathfrak{p}} (R_\mathfrak{p} \otimes_R M) \arrow[r, "\iota\otimes(R_\mathfrak{p}\otimes M)"'] & A \otimes_{R_\mathfrak{p}} (R_\mathfrak{p} \otimes_R M) \end{tikzcd} \qquad (*)$$

The vertical morphisms are the isomorphisms from Proposition 2.100. To see that this diagram commutes, note that along the top we take $(a \otimes r) \otimes m$ to $(\iota a \otimes r) \otimes m$ to $\iota a \otimes (r \otimes m)$. Then along the bottom we take $(a \otimes r) \otimes m$ to $a \otimes (r \otimes m)$ to $\iota a \otimes (r \otimes m)$, which is the same.

Now, the map

$$(\iota \otimes R_\mathfrak{p}) \otimes M : (A \otimes_{R_\mathfrak{p}} R_\mathfrak{p}) \otimes_R M \to (B \otimes_{R_\mathfrak{p}} R_\mathfrak{p}) \otimes_R M$$

is injective as an R-module homomorphism. In particular, it is injective as a function of sets, so it is injective as an $R_\mathfrak{p}$-module homomorphism. Thus, the top arrow of $(*)$ is injective, so the bottom arrow

$$\iota \otimes (R_\mathfrak{p} \otimes M) : A \otimes_{R_\mathfrak{p}} (R_\mathfrak{p} \otimes M) \to B \otimes_{R_\mathfrak{p}} (R_\mathfrak{p} \otimes M)$$

is also injective. This finishes. ■

We might hope the converse holds. Indeed, it does.

Proposition 4.143. Fix R a ring and M an R-module. If $M_\mathfrak{p}$ is a flat $R_\mathfrak{p}$-module for all primes $\mathfrak{p} \subseteq R$, then M is also flat.

Proof. By Remark 2.46, it suffices to fix some inclusion $\iota : A \hookrightarrow B$ so that we want to show that

$$M \otimes \iota : M \otimes_R A \to M \otimes_R B$$

is also an inclusion. By Corollary 2.86, it will be enough to show that $(M \otimes \iota)_\mathfrak{p}$ is injective for all primes $\mathfrak{p} \subseteq R$. For this, we fix any prime $\mathfrak{p}$ and draw the following diagram.

$$\begin{tikzcd} M_\mathfrak{p} \otimes_{R_\mathfrak{p}} A_\mathfrak{p} \arrow[r, "M_\mathfrak{p}\otimes\iota_\mathfrak{p}"] \arrow[d] & M_\mathfrak{p} \otimes_{R_\mathfrak{p}} B_\mathfrak{p} \arrow[d] \\ (M \otimes_R A)_\mathfrak{p} \arrow[r, "(M\otimes\iota)_\mathfrak{p}"'] & (M \otimes_R B)_\mathfrak{p} \end{tikzcd}$$

This diagram commutes by Remark 2.105, and the bottom arrow is $(M \otimes \iota)_\mathfrak{p}$ because this is our induced arrow. Thus, we see that it suffices to show that the top arrow is injective.

Well, $A \hookrightarrow B$ is injective, so Proposition 2.52 tells us that the map $\iota_\mathfrak{p} : A_\mathfrak{p} \hookrightarrow B_\mathfrak{p}$ is injective. But now, $M_\mathfrak{p}$ is a flat $R_\mathfrak{p}$-module, so this causes the map

$$M_\mathfrak{p} \otimes \iota_\mathfrak{p} : M_\mathfrak{p} \otimes_{R_\mathfrak{p}} A_\mathfrak{p} \to M_\mathfrak{p} \otimes_{R_\mathfrak{p}} B_\mathfrak{p}$$

to be injective. This finishes. ■

So we are motivated to study how flat modules behave under localization.

Proposition 4.144. Fix a local ring R with maximal ideal $\mathfrak{p}$. Further, let M be a finitely presented R-module. If M is flat, then M is free.

Proof. The idea is to use Corollary 3.36. For psychological reasons, we will pick up the following lemma, merely because it will make our lives a little easier; it is a surprise tool that will help us later.

Lemma 4.145. Fix a ring R and a short exact sequence

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

of R-modules. If C is finitely presented, and B is finitely generated, then A is also finitely generated.

Proof. The main point is to use the Snake lemma. Because C is finitely presented, we are promised an exact sequence

$$R^m \to R^n \to C \to 0.$$

As such, we lay our two exact sequences on top of each other, as follows.

$$\begin{tikzcd} & R^m \arrow[r] \arrow[d, dashed] & R^n \arrow[r] \arrow[d, dashed] & C \arrow[r] \arrow[d, equal] & 0 \\ 0 \arrow[r] & A \arrow[r] & B \arrow[r] & C \arrow[r] & 0 \end{tikzcd}$$

Because R^n is free and hence projective (by Lemma 4.55, say), we get a map $R^n \to B$ making the right square= commute, and so the diagram will induce a map $R^m \to A$ making the total diagram commute. Now, Lemma 4.83 gives us an exact sequence

$$\ker(C \to C) \to \operatorname{coker}(R^m \to A) \to \operatorname{coker}(R^n \to B) \to \operatorname{coker}(C \to C).$$

Because $C \to C$ is id_C, these terms are zero, so the above is in fact an isomorphism $\operatorname{coker}(R^m \to A) \cong \operatorname{coker}(R^n \to B)$.

As such, we note that B will project onto $\operatorname{coker}(R^n \to B)$; thus, $\operatorname{coker}(R^n \to B)$ and so $\operatorname{coker}(R^m \to A)$ is finitely generated. Further, $\operatorname{im}(R^m \to A)$ is (by definition) projected onto by R^m and therefore finitely generated, so we have the short exact sequence

$$0 \to \operatorname{im}(R^m \to A) \to A \to \operatorname{coker}(R^m \to A) \to 0,$$

where the ends are finitely generated. By building finitely generated free resolutions via Remark 4.89 (e.g., with $R^x \twoheadrightarrow \operatorname{im}(R^m \to A)$ and $R^y \twoheadrightarrow \operatorname{coker}(R^m \to A)$) for either ends, Proposition 4.95 promises us a surjection $R^{x+y} \twoheadrightarrow A$ making the following diagram commute.

$$\begin{tikzcd} 0 \arrow[r] & \operatorname{im}(R^m \to A) \arrow[r] & A \arrow[r] & \operatorname{coker}(R^m \to A) \arrow[r] & 0 \\ 0 \arrow[r] & R^x \arrow[r] \arrow[u] & R^{x+y} \arrow[r] \arrow[u] & R^y \arrow[r] \arrow[u] & 0 \end{tikzcd}$$

So A is in fact finitely generated (the middle arrow is a surjection either by construction or by Lemma 4.83), which is what we wanted. ■

Now, M is finitely generated, so we can find a free module of finite rank R^n with a surjection $\pi_0 : R^n \twoheadrightarrow M$. Of course, n might be too large, so we would like to refine our n; we do this by looking at $M/\mathfrak{p}M$.

In particular, tensoring by $- \otimes_R R/\mathfrak{p}$, we get an induced surjection

$$(R/\mathfrak{p})^n \cong (R \otimes_R R/\mathfrak{p})^n \cong R^n \otimes_R R/\mathfrak{p} \overset{\pi_0}{\twoheadrightarrow} M \otimes_R R/\mathfrak{p} \cong M/\mathfrak{p}M,$$

where the last isomorphism is by Proposition 2.96. This is all to say that $M/\mathfrak{p}M$ is a finite-dimensional $R/\mathfrak{p}$-vector space, so give it a dimension d with basis

$$\{m_1 + \mathfrak{p}M, \ldots, m_d + \mathfrak{p}M\}.$$

In particular, Corollary 3.36 tells us that these elements $\{m_1, \ldots, m_d\}$ will generate M, so we get a surjection

$$\pi : R^d \twoheadrightarrow M$$

by sending the basis vector $e_i \in R^d$ to $\pi : e_i \mapsto m_i$.

We would like to show that $\ker \pi$ is zero. Well, setting $K \coloneqq \ker \pi$, we get a short exact sequence

$$0 \to K \to R^d \to M \to 0,$$

which by Lemma 4.145 forces K to be finitely generated. We will use Nakayama's lemma to get us all the way to $K = 0$. We draw the following diagram.

$$\begin{tikzcd}
\operatorname{Tor}_1^R(M, R/\mathfrak{p}) \arrow[r] & \operatorname{Tor}_0^R(K, R/\mathfrak{p}) \arrow[r] \arrow[d, equal] & \operatorname{Tor}_0^R\left(R^d, R/\mathfrak{p}\right) \arrow[r] \arrow[d, equal] & \operatorname{Tor}_0^R(M, R/\mathfrak{p}) \arrow[r] \arrow[d, equal] & 0 \\
0 \arrow[r] & K \otimes_R R/\mathfrak{p} \arrow[r] \arrow[d] & R^d \otimes_R R/\mathfrak{p} \arrow[r] \arrow[d] & M \otimes_R R/\mathfrak{p} \arrow[r] \arrow[d] & 0 \\
0 \arrow[r] & K/\mathfrak{p}K \arrow[r] & R^d/\mathfrak{p}R^d \arrow[r] & M/\mathfrak{p}M \arrow[r] & 0
\end{tikzcd} \tag{$*$}$$

Note that the top two rows of the diagram commute by Remark 4.110. The bottom two rows of the diagram commute and feature vertical isomorphisms by Remark 2.97.

Additionally, the top row is exact by Theorem 4.122, but we see that $\operatorname{Tor}_1^R(M, R/\mathfrak{p}) \cong \operatorname{Tor}_1^R(R/\mathfrak{p}, M)$ by Lemma 4.120, which is $\operatorname{Tor}_1^R(R/\mathfrak{p}, M) = 0$ by Theorem 4.133, so in fact the top row is short exact, so it follows by the commutativity of the diagram and the fact that all vertical morphisms are isomorphisms that all the rows are exact.

Now, $\dim_{R/\mathfrak{p}} M/\mathfrak{p}M = d$, and $R^d \otimes_R R/\mathfrak{p} \cong (R \otimes_R R/\mathfrak{p})^d \cong (R/\mathfrak{p})^d$ is also of dimension d, so the fact that the map $R^d/\mathfrak{p}R^d \twoheadrightarrow M/\mathfrak{p}M$ is surjective forces this to be an isomorphism. So the exactness of the bottom row of $(*)$ thus forces $K/\mathfrak{p}K = 0$. Because R is local with maximal ideal $\mathfrak{p}$, we conclude that $K = 0$ by Theorem 3.33. This gives $R^d \cong M$, finishing. ■

4.4.3 Flatness and Projectivity

As a consequence of all of our hard work, we get the following lovely result.

> **Theorem 4.146.** Fix a ring R and a finitely presented module M. Then M is flat if and only if M is projective.

Proof. We claim that the following conditions are all equivalent.

(a) M is flat.

(b) $M_\mathfrak{p}$ is flat for all prime ideal $\mathfrak{p} \subseteq R$.

(c) $M_\mathfrak{p}$ is free for all prime ideals $\mathfrak{p} \subseteq R$.

(d) M is projective.

The fact that (a) implies (b) is by Proposition 4.143. The implication (b) to (c) is by Proposition 4.144 because $R_\mathfrak{p}$ is a local ring (with maximal ideal by $\mathfrak{p}R_\mathfrak{p}$), by Proposition 2.15. Then (c) implies (d) by Proposition 4.58. Lastly, (d) implies (a) by Proposition 4.59. ■

Remark 4.147. The above result is amazing: we proved this essentially by looking at the module M locally at all primes, but the final result has nothing to do with localization!

However, the finitely generated condition is necessary.

Exercise 4.148. We show that $\mathbb{Q}$ is a flat but not projective $\mathbb{Z}$-module.

Proof. We will be brief. The $\mathbb{Z}$-module $\mathbb{Q} = \mathbb{Z}_{(0)}$ is flat (by Corollary 2.53), but $\mathbb{Q}$ is not projective. To see this, note that each $q \in \mathbb{Q}$ creates a map $\pi_q : \mathbb{Z} \to \mathbb{Q}$

$$\pi_q : k \mapsto kq.$$

These glue together to create a map $\pi : \mathbb{Z}^{\oplus\mathbb{Q}} \to \mathbb{Q}$, which is surjective because each $x \in \mathbb{Q}$ has

$$\pi\left(\{1_{q=x}\}_{q\in\mathbb{Q}}\right) = \sum_{q\in\mathbb{Q}} \pi_q(1_{q=x}) = \sum_{q\in\mathbb{Q}} 1_{q=x}q = q.$$

However, $\operatorname{Hom}_{\mathbb{Z}}\left(\mathbb{Q}, \mathbb{Z}^{\oplus\mathbb{Q}}\right) = 0$ because the projection onto any coordinate gives a map $\mathbb{Q} \to \mathbb{Z}$, which must be 0: if $\varphi : \mathbb{Q} \to \mathbb{Z}$ is a morphism such that $\varphi(q) = n \neq 0$, then $2n\varphi(q/2n) = \varphi(q) = n$, so $\varphi(q/2n) = 1/2 \notin \mathbb{Z}$, which does not make sense.

Thus, the short exact sequence

$$0 \to \ker\pi \to \mathbb{Z}^{\oplus\mathbb{Q}} \xrightarrow{\pi} \mathbb{Q} \to 0$$

cannot split because the only possible lift for π is 0, which doesn't work. So $\mathbb{Q}$ is not projective by part(b) of Lemma 4.55. ■

THEME 5
COMPLETIONS

Completion is a goal, but we hope it is never the end.

—Sarah Lewis

5.1 March 8

We now shift gears in class to talk about completions.

5.1.1 Completions, Algebraically

We shift gears to talk about completion. The idea is to give a ring a topology by more or less by thinking about a filtration like a fundamental system of neighborhoods around the identity.

Definition 5.1 (Completion, rings)**.** Fix R with a filtration $\mathcal{J}$ given by

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

Then we define the *completion* $\widehat{R}_{\mathcal{J}}$ as a subring of $\prod_{s\in\mathbb{N}} R/I_s$ by

$$\widehat{R}_{\mathcal{J}} = \left\{ (r_0, r_1, \ldots) \in \prod_{s\in\mathbb{N}} R/I_s : r_i \equiv r_j \pmod{I_j} \text{ for } i > j \right\}.$$

Remark 5.2 (Nir)**.** This construction is also denoted

$$\varprojlim_s R/I_s.$$

As usual, the most interesting filtrations for us will be the I-adic filtrations, especially when I is a maximal ideal.

We have the following check.

Lemma 5.3. Fix R with a filtration $\mathcal{J}$. Then $\widehat{R}_{\mathcal{J}}$ is a ring.

Proof. For concreteness, label our filtration $\mathcal{J}$ by

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

The ring structure of $\widehat{R}_{\mathcal{J}}$ is inherited from the product $\prod_{s\in\mathbb{N}} R/\mathfrak{I}_s$, so we merely have to run checks for being a subring.

- We note that the identity element of $\prod_{s\in\mathbb{N}} R/I_s$ is $\{[1]_{I_s}\}_{s\in\mathbb{N}}$. To see that this is in $\widehat{R}_{\mathcal{J}}$, we see that

  $$[1]_{I_n} \equiv [1]_{I_m} \pmod{I_m}$$

  for $n > m$.
- We show closure under addition and multiplication. Indeed, if $\{r_n\}_{n\in\mathbb{N}}, \{s_n\}_{n\in\mathbb{N}} \in \widehat{R}_{\mathcal{J}}$, then the sum is

  $$\{r_n + s_n\}_{n\in\mathbb{N}}$$

  To see that this lives in $\widehat{R}_{\mathcal{J}}$, we see that $n > m$ has $r_s \equiv r_m \pmod{I_m}$ and $s_n \equiv s_m \pmod{I_m}$, so

  $$r_n + s_n \equiv r_m + s_m \pmod{I_m} \qquad r_s s_n \equiv r_m s_m \pmod{I_m},$$

  which finishes.
- We show closure under negation. Indeed, if $\{r_n\}_{n\in\mathbb{N}} \in \widehat{R}_{\mathcal{J}}$, then $r_n \equiv r_m \pmod{I_m}$ for $n > m$, so

  $$-r_n \equiv -r_m \pmod{I_m},$$

  so $\{-r_n\}_{n\in\mathbb{N}}$ lives in $\widehat{R}_{\mathcal{J}}$. This is our negative element in $\prod_{s\in\mathbb{N}} R/I_s$, so we are done.

The above checks show that we have a subring. ■

Let's see some examples.

Exercise 5.4. Fix $R := k[x]$ and $\mathfrak{m} := (x)$ a maximal ideal. We claim $\widehat{R}_{\mathfrak{m}} \cong k[\![x]\!]$.

Proof. We see $\widehat{R}_{\mathfrak{m}}$ consists of sequences of polynomials $\{p_n(x)\}_{n\in\mathbb{N}}$ such that

$$p_n \equiv p_m \pmod{x^m}$$

for $n > m$. To be explicit, we set

$$p_n(x) := \sum_{k=0}^{\infty} a_{n,k} x^k$$

so that we know

$$\sum_{k=0}^{\infty} a_{n,k} x^k = p_n(x) \equiv p_m(x) = \sum_{k=0}^{\infty} a_{m,k} x^k \pmod{x^m}.$$

In particular, we see that are forced to have $a_{n,k} = a_{m,k}$ for $k < m$ because the above equation tells us that x^m divides

$$\sum_{k=0}^{m-1} (a_{n,k} - a_{m,k}) x^k,$$

which can only be possible if all these coefficients vanish by degree arguments.

We are ready to construct our isomorphism $\widehat{R}_{\mathfrak{m}} \cong k[\![x]\!]$: we take the above sequence $\{p_n(x)\}_{n\in\mathbb{N}}$. We set

$$\varphi\left(\{p_n(x)\}_{x\in\mathbb{N}}\right) := \sum_{k=0}^{\infty} a_{k+1,k} x^k.$$

This map is of course well-defined. Our inverse map is

$$\psi\left(\sum_{k=0}^{\infty}a_kx^k\right)=\left\{\sum_{k=0}^{n-1}a_kx^k\right\}_{n\in\mathbb{N}}.$$

We run the following checks.

- We check that ψ is well-defined. Indeed, if $n>m$, then we see

$$\sum_{k=0}^{n-1}a_kx^k\equiv\sum_{k=0}^{m-1}a_kx^k\pmod{x^m},$$

  which is what we need to live $\widehat{R}_{\mathfrak{m}}$.

- We check $\varphi\circ\psi$ is the identity. Indeed, we see that

$$\varphi\left(\psi\left(\sum_{k=0}^{\infty}a_kx^k\right)\right)=\varphi\left(\left\{\sum_{k=0}^{n-1}a_kx^k\right\}_{n\in\mathbb{N}}\right)=\sum_{k=0}^{\infty}a_{k,k+1}x^k,$$

  but $a_{k,k+1}=a_k$ by construction, so we are done.

- We check $\psi\circ\varphi$ is the identity. Indeed, we see that

$$\psi\left(\varphi\left(\left\{\sum_{k=0}^{\infty}a_{n,k}x^k\right\}_{n\in\mathbb{N}}\right)\right)=\psi\left(\sum_{k=0}^{\infty}a_{k+1,k}x^k\right)=\left\{\sum_{k=0}^{n-1}a_{k+1,k}x^k\right\}_{n\in\mathbb{N}}.$$

  To see that this is identity, we need to show that

$$\sum_{k=0}^{\infty}a_{n,k}x^k\equiv\sum_{k=0}^{n-1}a_{k+1,k}x^k\pmod{x^n},$$

  for which we have to show that $a_{n,k}=a_{k+1,k}$ for $k<n$. But by definition of $\widehat{R}_{\mathfrak{m}}$, we see that

$$\sum_{k=0}^{\infty}a_{n,k}x^k\equiv\sum_{k=0}^{\infty}a_{k+1,k}x^k\pmod{x^{k+1}},$$

  so we get the desired result upon comparing the x^k term above.

- We check that ψ preserves addition. This is a matter of force. We write

$$\begin{aligned}\varphi\left(\sum_{k=0}^{\infty}a_kx^k+\sum_{k=0}^{\infty}b_kx^k\right)&=\varphi\left(\sum_{k=0}^{\infty}(a_k+b_k)x^k\right)\\&=\left\{\sum_{k=0}^{n-1}(a_k+b_k)x^k\right\}_{n\in\mathbb{N}}\\&=\left\{\sum_{k=0}^{n-1}a_kx^k\right\}_{n\in\mathbb{N}}+\left\{\sum_{k=0}^{n-1}b_kx^k\right\}_{n\in\mathbb{N}}\\&=\varphi\left(\sum_{k=0}^{\infty}a_kx^k\right)+\varphi\left(\sum_{k=0}^{\infty}b_kx^k\right).\end{aligned}$$

- We check that ψ preserves multiplication. Again, this is a matter of force. We write

$$\begin{aligned}\varphi\left(\sum_{k=0}^{\infty}a_kx^k\cdot\sum_{k=0}^{\infty}b_kx^k\right)&=\varphi\left(\sum_{m=0}^{\infty}\sum_{k+\ell=m}(a_kb_\ell)x^m\right)\\&=\left\{\sum_{m=0}^{n-1}\sum_{k+\ell=m}(a_kb_\ell)x^m\right\}_{n\in\mathbb{N}}\\&=\left\{\sum_{m=0}^{n-1}a_kx^k\cdot\sum_{\ell=0}^{n-1}a_\ell x^\ell\right\}_{n\in\mathbb{N}},\end{aligned}$$

  where in the last equality we have used the fact that the terms of degree at least x^n will vanish in the nth term. Continuing we see

$$\begin{aligned}\varphi\left(\sum_{k=0}^{\infty}a_kx^k\cdot\sum_{k=0}^{\infty}b_kx^k\right)&=\left\{\sum_{k=0}^{n-1}a_kx^k\right\}_{n\in\mathbb{N}}\cdot\left\{\sum_{k=0}^{n-1}b_kx^k\right\}_{n\in\mathbb{N}}\\&=\varphi\left(\sum_{k=0}^{\infty}a_kx^k\right)\varphi\left(\sum_{k=0}^{\infty}b_kx^k\right).\end{aligned}$$

- We check that ψ preserves identities. Well, we note $\psi(1)=\{1\}_{n\in\mathbb{N}}$.

The first three checks shows that ψ is bijective, and the last three checks show that ψ is a homomorphism. So we are done. ■

Example 5.5. Fix $R:=\mathbb{Z}$ with $\mathfrak{m}:=(p)$. Then the ring $\widehat{R}_{\mathfrak{m}}$ is called the p-adic integers, more commonly denoted $\mathbb{Z}_p$. This ring consists of sequences $\{b_n\}_{n\in\mathbb{N}}$ which behave as "formal power series" in p in the following way. Note $b_{n+1}-b_n\equiv 0\pmod{p^n}$, so we can set $a_n:=\frac{b_{n+1}-b_n}{p^n}\in\mathbb{Z}/p\mathbb{Z}$; in particular, we see that

$$b_n=\sum_{k=0}^{n-1}(b_{k+1}-b_k)=\sum_{k=0}^{n-1}a_kp^k.$$

Taking $n\to\infty$ recovers a power series in p.

Example 5.6. The 2-adic integer $u\in\mathbb{Z}_2$ given by

$$u:=1+2+2^2+2^3+\cdots$$

is actually just -1. To be explicit, we set

$$u_n\equiv\sum_{k=0}^{n-1}2^k\pmod{2^n}$$

and consider the sequence $\{u_k\}_{k\in\mathbb{N}}$; notably, $u_n\equiv u_m\pmod{2^m}$ for $n>m$ by simply expanding out u_n and u_m. Now, if we multiply $(1-2)u$, then we see that

$$(1-2)u_n=(1-2)\left(\sum_{k=0}^{n-1}2^k\right)=1-2^n\equiv 1\pmod{2^n}.$$

Thus, $\{(1-2)u_n\}_{n\in\mathbb{N}}=\{1\}_{n\in\mathbb{N}}$, so $(1-2)u=1$. After rearranging, we see that $u=-1$.

5.1.2 Complete Rings

In the previous examples, we might have noticed that there are natural inclusions $k[x] \subseteq k[\![x]\!]$ and $\mathbb{Z} \subseteq \mathbb{Z}_2$. More generally, we have the following.

Lemma 5.7. Fix R a ring and $\mathcal{J}$ a filtration. Then there is a natural map $R \to \widehat{R}_{\mathcal{J}}$ by $r \mapsto \{r\}_{n\in\mathbb{N}}$. If $\mathcal{J}$ is the I-adic filtration for a proper ideal I, and R is local or a domain, then this map is injective.

Proof. For now, denote the filtration $\mathcal{J}$ by

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

Let $\iota : R \to \widehat{R}_{\mathcal{J}}$ by $r \mapsto \{r\}_{n\in\mathbb{N}}$. To see that ι is well-defined, we note that

$$r \equiv r \pmod{I_s}$$

for any ideal I_s in the filtration $\mathcal{J}$, so we are done. To see that ι is a ring homomorphism, note that we have small ring homomorphisms

$$\pi_s : R \twoheadrightarrow R/I_s$$

by $r \mapsto [r]_{I_s}$, which will glue into a larger map

$$\pi : R \to \prod_{s\in\mathbb{N}} R/I_s$$

by $r \mapsto \{r\}_{s\in\mathbb{N}}$. In particular, we see that $\iota = \pi$, and we are promised that π is a ring homomorphism by universal property, so we are done.

Now take I to be a proper ideal and fix $I_s := I^s$ so that $\mathcal{J}$ is the I-adic filtration. We show that ι is injective. Indeed, if $\iota(r) = 0$, then we have that

$$r \equiv 0 \pmod{I^s}$$

for all s. In particular,

$$r \in \bigcap_{s\in\mathbb{N}} I^s.$$

Thus, if R is local or a domain, we see that Corollary 4.43 forces $r = 0$, so indeed, $\ker\iota$ is trivial, making ι injective. ■

Notably, the image of an ideal need not be an ideal; for example, the inclusion $\mathbb{Z} \hookrightarrow \mathbb{Q}$ does not map the ideal $\mathbb{Z} \subseteq \mathbb{Z}$ to an ideal of $\mathbb{Q}$.

The above inclusion gives rise to the following definition, which is our motivation for the word "completion."

Definition 5.8 (Complete)**.** Fix a filtration $\mathcal{J}$ and a ring R. Then the ring R is *complete with respect to* $\mathcal{J}$ if and only if $\widehat{R}_{\mathcal{J}} = R$, in that the natural map $\iota : R \to \widehat{R}_{\mathcal{J}}$ is an isomorphism.

Before actually showing that the completion is complete, we need to talk about which filtration we are complete with respect to.

Notation 5.9. Fix R a ring and $\mathcal{J}$ a filtration. Then, given an ideal $I \subseteq R$ of the filtration $\mathcal{J}$, we let $\widehat{I}$ denote the kernel of the projection map (onto the Ith coordinate) $\widehat{R}_{\mathcal{J}} \twoheadrightarrow R/I$.

Note that $\widehat{R}_{\mathcal{J}} \twoheadrightarrow R$ is indeed surjective because $\iota(r)$ maps to r under this projection.

Remark 5.10. One might wish that we had used the ideal generated by I under the natural map $R \to \widehat{R}_{\mathcal{J}}$ instead. We will show these notions coincide under the I-adic filtration when R is Noetherian later in Proposition 5.33.

Anyways, here is our result.

Proposition 5.11. Fix R a ring and $\mathcal{J}$ a filtration denoted by

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

Then the completion $\widehat{R} := \widehat{R}_{\mathcal{J}}$ is a complete ring with respect to the induced filtration $\widehat{\mathcal{J}}$ given by

$$\widehat{R} = \widehat{I}_0 \supseteq \widehat{I}_1 \supseteq \widehat{I}_2 \supseteq \cdots.$$

Proof. We very quickly check that $n > m$ implies $I_n \subseteq I_m$, so the kernel of $\widehat{R} \to R/I_n$ is smaller than the kernel of $\widehat{R} \to R/I_m$, so $\widehat{I_n} \subseteq \widehat{I_m}$. So indeed, $\widehat{\mathcal{J}}$ is indeed a filtration.

Now, for notational ease, set $S := \widehat{R}$ and $\widehat{S} := \widehat{S}_{\widehat{\mathcal{J}}}$ its completion so that we are showing that the map $\widehat{\iota} : S \to \widehat{S}$ is an isomorphism. We already know that $\widehat{\iota}$ is a ring homomorphism by Lemma 5.7, so it suffices to show that $\widehat{\iota}$ is a bijection.

Well, by definition of $\widehat{I}_s$, we see that

$$\pi_s : \widehat{R}/\widehat{I}_s \to R/I_s$$

by $\{r_n\}_{n\in\mathbb{N}} \mapsto [r_s]_{I_s}$ is an isomorphism. On the other hand, the map $\iota : R \to \widehat{R}/\widehat{I}_s$ takes r to $\{[r]\}_{n\in\mathbb{N}}$. In particular,

$$\pi_s(\iota(r)) = [r]_{I_s},$$

so $I_s \subseteq \ker(\pi_s \circ \iota)$, so $\pi_s \circ \iota$ will induce a map $R/I_s \to R/I_s$ which is the identity. Because π_s is an isomorphism, we see that $\ker \iota$ must be I_s, so we get an induced map $\iota_s : R/I_s \to \widehat{R}/\widehat{I}_s$ which is inverse to π_s and therefore an isomorphism.

We now glue the ι_s together to show $\widehat{\iota}$ is a bijection. Notably, they glue together to give us a bijection

$$\varphi : \prod_{s\in\mathbb{N}} R/I_s \to \prod_{s\in\mathbb{N}} \widehat{R}/\widehat{I}_s$$

by $\varphi : \{[r_s]\}_{s\in\mathbb{N}} \mapsto \{[\iota(r_s)]_{\widehat{I}_s}\}_{s\in\mathbb{N}}$. In particular, restricting to $\widehat{R}$, we see that the nth component comes out to

$$\iota(r_n) \stackrel{*}{\equiv} \{[r_s]\}_{s\in\mathbb{N}} = (\widehat{\iota}(\{[r_s]\}_{s\in\mathbb{N}}))_n \pmod{\widehat{I}_n},$$

where we have to check $\stackrel{*}{\equiv}$ by hand on coordinates: for $m < n$, we have $r_n \equiv r_m \pmod{I_m}$, so $[r_n] = [r_m]$ here. For $m = n$, there is nothing to say, and for $m > n$, we note that $\iota(r_n) - \{[r_s]\}_{s\in\mathbb{N}}$ now has a zero component in the I_n term, so it lives in the kernel of the map $\widehat{R} \to R/I_n$, so we get our equivalence $\pmod{\widehat{I}_n}$.

In particular, the glued map φ is equal to $\widehat{\iota}$. Because φ was injective, it follows that $\widehat{\iota}$ is also injective. We now show that $\widehat{\iota}$ is surjective. Well, given an element of

$$\widehat{S} \subseteq \prod_{s\in\mathbb{N}} \widehat{R}/\widehat{I}_s,$$

we note that it will have exactly one pull-back along φ, and $\varphi|_{\widehat{R}} = \widehat{\iota}$ as shown above, so it suffices to show that this pull-back is an element of $\widehat{R}$.

Well, fix our element $\{\hat{r}_s\}_{s\in\mathbb{N}} \in \widehat{S}$, where $\hat{r}_s = \{r_{s,q}\}_{q\in\mathbb{N}} \in \widehat{R}$. The inverse map of φ is made by gluing together the inverse maps of ι_s, but we know these maps as π_s. Thus,

$$\varphi^{-1}\left(\{\hat{r}_s\}_{s\in\mathbb{N}}\right) = \{\iota_s^{-1}(\hat{r}_s)\}_{s\in\mathbb{N}} = \{\pi_s(\hat{r}_s)\}_{s\in\mathbb{N}} = \{r_{s,s}\}_{s\in\mathbb{N}}$$

To show that this is a well-defined element of $\widehat{R}$, it remains to show that $n > m$ has $r_{n,n} \equiv r_{m,m} \pmod{I_m}$. Well, at the very least we know that

$$\{r_{n,q}\}_{n\in\mathbb{N}} - \{r_{m,q}\}_{m\in\mathbb{N}} \in \widehat{I_m}$$

because $\{\hat{r}_s\}_{s\in\mathbb{N}} \in \widehat{S}$, so we project $\{r_{n,q}\}_{n\in\mathbb{N}} - \{r_{m,q}\}_{m\in\mathbb{N}}$ onto the mth coordinate to be forced to have

$$r_{n,m} \equiv r_{m,m} \pmod{I_m}$$

by definition of $\widehat{I_m}$. However, $r_{n,n} \equiv r_{n,m} \pmod{I_n}$ because $\hat{r}_n \in \widehat{R}$, so we are done. ■

5.1.3 The Krull Topology

Let's have a little fun with our completions.

Warning 5.12. The following two subsections (on the Krull topology and the topological interpretation of completion) are very topological in nature and were not covered in class. They appear in these notes because they are fun.

Definition 5.13 (Krull topology)**.** Fix R a ring and $\mathcal{J}$ a filtration. Then we define the *Krull topology* on R to have a basis consisting of $\varnothing$ as well as the open sets $a + I$ for any $a \in R$ and $I \in \mathcal{J}$.

Here is our key example.

Example 5.14. The standard topology on the p-adic integers $\mathbb{Z}_p$ is the Krull topology induced by the (p)-adic filtration.

We run some checks on this topology.

Lemma 5.15. Fix R a ring and $\mathcal{J}$ a filtration. Then the Krull topology is a topology.

Proof. We merely have to check that the claimed open sets do in fact form a basis for a topology.

- We show that our basis covers R. Fixing any $I \in \mathcal{J}$, we note that

$$\bigcup_{a\in R}(a + I) = R,$$

  so our open sets do cover R.

- We show that our basis is closed under intersection. Fix any two basis elements $a+I$ and $b+J$. Because $\mathcal{J}$ is a filtration, either $I \subseteq J$ or $J \subseteq I$; without loss of generality, take the former case.

  Now, if $b \equiv a \pmod{J}$, then $(a+I) \subseteq (b+J)$ because $I \subseteq J$. So here, we have $(a+I)\cap(b+J) = (a+I)$, implying that we are closed intersection.

  Otherwise, $b \not\equiv a \pmod{J}$, in which case $x \in a + I \subseteq a + J$ implies $x \notin b + J$, so $(a + I) \cap (b + J) = \varnothing$, finishing. ■

Lemma 5.16. Fix R a ring and $\mathcal{J}$ a filtration. Then the Krull topology makes R into a topological ring; i.e., the addition and multiplication maps $R \times R \to R$ are both continuous.

Proof. We run our checks separately.

- We show that the addition map $R \times R \to R$ is continuous. For brevity, name this map $f : R \times R \to R$ by $f(a, b) = a + b$. We need to show that the pre-image of any open set $U \subseteq R$ has $f^{-1}(U) \subseteq R \times R$ still open. Because we have a basis, it suffices to take U to be a basis element.

  If $U = \varnothing$, then $f^{-1}(\varnothing) = \varnothing$, which is open. Otherwise, we are looking at $f^{-1}(x + I)$ for some open set $x + I$. Well,

$$\begin{aligned} f^{-1}(x+I) = \{(a,b) : a+b \in x+I\} &= \bigcup_{(r+I)\in R/I} \{(a,b) : a \in (r+I), b \in ((x-a)+I)\} \\ &= \bigcup_{(r+I)\in R/I} (r+I) \times ((x-r)+I). \end{aligned}$$

  Now, each of the sets $(r + I) \times ((x - r) + I)$ are in fact open in the product topology $R \times R$, so we are done.

- We show that the multiplication map $R \times R \to R$ is continuous. Again, we set $g : R \times R \to R$ by $g(a, b) := ab$ to be our multiplication map. As with last time, it suffices to show that the pre-image of any basis element under g is an open set in $R \times R$.

  If $U = \varnothing$, then $g^{-1}(\varnothing) = \varnothing$, which is open. Otherwise, we are looking at $g^{-1}(x + I)$ for some open set $x + I$. For this, we compute

$$g^{-1}(x+I) = \{(a,b) : ab \in x+I\} = \bigcup_{(r+I),(s+I)\in R/I} \{(a,b) : a \in (r+I).b \in (s+I), ab \in (x+I)\}.$$

  At this point, we see $a \in r + I$ and $b \in s + I$ implies that $ab \in x + I$ if and only if $rs \in x + I$. Thus, we can move this condition outside and write

$$g^{-1}(x+I) = \bigcup_{\substack{(r+I),(s+I)\in R/I \\ rs\in x+I}} \{(a,b) : a \in (r+I), b \in (s+I)\} = \bigcup_{\substack{(r+I),(s+I)\in R/I \\ rs\in x+I}} (r+I) \times (s+I),$$

  which we can see is the union of basis of elements in $R \times R$. ■

Remark 5.17. Fix any $a \in R$. Because the map $x \mapsto (a, x)$ is a continuous map $R \to R \times R$ (it is the product of continuous maps), we see that the composites

$$x \mapsto (a,x) \mapsto a+x \qquad \text{and} \qquad x \mapsto (a,x) \mapsto ax$$

are also both continuous.

The Krull topology need not always be Hausdorff, but it is Hausdorff for many well-behaved rings and filtrations.

Example 5.18. Fix the ring $R := \mathbb{Z} \times \mathbb{Z}$ and the proper ideal $I := (2) \times \mathbb{Z}$, and endow R with the Krull topology induced by the I-adic filtration. We claim that $\{0\}$ is not closed.

Lemma 5.19. Fix a Noetherian ring R and a proper ideal $I \subsetneq R$, and endow R with the Krull topology induced by the I-adic filtration. If R is local or a domain, then R is Hausdorff.

Proof. The point is to use the Krull intersection theorem. Namely, we need to show that the sets $\{a\} \subseteq R$ are closed for any $a \in R$. Well, we note that, by Corollary 4.43, we have

$$R \setminus \{0\} = R \Bigg\backslash \bigcap_{s\geq 0} I^s = \bigcup_{s\geq 0} (R \setminus I^s) = \bigcup_{s\geq 0} \bigcup_{a\notin I^s} (a + I^s).$$

So $R \setminus \{0\}$ is open, thus making $\{0\}$ closed.

To finish, we cop out and use the fact that we live in a topological ring. Fixing any $a \in R$, note that Remark 5.17 tells us that the map $\mu_a : x \mapsto x - a$ is continuous. Thus, because $\{0\}$ is closed, we see that

$$\mu_a^{-1}(\{0\}) = \{a\}$$

is also closed, finishing. ■

So we see that the Krull topology is reasonably nice.

5.1.4 Completions, Topologically

For the discussion that follows, fix a ring R with a filtration $\mathcal{J}$ given by

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

Now, in the example $\mathbb{Z}_p$, we see that we can define

$$d(a,b) := p^{-\max\left\{k \in \mathbb{N} : a-b \in \left(p^k\right)\right\}},$$

which we can check forms a metric on $\mathbb{Z}_p$. In fact, this restricts to a metric on $\mathbb{Z}$, for which $\mathbb{Z}_p$ is the completion. (We will be able to justify this claim shortly.) This is our first hint of that the name "completion" should be a topological notion. In particular, it will turn out that a ring being "complete" with respect to a filtration means that every Cauchy sequence converges to some limit.

To generalize the case of $\mathbb{Z}_p$, we can still fix some $c > 1$ and define the function

$$d(a,b) := c^{-\max\{k \in \mathbb{N} : a-b \in I_k\}},$$

where $a, b \in R$. For our edge case, if $a - b \in I_k$ for arbitrarily large k, then $a - b \in I_k$ for each k, so we might as well set $d(a,b) = 0$.

This edge case, ultimately, is where we are going to have problems: it is possible for the intersection of all the I_k to be nonzero, in which case any element

$$r \in \bigcap_{k \geq 0} I_k$$

would have $d(r, 0) = 0$, so d cannot be a metric. However, this is the only obstruction.

Lemma 5.20. Fix a ring R with a filtration $\mathcal{J}$, notated

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

Further, suppose that $x \in I$ for each $I \in \mathcal{J}$ implies $x = 0$. Then, fixing a real number $c > 1$, the function $d : R^2 \to \mathbb{R}$ defined by

$$d(a,b) := \begin{cases} c^{-\max\{k \in \mathbb{N} : a-b \in I_k\}} & a - b \notin I_n \text{ for some } n, \\ 0 & \text{else}, \end{cases}$$

is a metric on R.

Proof. Observe that the function d is well-defined because $a - b \notin I_k$ for some n implies that $a - b \notin I_m$ for any $m \geq n$ because $I_m \subseteq I_n$, so this means that the set $\{k \in \mathbb{N} : a - b \in I_k\}$ does indeed have a maximum.

We have the following checks on d.

- Identity: fix $a, b \in R$. Note that $d(a,b) = 0$ if and only if $a - b \in I_k$ for each $I_k \in \mathcal{J}$, so $a - b = 0$ by hypothesis on $\mathcal{J}$, so $a = b$. Conversely, if $a = b$, then $a - b \in I_k$ for each k, so $d(a,b) = 0$.

- Symmetry: fix $a, b \in R$. Then $a - b \in I_k$ if and only if $-1(a-b) = b - a \in I_k$, so
$$\{k \in \mathbb{N} : a - b \in I_k\} = \{k \in \mathbb{N} : b - a \in I_k\}.$$
If both of these sets are $\mathbb{N}$, then $d(a,b) = d(b,a) = 0$. Otherwise, these sets have maximums, which must be the same $M \in \mathbb{N}$, so $d(a,b) = c^{-M} = d(b,a)$.
- Triangle inequality: fix $a, b, c \in R$. We need to show that
$$d(a,b) + d(b,c) \geq d(a,c).$$
If $a = b$ or $b = c$, then this inequality collapses to $d(x,y) \geq d(x,y)$.
The point is that if $a - b \in I_k$ and $b - c \in I_\ell$, then $a - c = a - b + b - c \in I_{\min\{k,\ell\}}$. In particular, fix
$$m := \max\{k \in \mathbb{N} : a - b \in I_k\} \qquad \text{and} \qquad n := \max\{\ell \in \mathbb{N} : b - c \in I_\ell\}.$$
Without loss of generality, we take $m \leq n$, which implies that $a - c = (a-b) + (b-c) \in I_m + I_n \subseteq I_m$, so
$$d(a,c) \leq c^{-m} \leq c^{-m} + c^{-n} = d(a,b) + d(b,c).$$
This is what we wanted.

These checks finish showing that d is a metric on R. ■

Continuing with our story, as with $\mathbb{Z}_p$, we see that elements of R are considered "close" if and only if their difference lies in the same "small" open set. In particular, for any $x \in R$ and $r \in \mathbb{R}^+$, some $a \in R$ has
$$\begin{aligned} d(a,x) < r &\iff c^{-\max\{k \in \mathbb{N} : a - x \in I_k\}} < r \\ &\iff -\max\{k \in \mathbb{N} : a - x \in I_k\} < \log_c r \\ &\iff \max\{k \in \mathbb{N} : a - x \in I_k\} > -\log_c r \\ &\iff a - x \in I_k \text{ for some } k > -\log_c r \\ &\iff a \in x + I_{\lceil -\log_c r \rceil}. \end{aligned}$$
Thus, any $r > 0$ will make $\{a \in R : d(a,x) < r\} = x + I_{\lceil -\log_c r \rceil}$ into some open set (where $I_k = R$ for $k < 0$); conversely, any open basis element $x + I_k$ arises in this way by choosing $r = c^{-k}$.

So it looks like our function d correctly induces the Krull topology as a metric. Of course, we need to overcome the Hausdorff obstruction for this to make sense, but we do have the following lemma.

Lemma 5.21. Work in the context of Lemma 5.20. Then the metric topology induced by d is the Krull topology induced by $\mathcal{J}$.

Proof. We get that d is a metric from Lemma 5.20. Further, d induces the Krull topology from the computation above. ■

With all of this set-up, it makes sense to think about the Krull topology as a metric space, which is the context where "completions" actually make topological sense: we want every Cauchy sequence to have a limit. In order to stop talking about topology (and worrying about the Hausdorff condition), we would like to translate these notions back to algebra.

Let's start with limits. An element $a \in R$ is a limit of the sequence $\{a_n\}_{n \in \mathbb{N}} \subseteq R$ (with respect to d) means that
$$\lim_{n \to \infty} d(a, a_n) = 0.$$
By definition of d, this is the same as requiring
$$\lim_{n \to \infty} \max\{k \in \mathbb{N} : a - a_n \in I_k\} = \infty.$$
This means that, for any bound $m \in \mathbb{N}$, there exists some N such that $n > N$ implies $\max\{k \in \mathbb{N} : a - a_n \in I_k\} > m$. However, this last condition is equivalent to $a - a_n \in I_m$ because $\mathcal{J}$ is a filtration. So we have the following definition.

Definition 5.22 (Limit)**.** Fix a ring R with a filtration $\mathcal{J} = \{I_k\}_{k\in\mathbb{N}}$. Then we say that an element $a \in \widehat{R}$ is the *limit* of a sequence $\{a_n\}_{n\in\mathbb{N}}$ if and only if, for each m, there exists N such that $a_n - a \in I_m$ for each $n > N$.

Now let's move to Cauchy sequences. A sequence $\{a_n\}_{n\in\mathbb{N}} \subseteq R$ is Cauchy (with respect to d) if and only if, for any $\varepsilon > 0$, there exists n such that $k, \ell > N$ implies

$$d(a_k, a_\ell) < \varepsilon.$$

By replacing ε with $-\log_c \varepsilon$, this is equivalent to saying that, for any $m \in \mathbb{N}$, there exists N such that $k, \ell > N$ implies

$$\max\{n \in \mathbb{N} : a_k - a_\ell \in I_n\} \geq m,$$

or equivalently, $a_k - a_\ell \in I_m$. So we have the following definition.

Definition 5.23 (Cauchy sequence)**.** Fix a ring R with a filtration $\mathcal{J} = \{I_k\}_{k\in\mathbb{N}}$. Then we say that a sequence $\{a_k\}_{k\in\mathbb{N}}$ is *Cauchy* if and only if, for each m, there exists N such that $a_k - a_\ell \in I_m$ for each $k, \ell > N$.

We are finally able to unite our two notions of completion.

Proposition 5.24. Fix a ring R with a filtration $\mathcal{J}$ such that $x \in I$ for each $I \in \mathcal{J}$ implies $I = 0$. Then $\widehat{R}_{\mathcal{J}}$ is the completion of R with respect to the Krull (metric) topology, where the needed inclusion $R \to \widehat{R}_{\mathcal{J}}$ is the canonical one.

Proof. We already have that R is a metric space from Lemma 5.20. We will construct $\widehat{R}$ as the completion of the metric space for R and then show that $\widehat{R} \cong \widehat{R}_{\mathcal{J}}$ as topological rings.

The completion $\widehat{R}$ consists of equivalence classes of Cauchy sequences of R, where two Cauchy sequences $\{a_n\}_{n\in\mathbb{N}} \sim \{b_n\}_{n\in\mathbb{N}}$ if and only if

$$d(a, b) := \lim_{n\to\infty} d(a_n, b_n) = 0.$$

Very quickly, we let S be the set of Cauchy sequences of R, and we note that we can give $S \subseteq R^{\mathbb{N}}$ a subring structure, with operations given by

$$\{a_n\}_{n\in\mathbb{N}} + \{b_n\}_{n\in\mathbb{N}} := \{a_n + b_n\}_{n\in\mathbb{N}} \qquad \text{and} \qquad \{a_n\}_{n\in\mathbb{N}} \cdot \{b_n\}_{n\in\mathbb{N}} := \{a_n b_n\}_{n\in\mathbb{N}}.$$

We quickly check that S is closed under these operations: for any bound $m \in \mathbb{N}$, there exists N such that $k, \ell > N$ implies $a_k - a_\ell, b_k - b_\ell \in I_m$, so

$$(a_k + b_k) - (a_\ell + b_\ell) \in I_m \qquad \text{and} \qquad a_k b_k - a_\ell b_\ell \in I_m$$

follows. To finish checking that S is a subring, we merely note that $\{1_R\}_{n\in\mathbb{N}}$ is a Cauchy sequence.

Now, $\widehat{R}$ is S modded out by the equivalence relation $\sim$ described above. To make this notion more ring-theoretic, we set

$$I := \{a \in S : a \sim 0\}.$$

In particular $\{a_n\}_{n\in\mathbb{N}} \sim \{b_n\}_{n\in\mathbb{N}}$ if and only if

$$0 = \lim_{n\to\infty} d(a_n, b_n) = \lim_{n\to\infty} d(a_n - b_n, 0)$$

if and only if $\{a_n\}_{n\in\mathbb{N}} - \{b_n\}_{n\in\mathbb{N}} \in I$. Thus, we see that $\widehat{R} = S/I$, as sets. However, we in fact claim that I is an ideal: if $\{a_n\}_{n\in\mathbb{N}}, \{b_n\}_{n\in\mathbb{N}} \in I$ and $\{r_n\}_{n\in\mathbb{N}}, \{s_n\}_{n\in\mathbb{N}} \in S$, then we need to show that

$$\{r_n a_n + s_n b_n\}_{n\in\mathbb{N}} \in I.$$

Well, $d(a_n, 0) \to 0$ and $d(b_n, 0) \to 0$ as $n \to \infty$, so for any m, there exists N such that $n > N$ implies $a_n, b_n \in I_m$, so $r_na_n + s_nb_n \in I_m$. Thus, $d(r_na_n + s_nb_n, 0) \to 0$ as $n \to \infty$.

Thus, we have given $\widehat{R} := S/I$ a ring structure as well as a topology. We claim that $S/I \cong \widehat{R}_J$; it will happen that this is also an isomorphism of topological rings, but we won't check the topological aspects of this isomorphism. We start by defining

$$\varphi : S \to \widehat{R}_J.$$

For this, we take some Cauchy sequence $\{a_n\}_{n\in\mathbb{N}}$. Then, for any index $m \in \mathbb{N}$, there exists N_m such that $k, \ell \geq N_m$ implies $a_k - a_\ell \in I_m$. As such, we define

$$\varphi\left(\{a_n\}_{n\in\mathbb{N}}\right) := \{[a_{N_m}]_{I_m}\}_{n\in\mathbb{N}}.$$

We have the following checks on φ.

- To start, we see that $[a_{N_m}]_{I_m}$ is well-defined: if N'_m is another constant such that $k, \ell \geq N'_m$ implies $a_k - a_\ell \in I_m$, then without loss of generality $N_m \geq N'_m$ so that $a_{N_m} - a_{N'_m} \in I_m$, so $[a_{N_m}]_{I_m} = [a_{N'_m}]_{I_m}$.
- Further, φ does actually output an element of $\widehat{R}_J$. We need to show that $a_{N_{m+1}} \equiv a_{N_m} \pmod{I_m}$ for any $m \in \mathbb{N}$. Well, N_{m+1} satisfies $k, \ell \geq N_{m+1}$ implies $a_k - a_\ell \in I_{m+1} \subseteq I_m$, so the argument from the previous point shows that
$$[a_{N_{m+1}}]_{I_m} = [a_{N_m}]_{I_m},$$
which is what we wanted.
- We show φ is surjective. Well, suppose that we have an element
$$\{[a_m]_{I_m}\} \in \widehat{R}_{\mathcal{J}}.$$
Well, we claim that $\{a_m\}_{m\in\mathbb{N}}$ is itself a Cauchy sequence, which will be our pre-image element. To see that this is a Cauchy sequence, we note that any $m \in \mathbb{N}$ has $k, \ell > m$ has
$$a_k - a_\ell \in I_{\min\{k,\ell\}} \subseteq I_m.$$
In fact, this computation shows that, in our definition of $\varphi(\{a_n\}_{n\in\mathbb{N}})$, we can set $m := N_m$ so that
$$\varphi(\{a_n\}_{n\in\mathbb{N}}) = \{[a_{N_m}]_{I_m}\}_{m\in\mathbb{N}} = \{[a_m]_{I_m}\}_{m\in\mathbb{N}},$$
which is what we wanted.
- We show φ has kernel I. In one direction, if $\{a_n\}_{n\in\mathbb{N}} \in I$, we see that, for any $m \in \mathbb{N}$, there exists N_m for which $a_n \in I_m$ for each $n \geq N_m$. Thus, $k, \ell \geq N_m$ will have $a_k - a_\ell \in I_m$, so we can set
$$\varphi\left(\{a_n\}_{n\in\mathbb{N}}\right) = \{[a_{N_m}]_{I_m}\}_{m\in\mathbb{N}} = \{[0]\}_{m\in\mathbb{N}},$$
which is what we wanted.

  Conversely, suppose that $\{a_n\}_{n\in\mathbb{N}}$ goes to 0 under φ. This means that, for any $m \in \mathbb{N}$, there exists N_m such that $k, \ell \geq N_m$ will have $a_k - a_\ell \in I_m$ and
$$a_{N_m} \in I_m.$$
  In particular, we see that any $k \geq N_m$ will have $a_k \in a_{N_m} + I_m = I_m$. So indeed, $a_n \to 0$ as $n \to \infty$.

The above checks finish showing our isomorphism of rings. We could show that φ is continuous as well (but won't do so here); the third point explicitly constructs our inverse, which we could also show is continuous (but again won't do it here).

We close the proof by remarking that, because the canonical maps $R \to \widehat{R}_{\mathcal{J}}$ and $R \to \widehat{R}$ above both simply take $r \in R$ to the constant sequence $\{[r_n]\}_{n\in\mathbb{N}} \in \widehat{R}_{\mathcal{J}}$ and $\{r_n\}_{n\in\mathbb{N}} + I \in \widehat{R}$ (respectively), we see that the following diagram commutes.

$$\begin{tikzcd} R \arrow[r] \arrow[d, equal] & \widehat{R} \arrow[d, "\varphi"] \\ R \arrow[r] & \widehat{R}_{\mathcal{J}} \end{tikzcd}$$

Indeed, going along the top, we take $r \in R$ to $\{r\}_{n\in\mathbb{N}}$ to $\{[r]\}_{n\in\mathbb{N}}$, which is the same as we get along the bottom. This shows that we can make $\widehat{R}_{\mathcal{J}}$ is not only isomorphic to the metric completion $\widehat{R}$, but in fact, the canonical inclusion $R \to \widehat{R}_{\mathcal{J}}$ is the inclusion needed by the completion. ■

And just for fun, let's unite our notions of complete.

Corollary 5.25. Fix a ring R and a filtration $\mathcal{J} = \{I_k\}_{k\in\mathbb{N}}$ such that $x \in I$ for all $I \in \mathcal{J}$ implies $x = 0$. Then R is complete with respect to the filtration $\mathcal{J}$ if and only if R is complete with respect to the Krull (metric) topology.

Proof. Note R is complete with respect to the Krull (metric) topology if and only if R is homeomorphic to its completion. But by Proposition 5.24, we see that the metric completion of R is $\widehat{R}_{\mathcal{J}}$ with the canonical inclusion $\iota : R \to \widehat{R}_{\mathcal{J}}$.

We already know that ι is injective because $x \in I$ for each $I \in \mathcal{J}$ implies $x = 0$. Thus, the only thing to worry about is that ι is surjective. Well, ι is surjective if and only if ι is an isomorphism of rings (because ι is a priori an injective homomorphism of rings), so R is metrically complete if and only if $\iota : R \to \widehat{R}_{\mathcal{J}}$ is an isomorphism. This finishes. ■

5.1.5 Completions are Local

Taking the completion also tends to look like localization. For example, taking the completion at a maximal ideal will also give a local ring.

Proposition 5.26. Fix a ring R complete with respect to an I-adic filtration. Then any element $1-a$ with $a \in I$ is a unit.

Proof. The point is to rigorize

$$\frac{1}{1-a} = 1 + a + a^2 + \cdots .$$

In particular, we set

$$b_m := \sum_{k=0}^{m-1} a^k$$

so that $(1-a)b_m = 1 - a^m \equiv 1 \pmod{I^m}$. Thus, we would like the "limit" of $\{b_m\}_{m\in\mathbb{N}}$ to be the inverse for $(1-a)$.

Because R is complete, let $\iota : R \to \widehat{R}_{\mathcal{J}}$ be the canonical inclusion, which we know to be an isomorphism. We note that $n \geq m$ implies that

$$b_n = \sum_{k=0}^{n-1} a^k \equiv \sum_{k=0}^{m-1} a^k = b_m \pmod{I^m}$$

because all higher terms of the sum vanish; thus, $\{b_m\}_{m\in\mathbb{N}} \in \widehat{R}_{\mathcal{J}}$. So we may set $b := \iota^{-1}\left(\{[b_m]_{I^m}\}_{m\in\mathbb{N}}\right)$, which will have

$$\iota((1-a)b) = \iota(1-a)\iota(b) = \{[1-a]_{I^m}\}_{m\in\mathbb{N}} \cdot \{[b_m]_{I^m}\}_{m\in\mathbb{N}} = \{[(1-a)b_m]_{I^m}\}_{m\in\mathbb{N}} = \{[1]\}_{m\in\mathbb{N}},$$

so $(1-a)b = 1$ follows because ι is ring isomorphism. ■

Corollary 5.27. Fix R a ring and $\mathfrak{m}$ a maximal ideal. Then $\widehat{R}_{\mathfrak{m}}$ is a local ring with maximal ideal $\widehat{\mathfrak{m}}$.

Proof. It suffices to check that $a \notin \widehat{\mathfrak{m}}$ implies that a is a unit. To start, we note that $a \not\equiv 0 \pmod{\widehat{\mathfrak{m}}}$, so because $\widehat{R}_{\mathfrak{m}}/\widehat{\mathfrak{m}} \cong R/\mathfrak{m}$ is a field, there exists $b \in \widehat{R}_{\mathfrak{m}}$ such that

$$ab \equiv 1 \pmod{\widehat{\mathfrak{m}}}.$$

In particular, $ab - 1 \equiv 0 \pmod{\widehat{\mathfrak{m}}}$, so $ab - 1 \in \widehat{\widehat{\mathfrak{m}}}$. Thus, we set $-c := ab - 1 \in \widehat{\mathfrak{m}}$ so that $c \in \widehat{\mathfrak{m}}$ and $ab = 1 - c$.

Now, we note from Proposition 5.11 that $\widehat{R}_{\mathfrak{m}}$ is complete with respect to the $\widehat{\mathfrak{m}}$-adic filtration, so Proposition 5.26 tells us that $1 - c$ is a unit in $\widehat{R}_{\mathfrak{m}}$. Thus, we find our d such that $(1 - c)d = 1$, so

$$a(bd) = (ab)d = (1 - c)d = 1,$$

which shows that a is indeed a unit. ■

Remark 5.28 (Nir). If $I \subseteq R$ is not a maximal ideal, we need not have $\widehat{R}_I$ be a local ring. For example, $\widehat{\mathbb{Z}}_{(n)}$ is not local if $n > 1$ is not prime: for any $p \mid n$, we see that we have a surjection

$$\widehat{\mathbb{Z}}_{(n)} \twoheadrightarrow \widehat{\mathbb{Z}}_{(n)}/\widehat{(n)} \cong \mathbb{Z}/n\mathbb{Z} \twoheadrightarrow \mathbb{Z}/p\mathbb{Z},$$

and the kernel of this surjection will be maximal because the codomain is a field. But each of these codomains are non-isomorphic (because we are choosing different characteristics p), so they give rise to separate maximal ideals.

5.1.6 Completions via the Associated Graded Ring

As usual, life is better (for completions) in the Noetherian case. To see this, we will want to keep track of all components of $\widehat{R}_{\mathcal{J}}$ simultaneously, for which we will use the associated graded ring.

Here is the key lemma we will use.

Lemma 5.29. Fix a ring R complete with respect to the filtration $\mathcal{J} = \{I_k\}_{k\in\mathbb{N}}$. Given an ideal I with elements $a_1, \ldots, a_n \in I$, if

$$(\operatorname{in} I) = (\operatorname{in} a_1, \ldots, \operatorname{in} a_n) \subseteq \operatorname{gr}_{\mathcal{J}} R,$$

then $I = (a_1, \ldots, a_n)$.

Proof. Fix some $f \in I$ so that we want to show $f \in (a_1, \ldots, a_n)$. We start by getting rid of zeroes so that we can properly talk about degrees. If $f = 0$, then we are done. Similarly, if any of the a_i are zero, then $\operatorname{in} a_i = 0$ as well, so it doesn't help us generate $(\operatorname{in} I)$ or I, so we can safely discard the element.

Otherwise, because R is complete with respect to $\mathcal{J}$, the natural map $R \to \widehat{R}_{\mathcal{J}}$ is injective, so $r \in I$ for each $I \in \mathcal{J}$ implies that $r = 0$. So by the contrapositive, $f \neq 0$ implies that $\operatorname{in} f \neq 0$ and in particular $d := \deg(\operatorname{in} f)$ makes sense. Similarly, $d_i := \deg(\operatorname{in} a_i)$ makes sense for each i.

The key to the proof is the following process. We start by writing

$$\operatorname{in} f = \sum_{i=1}^n g_i(\operatorname{in} a_i)$$

for some $g_i \in \operatorname{gr}_{\mathcal{J}} R$. By focusing on the degree $d = \deg f$, we see that we can assume each g_i is either 0 or homogeneous of degree $\deg(\operatorname{in} f) - \deg(\operatorname{in} a_i) = d - d_i$. For each g_i with $g_i \neq 0$, we have $g_i = [f_i]_{I_{d-d_i+1}} \in I_{d-d_i}/I_{d-d_i+1}$ where $f_i \in I_{d-d_i} \setminus I_{d-d_i+1}$ (for some $d_i \in \mathbb{N}$) so that $g_i = \operatorname{in} f_i$. In particular, we see that

$$[f]_{I_{d+1}} = \operatorname{in} f = \sum_{i=1}^n g_i(\operatorname{in} a_i) = \sum_{i=1}^n [f_i]_{I_{d-d_i+1}} \cdot [a_i]_{I_{d_i+1}} = \sum_{i=1}^n [f_i a_i]_{I_{d+1}}$$

Now, to show $f \in (a_1, \ldots, a_n)$, we see that it will suffice to show

$$f - \sum_{i=1}^n a_i f_i \stackrel{?}{\in} (a_1, \ldots, a_n),$$

which has the bonus that $f - \sum_{i=1}^n a_i f_i$ lives in I_{d+1} now.

In this way, we can push our problem to arbitrarily large degrees, allowing us to arbitrarily approximate f. Our hope is to show to the completion in order to make "arbitrarily close" into an actual equality. For psychological reasons, we will start by pushing f upwards so that $\deg f \geq d_i$ for each i so that I_{d-d_i} always makes sense. Namely, in the above process, when we say that g_i has $g_i = 0$ or $g_i = \operatorname{in} f_i$ with $f_i \in I_{d-d_i} \setminus I_{d-d_i+1}$, we can now always say that $g_i = [f_i]_{I_{d-d_i+1}}$ for some $f_i \in I_{d-d_i}$.

In particular, suppose that $\operatorname{in} f$ has some fixed degree d. Applying the process once, we are able to write

$$\underbrace{f - \sum_{i=1}^n f_{d,i} a_i}_{f_{d+1}} \in I_{d+1},$$

for some $f_{d,i} \in I_{d-d_i}$. Repeating this process, we claim that we can write

$$\underbrace{f - \sum_{e=0}^m \sum_{i=1}^n f_{d+e,i} a_i}_{f_{d+e+1}} \in I_{d+e+1}$$

such that $f_{d+e,i} \in I_{d+e-d_i}$. Indeed, for $e = 0$, we have just discussed how to do this. Then to increment, if $f_{d+e+1} \in I_{d+e+2}$ already, then we just set $f_{d+e+1,i} = 0$ for each i. Otherwise, $f_{d+e+1} \in I_{d+e+1} \setminus I_{d+e}$, so we are able to apply the process to write

$$f - \sum_{e=0}^m \sum_{i=1}^n f_{d+e,i} a_i - \sum_{i=1}^n f_{d+e+1,i} a_i \in I_{d+e+2},$$

where $f_{d+e+1,i} \in I_{d+e-d_i+1}$, which is what we wanted.

So to finish, we fix some i and set

$$h_{i,k} \coloneqq \sum_{e=0}^k f_{d+e,i}.$$

Because R is complete, these partial sums will converge. In particular, if $k > \ell$, then

$$h_{i,k} - h_{i,\ell} = \sum_{e=\ell+1}^k f_{d+e,i} \in I_{d-d_i+\ell} \subseteq I_\ell,$$

so $\{[h_{i,k}]_{I_k}\}_{k\in\mathbb{N}} \in \widehat{R}_{\mathcal{J}}$. But R is complete (!), so we can find $h_i \in R$ such that $\iota(h) = \{[h_{i,k}]_{I_k}\}_{k\in\mathbb{N}}$. In particular, for any $m \in \mathbb{N}$, we see that

$$f - \sum_{i=1}^n h_i a_i \equiv f - \sum_{i=1}^n h_{i,m} a_i \equiv 0 \pmod{I_m}$$

by construction of the h_i. So because ι must also be injective, we conclude that

$$f = \sum_{i=1}^n h_i a_i,$$

which finishes. ■

Here is a nice application, which begins to explain why we want the Noetherian condition.

Theorem 5.30. Fix a Noetherian ring R and an ideal $I \subseteq R$. Then $\widehat{R}_I$ is Noetherian.

Proof. For concreteness, let $\mathcal{J}$ be the I-adic filtration for R, and let $\widehat{\mathcal{J}}$ be the filtration for $\widehat{R}_I$ (given by $\{\widehat{I^k}\}_{k\in\mathbb{N}}$).

Now, pick up any ideal $I \subseteq \widehat{R}_I$. We will find finitely many generators for I by finding finitely many generators of $(\operatorname{in} I) \subseteq \operatorname{gr}_{\widehat{\mathcal{J}}} \widehat{R}_I$, which will be enough by Lemma 5.29. In fact, we claim that $\operatorname{gr}_{\widehat{\mathcal{J}}} \widehat{R}_I$ is Noetherian, which will guarantee that $(\operatorname{in} I)$ is finitely generated for free. For this, we have the following lemma.

Lemma 5.31. Fix a ring R with filtration $\mathcal{J} = \{I_k\}_{k\in\mathbb{N}}$, and give $\widehat{R}_{\mathcal{J}}$ the filtration $\widehat{\mathcal{J}}$ by

$$\widehat{R}_{\mathcal{J}} = \widehat{I}_0 \supseteq \widehat{I}_1 \supseteq \widehat{I}_2 \supseteq \cdots.$$

Then $\operatorname{gr}_{\mathcal{J}} R \cong \operatorname{gr}_{\widehat{\mathcal{J}}} \widehat{R}_{\mathcal{J}}$.

Proof. The point is to glue together isomorphisms $\widehat{I}_k/\widehat{I}_{k+1} \cong I_k/I_{k+1}$. We begin by exhibiting the needed isomorphisms. By definition, we have $\widehat{R}_{\mathcal{J}}/\widehat{I}_k \cong R/I$. Thus, we set up the following diagram.

$$\begin{tikzcd}
0 \arrow[r] & \dfrac{\widehat{I}_k}{\widehat{I}_{k+1}} \arrow[r] \arrow[d, dashed] & \dfrac{\widehat{R}_{\mathcal{J}}}{\widehat{I}_{k+1}} \arrow[r] \arrow[d] & \dfrac{\widehat{R}_{\mathcal{J}}}{\widehat{I}_k} \arrow[r] \arrow[d] & 0 \\
0 \arrow[r] & \dfrac{I_k}{I_{k+1}} \arrow[r] & \dfrac{R}{I_{k+1}} \arrow[r] & \dfrac{R}{I_k} \arrow[r] & 0
\end{tikzcd}$$

We know that the rows are exact by a direct computation. Additionally, the two maps on the right are isomorphisms. Now, this right square commutes: along the top, some $\{[r_s]\}_{s\in\mathbb{N}} + \widehat{I}_k$ goes to $\{[r_s]\}_{s\in\mathbb{N}} + \widehat{I}_{k+1}$ goes to $r_k + I_k$; along the bottom, we go to $r_{k+1} + I_{k+1}$ and then $r_{k+1} + I_k$, which is equal by definition of $\widehat{R}_{\mathcal{J}}$.

Thus, the diagram induces an isomorphism

$$\varphi_k : \frac{\widehat{I}_k}{\widehat{I}_{k+1}} \cong \frac{I_k}{I_{k+1}}.$$

To be explicit, this isomorphism merely follows the left square around: we take $\{[r_k]\}_{k\in\mathbb{N}} + \widehat{I}_{k+1} \in \widehat{I}_k/\widehat{I}_{k+1}$ to $\{[r_k]\}_{k\in\mathbb{N}} + \widehat{I}_{k+1}\widehat{R}_{\mathcal{J}}/\widehat{I}_{k+1}$ down to $r_{k+1} + I_{k+1} \in R/I_{k+1}$ and back to $r_{k+1} + I_{k+1} \in I_k/I_{k+1}$. This map is well-defined and an isomorphism by the above argument.

Now, we can glue our isomorphisms together to give an isomorphism

$$\operatorname{gr}_{\widehat{\mathcal{J}}} \widehat{R}_{\mathcal{J}} = \bigoplus_{k\ge 0} \frac{\widehat{I}_k}{\widehat{I}_{k+1}} \cong \bigoplus_{k\ge 0} \frac{I_k}{I_{k+1}} = \operatorname{gr}_{\mathcal{J}} R$$

of R-modules. To make this an isomorphism of rings, we need to check that we preserve multiplicative structure. Let φ be the above composite so that we need to show $\varphi(1) = 1$ and $\varphi(fg) = \varphi(f)\varphi(g)$. For the first, we see that

$$\varphi([1],[0],[0],\ldots) = ([1],[0],[0],\ldots)$$

by definition of φ. For the second, we already know that φ is additive, so by decomposing f and g into homogeneous components, it suffices to check for f and g homogeneous. That is, we take $f = [r]_{\widehat{I}_{k+1}}$ and $g = [s]_{\widehat{I}_{\ell+1}}$. Then

$$\varphi\left([r]_{\widehat{I}_{k+1}} \cdot [s]_{\widehat{I}_{\ell+1}}\right) = \varphi\left([rs]_{\widehat{I}_{k+\ell+1}}\right) = [rs]_{I_{k+\ell+1}} = [r]_{I_{k+1}} \cdot [s]_{I_{\ell+1}} = \varphi\left([r]_{\widehat{I}_{k+1}}\right)\varphi\left([s]_{\widehat{I}_{\ell+1}}\right),$$

which finishes. ■

Thus, we finish by noting that

$$\operatorname{gr}_{\widehat{\mathcal{J}}} \widehat{R}_I = \operatorname{gr}_I R$$

is Noetherian by Lemma 4.12. This finishes. ■

Remark 5.32 (Nir)**.** One might complain that this proof seems needless hard, but there is in fact some obstacle to overcome. For example, when one wants to show that $k[\![x]\!]$ is Noetherian (which is the completion of $k[x]$ at (x)), one usually has to use Weierstrass preparation, which is also a difficult technique.

5.1.7 Nice Special Cases

As another consequence, we can manifest Remark 5.10 under fairly restrictive hypotheses.

Proposition 5.33. Fix a Noetherian ring R and an ideal $I \subseteq R$, and endow R with the I-adic filtration. Then $\widehat{I^n} = I^n \widehat{R}_I$.

Proof. Let $\mathcal{J}$ be the I-adic filtration for R, and let $\widehat{\mathcal{J}}$ be the induced filtration of $\widehat{R}_I$ (given by $\{\widehat{I^k}\}_{k\in\mathbb{N}}$).

As before, the key trick is to look in $\operatorname{gr}_{\widehat{\mathcal{J}}} \widehat{R}_I$. By Lemma 5.31, this ring is isomorphic to $\operatorname{gr}_I R$ and hence Noetherian by Lemma 4.12. In particular, $(\operatorname{in} \widehat{I^n})$ and $(\operatorname{in} I^n \widehat{R}_I)$ will both be finitely generated.

By decomposing the generators into homogeneous parts, we can assume that all relevant generators are homogeneous and nonzero and therefore of the form $f + \widehat{I^{k+1}} \in \widehat{I^k}/\widehat{I^{k+1}}$, which is simply $\operatorname{in} f$ when nonzero. Thus, $(\operatorname{in} \widehat{I^k})$ and $(\operatorname{in} I^k \widehat{R}_I)$ are both finitely generated by initial forms.

With this in mind, we show that $\widehat{I^n}$ and $I^n \widehat{R}_I$ give rise to the same set of initial forms. Namely, we claim that these initial forms are exactly the ones of degree at least n (and 0).

- We work with $\widehat{I^n}$. In one direction, pick up some $\{[r_k]\}_{k\in\mathbb{N}} \in \widehat{I^n}$ so that $[r_n]_{I^n} = [0]_{I^n}$. Then, for any $k \le n$, we have $r_k \equiv r_n \equiv 0 \pmod{I^n}$, so the initial form for $\{[r_k]\}_{k\in\mathbb{N}} \in \widehat{I^n}$ is either 0 or of degree at least n.

  In the other direction, of course 0 is an initial form, so pick up some nonzero initial form $\{[r_k]\}_{k\in\mathbb{N}} + \widehat{I^{m+1}}$ of degree $m \ge n$ so that $\{[r_k]\}_{k\in\mathbb{N}} \in \widehat{I^m} \subseteq \widehat{I^n}$. In this case, we note that $\{[r_k]\}_{k\in\mathbb{N}} \notin \widehat{I^{m+1}}$ follows, so $\operatorname{in}\{[r_k]\}_{k\in\mathbb{N}}$ is exactly the initial form we wanted to exhibit.

- We work with $I^n \widehat{R}_I$. In one direction, pick up some element

$$\sum_{i=1}^m f_i \{[r_{i,k}]\}_{k\in\mathbb{N}} = \left\{\left[\sum_{i=1}^n f_i r_{i,k}\right]\right\}_{k\in\mathbb{N}} \in I^n \widehat{R_I},$$

  where the f_i live in I^n. Thus, we see that then nth coordinate is $\sum_i f_i r_{i,n} \in I^n$, so this element lives in $\widehat{I^n}$, so the above work shows that this element gives an initial form which is zero or of degree at least n.

  In the other direction, pick up some initial form $\{[r_k]\}_{k\in\mathbb{N}} + \widehat{I^{m+1}}$ of degree $m \ge n$. Then we see

$$\{[r_k]\}_{k\in\mathbb{N}} - \{[r_{m+1}]\}_{k\in\mathbb{N}}$$

  will vanish in the $m+1$ coordinate, so this difference lives in $\widehat{I^{m+1}}$. So our initial form is actually $\{[r_{m+1}]\}_{k\in\mathbb{N}} + \widehat{I^{m+1}}$. If this is 0, then of course we can get 0 from $I^n \widehat{R}_I$. Otherwise, $r_{m+1} \notin I^{m+1}$, so

$$\{[r_{m+1}]\}_{k\in\mathbb{N}} + \widehat{I^{m+1}} = \operatorname{in}\{[r_{m+1}]\}_{k\in\mathbb{N}}.$$

  However, we now note that $\{[r_{m+1}]\}_{k\in\mathbb{N}} = r_{m+1} \cdot \{[1]\}_{k\in\mathbb{N}}$ lives in $I^n \widehat{R}_I$ because $r_{m+1} \in I^m \subseteq I^n$. This finishes the check.

Now, if $(\operatorname{in}\widehat{I^n})$ is generated by some initial forms $\operatorname{in}a_1,\ldots,\operatorname{in}a_m$, then these initial forms also arise from $(\operatorname{in}I^n\widehat{R}_I)$, so $(\operatorname{in}\widehat{I^n})\subseteq(\operatorname{in}I^n\widehat{R}_I)$; running this argument in reverse gives the equality, so we see that

$$(\operatorname{in}\widehat{I^n})=(\operatorname{in}a_1,\ldots,\operatorname{in}a_m)=(\operatorname{in}I^n\widehat{R}_I),$$

so

$$\widehat{I^n}=(a_1,\ldots,a_m)=I^n\widehat{R}_I$$

by Lemma 5.29. This finishes. ■

Corollary 5.34. Fix a Noetherian ring R and an ideal $I\subseteq R$, and endow R with the I-adic filtration. Then $\operatorname{gr}_I R\cong\operatorname{gr}_{I\widehat{R}_I}\widehat{R}_I$.

Proof. We string together our isomorphisms. Let $\widehat{\mathcal{J}}$ be the filtration on $\widehat{R}_I$ induced by the I-adic filtration on R; that is, $\mathcal{J}=\{\widehat{I^k}\}_{k\in\mathbb{N}}$. Note Lemma 5.31 gives

$$\operatorname{gr}_I R\cong\operatorname{gr}_{\widehat{\mathcal{J}}}\widehat{R}_I=\bigoplus_{s\geq0}\frac{\widehat{I^s}}{\widehat{I^{s+1}}}.$$

Now, using Proposition 5.33, we see this is

$$\bigoplus_{s\geq0}\frac{\widehat{I^s}}{\widehat{I^{s+1}}}=\bigoplus_{s\geq0}\frac{I^s\widehat{R}_I}{I^{s+1}\widehat{R}_I}.$$

We thus claim that $I^s\widehat{R}_I=(I\widehat{R}_I)^s$. By fully distributing an element of $(I\widehat{R}_I)^s$ as

$$\prod_{k=1}^{s}\sum_{i=1}^{n_k}a_ir_i,$$

we see that the a_i will collect to give us a term in $I^s\widehat{R}_I$. And conversely, an element

$$\sum_{i=1}^{n}\left(\prod_{k=1}^{s}a_{i,k}\right)r_i$$

in $I^s\widehat{R}_I$ can be written as

$$\sum_{i=1}^{n}r_k\left(\prod_{k=1}^{n}a_{i,k}\cdot1_{\widehat{R}_I}\right),$$

which now lives in $(I\widehat{R}_I)^s$ term-wise.

Thus, we have the equality

$$\bigoplus_{s\geq0}\frac{I^s\widehat{R}_I}{I^{s+1}\widehat{R}_I}=\bigoplus_{s\geq0}\frac{(I\widehat{R}_I)^s}{(I\widehat{R}_I)^{s+1}}=\operatorname{gr}_{I\widehat{R}_I}\widehat{R}_I,$$

which is what we wanted. Notably, the multiplicative structure is simply carried through the equalities as a multiplication endowed by the grading. ■

5.1.8 Completion for Modules

We close class by quickly stating the story of completions for modules.

Definition 5.35 (Completion, modules)**.** Fix a ring R and filtration $\mathcal{J} = \{I_k\}_{k\in\mathbb{N}}$. Further, given an R-module M, there is an induced filtration (which we also name $\mathcal{J}$) given by

$$M = I_0M \supseteq I_1M \supseteq I_2M \supseteq \cdots.$$

Then we define

$$\widehat{M}_{\mathcal{J}} = \left\{(m_0, m_1, \ldots) \in \prod_{s\in\mathbb{N}} M/I_sM : m_i \equiv m_j \pmod{I_jM} \text{ for } i > j\right\}$$

Remark 5.36 (Nir)**.** Again, we might also denote this by

$$\varprojlim_s M/I_sM.$$

We can quickly check that $\widehat{M}_{\mathcal{J}}$ is at least an R-submodule of $\prod_{s\in\mathbb{N}} M/I_sM$: for any r, $s \in R$ and $\{[m_k]\}_{k\in\mathbb{N}}$, $\{[s_k]\}_{k\in\mathbb{N}} \in \widehat{M}_{\mathcal{J}}$, we see that our action gives

$$r \cdot \{[m_k]\}_{k\in\mathbb{N}} + s \cdot \{[n_k]\}_{k\in\mathbb{N}} = \{[rm_k + sn_k]\}_{k\in\mathbb{N}}.$$

Now, for $i > j$, we see that $m_i \equiv m_j \pmod{I_jM}$ and $n_i \equiv n_j \pmod{I_jM}$, so

$$rm_i + sn_i \equiv rm_j + sn_j \pmod{I_j},$$

so $r \cdot \{[m_k]\}_{k\in\mathbb{N}} + s \cdot \{[n_k]\}_{k\in\mathbb{N}} \in \widehat{M}_{\mathcal{J}}$ follows.

In fact, we have a little stronger structure.

Lemma 5.37. Fix a ring R and filtration $\mathcal{J}$. Then $\widehat{M}_{\mathcal{J}}$ is an $\widehat{R}_{\mathcal{J}}$-submodule.

Proof. The $\widehat{R}_{\mathcal{J}}$-action on $\widehat{M}_{\mathcal{J}}$ will be given by

$$\{[r_k]_{I_k}\}_{k\in\mathbb{N}} \cdot \{[m_k]_{I_kM}\}_{k\in\mathbb{N}} = \{[r_km_k]_{I_kM}\}_{k\in\mathbb{N}}.$$

Notably, the action of R/I_k on M/I_kM is well-defined because $r \equiv s \pmod{I_k}$ and $m \equiv n \pmod{I_kM}$ will have

$$rm - sn = r(m-n) + (r-s)n \in I_kM.$$

Further, $\widehat{M}_{\mathcal{J}}$ is closed under this action: again fix $\{[r_k]\}_{k\in\mathbb{N}} \in \widehat{R}_{\mathcal{J}}$ and $\{[m_k]\}_{k\in\mathbb{N}} \in \widehat{M}_{\mathcal{J}}$. Then, if $i > j$, then we see that $r_i \equiv r_j \pmod{I_j}$ and $m_i \equiv m_j \pmod{I_jM}$, so

$$r_im_i \equiv r_jm_j \pmod{I_jM}$$

by the exact same check as above.

So we have provided a well-defined action. To show that we actually have a module structure, we pick up two pairs of elements $\{[r_k]\}_{k\in\mathbb{N}}, \{[s_k]\}_{k\in\mathbb{N}} \in \widehat{R}_{\mathcal{J}}$ and $\{[m_k]\}_{k\in\mathbb{N}}, \{[s_k]\}_{k\in\mathbb{N}} \in \widehat{M}_{\mathcal{J}}$ and run the following checks.

- Associativity: we see

$$\{[r_k]\}_{k\in\mathbb{N}} \cdot (\{[s_k]\}_{k\in\mathbb{N}} \cdot \{[m_k]\}_{k\in\mathbb{N}}) = \{[r_ks_km_k]\}_{k\in\mathbb{N}} = (\{[r_k]\}_{k\in\mathbb{N}} \cdot \{[s_k]\}_{k\in\mathbb{N}}) \cdot \{[m_k]\}_{k\in\mathbb{N}}.$$

- Distributivity: we see

$$\begin{aligned}(\{[r_k]\}_{k\in\mathbb{N}}+\{[s_k]\}_{k\in\mathbb{N}})\cdot\{[m_k]\}_{k\in\mathbb{N}}&=\{[r_km_k+s_km_k]\}_{k\in\mathbb{N}}\\&=(\{[r_k]\}_{k\in\mathbb{N}}\cdot\{[m_k]\}_{k\in\mathbb{N}})+(\{[s_k]\}_{k\in\mathbb{N}}\cdot\{[m_k]\}_{k\in\mathbb{N}}).\end{aligned}$$

- Distributivity: we see

$$\begin{aligned}\{[r_k]\}_{k\in\mathbb{N}}(\{[m_k]\}_{k\in\mathbb{N}}+\{[n_k]\}_{k\in\mathbb{N}})&=\{[r_km_k+r_kn_k]\}_{k\in\mathbb{N}}\\&=(\{[r_k]\}_{k\in\mathbb{N}}\cdot\{[m_k]\}_{k\in\mathbb{N}})+(\{[r_k]\}_{k\in\mathbb{N}}\cdot\{[n_k]\}_{k\in\mathbb{N}}).\end{aligned}$$

- Identity: we see
$$\{[1]\}_{k\in\mathbb{N}}\cdot\{[m_k]\}_{k\in\mathbb{N}}=\{[m_k]\}_{k\in\mathbb{N}}.$$

These checks finish. ■

To finish class, we have the following result, in analogy with the case of localization (namely, Proposition 2.49 and Corollary 2.53).

Theorem 5.38. Fix R a Noetherian ring with an ideal $I\subseteq R$ and M a finitely generated R-module.

(a) We have that $\widehat{M}_I\cong\widehat{R}_I\otimes_R M$, and this isomorphism is natural in M.

(b) We have that $\widehat{R}_I$ is a flat R-module.

Proof. This will be proven next class. ■

5.2 March 10

We continue discussing completion.

5.2.1 Refining Inverse Limits

Recall that we had a notion of completion for modules as follows.

Definition 5.35 (Completion, modules)**.** Fix a ring R and filtration $\mathcal{J}=\{I_k\}_{k\in\mathbb{N}}$. Further, given an R-module M, there is an induced filtration (which we also name $\mathcal{J}$) given by

$$M=I_0M\supseteq I_1M\supseteq I_2M\supseteq\cdots.$$

Then we define

$$\widehat{M}_{\mathcal{J}}=\left\{(m_0,m_1,\ldots)\in\prod_{s\in\mathbb{N}}M/I_sM:m_i\equiv m_j\pmod{I_jM}\text{ for }i>j\right\}$$

Here is our primary example.

Example 5.39. If we fix an ideal $I\subseteq R$, then we are granted an I-adic filtration of M, which gives the I-adic completion of M. In particular, this is an $\widehat{R}_I$-module by Lemma 5.37.

We are going to want some freedom in changing our exact filtration, so we have the following sequence of lemmas. To start, subsequences don't do anything to our inverse limit.

Lemma 5.40. Fix an R-module M with a filtration $\mathcal{J} = \{M_k\}_{k\in\mathbb{N}}$. Then, for any strictly increasing function $\alpha : \mathbb{N} \to \mathbb{N}$, we have

$$\varprojlim M/M_{\alpha k} \cong \varprojlim M/M_k.$$

Proof. We proceed by force. For any k, we note that $\alpha k \geq k$ (e.g., by induction because α is strictly increasing), so $M_k \supseteq M_{\alpha k}$, so we have an induced map

$$\psi_k : M/M_{\alpha k} \twoheadrightarrow M/M_k.$$

As such, we define the map $\psi : \prod_k M/M_{\alpha k} \to \prod_k M/M_k$ by

$$\psi : \{m_k + M_{\alpha k}\}_{k\in\mathbb{N}} \mapsto \{m_k + M_k\}_{k\in\mathbb{N}}$$

created by gluing the maps ψ_k. We claim that ψ descends to the desired isomorphism: let φ be the restriction of ψ to $\varprojlim M/M_{\alpha k}$. We have the following checks on φ.

- The image of φ is contained in $\varprojlim M/M_k$. Indeed, fix some $\{m_k + M_{\alpha k}\}_{k\in\mathbb{N}}$, which goes to $\{m_k + M_k\}_{k\in\mathbb{N}}$. For any $i > j$, we need to show that

  $$m_i \equiv m_j \pmod{M_i}.$$

  Well, by hypothesis, we see that $m_i \equiv m_j \pmod{M_{\alpha i}}$, so $m_i - m_j \in M_{\alpha i} \subseteq M_i$, which is what we wanted.

- The image of φ contains $\varprojlim M/M_k$. For this, we create an inverse map of sets. Indeed, fix some $\{m_k + M_k\}_{k\in\mathbb{N}}$, and we note that

  $$\varphi : \{m_{\alpha k} + M_{\alpha k}\}_{k\in\mathbb{N}} \mapsto \{m_{\alpha k} + M_k\}_{k\in\mathbb{N}}.$$

  So we claim that $\{m_{\alpha k} + M_{\alpha k}\}_{k\in\mathbb{N}}$ is the desired input. First, this input is valid: for any $i > j$, we see that $m_{\alpha i} \equiv m_{\alpha j} \pmod{M_{\alpha i}}$ by hypothesis on the m_i.

  But second, we note that $\alpha k \geq k$ implies that

  $$m_{\alpha k} \equiv m_k \pmod{M_k},$$

  so $\{m_{\alpha k} + M_k\}_{k\in\mathbb{N}} = \{m_k + M_k\}_{k\in\mathbb{N}}$, so we have indeed hit the desired coset.

- The kernel of φ is trivial. Indeed, suppose that $\{m_k + M_{\alpha k}\}_{k\in\mathbb{N}}$ goes to 0 under φ, which means that

  $$m_k + M_k = 0 + M_k$$

  for each k. But this implies that $m_{\alpha k} \in M_{\alpha k}$ while $\alpha k \geq k$, so the hypothesis on the m_k implies that

  $$m_k \equiv m_{\alpha k} \equiv 0 \pmod{M_{\alpha k}},$$

  so the $m_k + M_{\alpha k}$ all vanish. This finishes.

Thus, we have shown that φ will inject onto $\varprojlim M/M_k$ and therefore witnesses the needed isomorphism

$$\varprojlim M/M_{\alpha k} \cong \varprojlim M/M_k.$$

This finishes. ■

Next, we note that containment is fairly well-behaved.

Lemma 5.41. Fix an R-module M with filtrations $\mathcal{J} = \{M_k\}_{k\in\mathbb{N}}$ and $\mathcal{J}' = \{M_k'\}_{k\in\mathbb{N}}$ such that $M_k \subseteq M_k'$ for each k. Then the map

$$\{m_k + M_k\}_{k\in\mathbb{N}} \mapsto \{m_k + M_k'\}_{k\in\mathbb{N}}$$

defines a morphism $\varprojlim M/M_k \to \varprojlim M/M_k'$.

Proof. For any fixed k, that $M_k \subseteq M_k'$ induces a morphism $\psi_k : M/M_k \to M/M_k'$ by

$$\psi_k : m_k + M_k \to m_k + M_k'.$$

These glue together to a morphism

$$\psi : \prod_{k\in\mathbb{N}} M/M_k \to \prod_{k\in\mathbb{N}} M/M_k'.$$

Let φ be the restriction of this map to $\varprojlim M/M_k$, and we need to show $\operatorname{im}\varphi \subseteq \varprojlim M/M_k'$. Well, fix $\{m_k + M_k\}_{k\in\mathbb{N}}$ in $\varprojlim M/M_k$. Then, for any $i > j$, we see that

$$m_i - m_j \in M_j \subseteq M_j',$$

so it follows

$$\{m_k + M_k'\}_{k\in\mathbb{N}} \in \varprojlim M/M_k',$$

which is what we wanted. ∎

We can then synthesize the above two lemmas to give the following refinement result.

Lemma 5.42. Fix an R-module M with filtrations $\mathcal{J} = \{M_k\}_{k\in\mathbb{N}}$ and $\mathcal{J}' = \{M_k'\}_{k\in\mathbb{N}}$. Further, suppose that, for all i, there exists j such that $M_i \supseteq M_j'$; similarly, there exists (perhaps another) j such that $M_i' \supseteq M_j$. Then we have an isomorphism

$$\varprojlim M/M_i \cong \varprojlim M/M_i'$$

Proof. In general, if we have two inverse limits, the way to define an inverse limit is to define a map into each of the components. To manifest this idea, we pick up strictly increasing $\alpha, \beta, \gamma : \mathbb{N} \to \mathbb{N}$ such that

$$M_j \supseteq M'_{\alpha(j)} \supseteq M_{\beta(j)} \supseteq M'_{\gamma(j)}. \tag{$*$}$$

To show that such α, β, γ all actually exist, we proceed inductively: we can start with $\alpha(0) = \beta(0) = \gamma(0)$ because $M_0 = M_0' = M$. Then, if we have defined all three up to $n \in \mathbb{N}$, we increment in three steps.

- We find some n' such that $M_n \supseteq M'_{n'}$. Then we can set $\alpha(n+1) = \max\{n', \alpha n + 1\}$, which works because $M'_{n'} \supseteq M_{\alpha(n+1)}$ while $\alpha(n+1) > \alpha(n)$.
- We find some n' such that $M'_{\alpha(n+1)} \supseteq M_{n'}$. Then we can set $\beta(n+1) = \max\{n', \beta n + 1\}$, which works because $M'_{\alpha(n+1)} \supseteq M_{\beta(n+1)}$ while $\beta(n+1) > \beta(n)$.
- We find some n' such that $M_{\beta(n+1)} \supseteq M'_{n'}$. Then we can set $\gamma(n+1) = \max\{n', \gamma n + 1\}$, which works because $M_{\beta(n+1)} \supseteq M'_{\gamma(n+1)}$ while $\gamma(n+1) > \gamma(n)$.

Anyways, the point is that our α, β, γ induce morphisms

$$\varprojlim M/M'_{\gamma(j)} \to \varprojlim M/M_{\beta(j)} \to \varprojlim M/M'_{\alpha(j)} \to \varprojlim M/M_j$$

by Lemma 5.41. In fact, Lemma 5.40 lets us remove the α,β,γ to set up the following commutative diagram.

$$\begin{tikzcd}
\varprojlim M/M'_{\gamma(j)} \arrow[r] \arrow[d] & \varprojlim M/M_{\beta(j)} \arrow[r] \arrow[d] & \varprojlim M/M'_{\alpha(j)} \arrow[r] \arrow[d] & \varprojlim M/M_j \arrow[d] \\
\varprojlim M/M'_j \arrow[r, dashed, "f"] & \varprojlim M/M_j \arrow[r, dashed, "g"] & \varprojlim M/M'_j \arrow[r, dashed, "h"] & \varprojlim M/M_j
\end{tikzcd}$$

Namely, the vertical morphisms are isomorphisms and therefore induce the morphisms on the bottom row. We claim that gf and hg are both the identity. Indeed, tracking through the morphisms in the commutative diagram, we see that fg moves as follows.

$$\begin{tikzcd}
\{m_{\gamma k}+M'_{\gamma k}\}_{k\in\mathbb{N}} \arrow[r] \arrow[d] & \{m_{\gamma k}+M_{\beta k}\}_{k\in\mathbb{N}} \arrow[r] \arrow[d] & \{m_{\gamma k}+M'_{\alpha k}\}_{k\in\mathbb{N}} \arrow[r] \arrow[d] & \bullet \arrow[d] \\
\{m_k+M'_k\}_{k\in\mathbb{N}} \arrow[r, dashed, "f"] & \bullet \arrow[r, dashed, "g"] & \{m_{\gamma k}+M'_k\}_{k\in\mathbb{N}} \arrow[r, dashed, "h"] & \bullet
\end{tikzcd}$$

This is the identity because $\gamma k\ge k$ (because γ is strictly increasing), so $m_k+M'_k=m_{\gamma k}+M'_k$ for any k.

Similarly, we track hg as follows.

$$\begin{tikzcd}
\bullet \arrow[r] \arrow[d] & \{m_{\beta k}+M_{\beta k}\}_{k\in\mathbb{N}} \arrow[r] \arrow[d] & \{m_{\beta k}+M'_{\alpha k}\}_{k\in\mathbb{N}} \arrow[r] \arrow[d] & \{m_{\beta k}+M_k\}_{k\in\mathbb{N}} \arrow[d] \\
\bullet \arrow[r, dashed, "f"] & \{m_k+M_k\}_{k\in\mathbb{N}} \arrow[r, dashed, "g"] & \bullet \arrow[r, dashed, "h"] & \{m_{\beta k}+M_k\}_{k\in\mathbb{N}}
\end{tikzcd}$$

Again, this is the identity because $\beta k\ge k$ everywhere implies that $m_k+M_k=m_{\beta k}+M_k$ for any k.

Thus, we see that g is a morphism with both a left and a right inverse, so it is an isomorphism. (For example, a left inverse shows that g is injective, and a right inverse shows that g is surjective.) This is what we wanted to prove, so we are done. ■

Remark 5.43 (Nir)**.** Another way to prove Lemma 5.42 is to note that both filtrations will induce the same topology on M and therefore will be isomorphic as completions.

5.2.2 Completion for Modules

We now return to talking about completions. We want to show that $\widehat{R}_I$ is flat, so we will want to talk about short exact sequences.

Lemma 5.44. Fix R a Noetherian ring and an ideal I. Further, suppose that we have a short exact sequence

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

of finitely generated R-modules. Then we have a short exact sequence

$$0\to\widehat{A}\to\widehat{B}\to\widehat{C}\to 0$$

of completions.

Proof. We start with the short exact sequence

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

and tensor by $-\otimes R/I^s$ to get a right-exact sequence

$$A/I^sA \to B/I^sB \to C/I^sC \to 0.$$

We can show by hand that this gives us a surjection $\widehat{B} \twoheadrightarrow \widehat{C}$, but we need this to be exact on the left. Well, the next best thing that we can write down is

$$0 \to \frac{A}{A\cap I^sB} \to \frac{B}{I^sB} \to \frac{C}{I^sC},$$

so because taking inverse limits is left exact, we have a left-exact sequence

$$0 \to \varprojlim \frac{A}{A\cap I^sB} \to \varprojlim \frac{B}{I^sB} \to \varprojlim \frac{C}{I^sC}.$$

It remains to show that our left term is $\widehat{A}$. Well, by the Artin–Rees lemma (!), we see that the filtration

$$A\cap I^sB$$

is an I-stable filtration. In other words, there is an n such that $I^k(A\cap I^nB) = A\cap I^{n+k}B \subseteq I^kA$ for sufficiently large k. Applying Lemma 5.42 finishes. ■

The point of this is that we see completion is an exact functor. In fact, as with localization, there is a flat module hiding in the background.

Theorem 5.38. Fix R a Noetherian ring with an ideal $I\subseteq R$ and M a finitely generated R-module.

(a) We have that $\widehat{M}_I \cong \widehat{R}_I \otimes_R M$, and this isomorphism is natural in M.

(b) We have that $\widehat{R}_I$ is a flat R-module.

Proof. So we show (a). If $M\cong R$, then we are done. Because tensoring and completion commutes with taking direct sums, we see that (a) remains true for $M\cong R^n$ for $n\in\mathbb{N}$. Otherwise, because we live in a Noetherian world, M is finitely presented, so we have a right-exact sequence

$$G\to F\to M\to 0$$

where F and G are both free of finite rank. Tensoring with $\widehat{R}_I$, we see that

$$G\otimes_R \widehat{R}_I \to G\otimes_R \widehat{R}_I \to M\otimes_R \widehat{R} \to 0.$$

We also have the short exact sequence

$$\widehat{G}_I \to \widehat{F}_I \to \widehat{M}_I \to 0,$$

so we slap them on top of each other to build the following diagram.

$$\begin{tikzcd}
G\otimes_R \widehat{R}_I \arrow[r] \arrow[d] & F\otimes_R \widehat{R}_I \arrow[r] \arrow[d] & M\otimes_R \widehat{R}_I \arrow[r] \arrow[d] & 0 \\
\widehat{G}_I \arrow[r] & \widehat{F}_I \arrow[r] & \widehat{M}_I \arrow[r] & 0
\end{tikzcd}$$

In particular, the two left maps are isomorphisms, so the right map is also an isomorphism by the Snake lemma.

We now show (b). We would like to use the previous lemma, but it only works for finitely generated modules instead of general short exact sequences. But have no fear—it suffices to show that the natural inclusion

$$J\otimes_R \widehat{R}_I \to \widehat{R}_I$$

is an inclusion for any finitely generated J by our flatness criterion, which we do have, so we are done. ■

Remark 5.45 (Nir)**.** It is in fact necessary that M be finitely generated. For example, take $R = \mathbb{Z}$ and $I = (p)$ and $M = \mathbb{Q}$. In this case, $\widehat{R}_I \otimes_R M = \mathbb{Q}_p$, but $\widehat{M}_I = 0$ because $M/I^sM = \mathbb{Q}/(p^s)\mathbb{Q} = \mathbb{Q}/\mathbb{Q} = 0$ for all s.

5.2.3 Examples of Hensel's Lemma

Let's continue talking about number theory. Hensel's lemma is a way to lift solutions to polynomial equations from quotients up to complete rings. More precisely, we have the following.

Theorem 5.46 (Hensel's lemma)**.** Suppose that R is a ring complete with respect to an I-adic filtration, and pick up a polynomial $f(x) \in R[x]$. Now, suppose we have $a \in R$ such that

$$f(a) \equiv 0 \pmod{f'(a)^2 I}.$$

Then there exists $b \in R$ such that $b \equiv a \pmod{f'(a)m}$ and $f(b) = 0$.

We do a few examples before proving the lemma.

Exercise 5.47. We solve for $x \in k[\![t]\!]$ in the equation $x^2 = 1 + t$, where $k[\![t]\!]$ is complete with respect to (t).

Proof. Note that $x_0 = 1$ is a solution in $R/(t)$. So we hope that we can find a solution $u \in k[\![t]\!]$ such that $u \equiv 1 \pmod{t}$ such that $u^2 = 1 + t$. Well, from the general binomial theorem, we can write

$$\sqrt{1+t} = \sum_{k=0}^{\infty} \binom{1/2}{k} t^k.$$

We can check that this works. ∎

Exercise 5.48. Fix $a \in \mathbb{Z}_p$ for an odd prime p. We discuss when we can solve $x^2 \equiv a$.

Proof. If $a = 0$, then we are done. Otherwise, write $a = bp^n$ where $b \in \mathbb{Z}_p \setminus p\mathbb{Z}_p$. If n is odd, there is no solution; so we let $n = 2k$ and write

$$\left(x/p^k\right)^2 = b,$$

so we are solving $y^2 = b$, where $b \in \mathbb{Z}_p \setminus p\mathbb{Z}_p$. Now, if a solution is to exist, then we require $b \pmod{p}$ to be a perfect square, so find $x_0 \in \mathbb{F}_p$ such that

$$x_0^2 \equiv b \pmod{p}.$$

To check that we can lift by Hensel's lemma, we need to check the derivative, but when p is odd, then our derivative is $2x_0$, which is nonzero because x_0 is nonzero.

Let's actually show how we can solve this. Well, expand out x in a p-adic series as

$$\left(\sum_{k=0}^{\infty} x_k p^k\right)^2 = b =: \sum_{k=0}^{\infty} b_k p^k.$$

We already have x_0. For x_1, we check the linear term to find

$$2x_0x_1 \equiv b_1 \pmod{p},$$

from which we extract b_1. More generally, this term reads as

$$x_0x_n + \sum_{k=1}^{n} x_kx_{n-k} = b_n,$$

from which we can solve for x_n recursively. ■

Exercise 5.49. We show that $x^2 = b$ has a solution in $\mathbb{Z}_2$ if b is an odd perfect square $\pmod 8$. In other words, we require $b \equiv 1 \pmod 8$.

Proof. Simply use Hensel's lemma, but now $f'(a)^2 \cdot 2$ is divisible by a factor of 8. ■

5.2.4 Proof of Hensel's Lemma

With sufficient motivation, we now turn to a proof of Theorem 5.46. We have the following universal property.

Proposition 5.50. Fix S an R-algebra such that S is complete with respect to an ideal $I \subseteq S$. If $I = (f_1, \ldots, f_n)$ is finitely generated, then there is a unique homomorphism

$$\varphi : R[\![x_1, \ldots, x_n]\!] \to S$$

such that $x_\bullet \mapsto f_\bullet$, and φ is continuous under the induced I-adic topology. In fact, the following hold.

- If $R \to S/I$ is surjective, then φ is surjective.
- If the induced map $R[x_1, \ldots, x_n] \to \operatorname{gr}_I S$, then φ is injective.

Remark 5.51. This is intended to be an analog for the universal property of polynomial algebras.

Proof. To construct φ, it suffices to note that $R[\![x_1, \ldots, x_n]\!]$ is the completion of $R[x_1, \ldots, x_n]$ with respect to the ideal $\mathfrak{m} = (x_1, \ldots, x_n)$ and then construct a system of maps

$$\varphi_k : \frac{R[x_1, \ldots, x_n]}{\mathfrak{m}^k} \to \frac{S}{I^k}.$$

Alternatively, we can note that the restricted map on $R[x_1, \ldots, x_n] \to S$ is forced and use continuity to fill in for the rest of $R[\![x_1, \ldots, x_n]\!]$.

For the surjectivity check, we note that we can lift to

$$\varphi_k : \frac{R[x_1, \ldots, x_n]}{\mathfrak{m}^k} \to \frac{S}{I^k}$$

is surjective, so going to the completion provides the result.

Lastly, we note that the condition tells us that

$$\bigcap_i I^i = 0 \implies \bigcap \mathfrak{m}^i = 0.$$

To finish our injectivity check, we note more generally that if $\varphi : A \to B$ is a map of filtered algebras, then we can build an associated map $\operatorname{gr}\varphi : \operatorname{gr} A \to \operatorname{gr} B$. Then if $\operatorname{gr}\varphi$ is injective (as seen above), then φ is also injective. This gives the result after some care. ■

Corollary 5.52. Fix $\varphi : R[\![x]\!] \to R[\![x]\!]$ some morphism. Further, find $f \in (x)$ such that $f \equiv x \pmod{x^2}$. Then if $\varphi(x) = f$ and $\varphi(r) = r$ for $r \in R$, then φ is an isomorphism.

Proof. Use the previous lemma to construct φ and then run the previous surjectivity and injectivity check. ■

Remark 5.53. In fact, there is an explicit inverse map for this φ.

We are now ready to prove Theorem 5.46.

Proof of Theorem 5.46. We use Newton's lemma to build our solution b. For ease of mind, we set $e := f'(a)$ so that we know

$$f(a) \equiv 0 \pmod{e^2 m}.$$

Now, we can write $f(a + ex)$, which upon expansion via the binomial theorem looks like

$$f(a + ex) = f(a) + f'(a)ex + h(x)(ex)^2$$

for some $h \in R[x]$. Using $f'(a) = e$, we get

$$f(a + ex) = f(a) + e^2\left(x + x^2 h(x)\right).$$

Now, consider the homomorphism $\varphi : R[\![x]\!] \to R[\![x]\!]$ by $\varphi(x) := x + x^2 h(x)$, but the previous corollary tells us that φ is an isomorphism! So we see

$$f\left(a + e\varphi^{-1}(x)\right) = f(a) + e^2 x$$

by plugging in. To finish, we build $\psi : R[\![x]\!] \to R$ by $\psi(x) = -c$, where $f(a) = e^2 c$ and can compute that

$$f\left(a + e\psi\varphi^{-1}(x)\right) = f(a) - e^2 c = 0,$$

which finishes. ■

Remark 5.54. We can show that the solution above is unique, provided that $f'(a)$ is not a zero-divisor. We will omit this proof.

5.3 March 15

Today's notes were transcribed from Miles's notes of the class. Thank you, Miles! We are finishing up completions today.

5.3.1 Idempotents

We recall the following definitions.

Definition 5.55 (Idempotent)**.** Fix a ring R. An element $e \in R$ is *idempotent* if and only if $e^2 = e$.

Remark 5.56. Equivalently, $e \in R$ is idempotent if and only if e is a root of the polynomial $f(x) = x^2 - x$.

Remark 5.57. If $e \in R$ is idempotent, then we can give Re a ring structure, where the addition and multiplication are inherited from R. In particular, we are closed under addition as $re + se = (r+s)e$, and we are closed under multiplication as $re \cdot se = rse^2 = (rs)e$.

However, our identity element is now e, which works because $e \cdot re = re \cdot e = re^2 = re$ for any $re \in Re$. The coherence (commutativity, associativity, distributivity, etc.) checks are all inherited directly from R.

Example 5.58. If $e \in E$ is an idempotent, then $1-e$ is also an idempotent: we can directly compute

$$(1-e)^2 = 1 - e - e + e^2 = 1 - e - e + e = 1 - e.$$

Lemma 5.59. Fix e an idempotent of a ring R. Then $R \cong Re \times R(1-e)$.

Proof. This was on the homework. ■

We will want to lift idempotents, but we will want to keep track of a little more data.

Definition 5.60 (Orthogonal idempotents)**.** Fix R a ring. Then a set $E \subseteq R$ of idempotents of R is *orthogonal* if and only if $ee' = 0$ for any two distinct $e, e' \in E$.

Example 5.61. Fix $e \in R$ an idempotent. Then the elements $\{e, 1-e\}$ are orthogonal. In particular, these are orthogonal because

$$e(1-e) = e - e^2 = e - e = 0.$$

Here are some reasons to care about orthogonal idempotents. For one, they give more idempotents.

Lemma 5.62. Fix R a ring and $E \subseteq R$ any finite set of orthogonal idempotents. Then

$$\sum_{e \in E} e$$

is another idempotent.

Proof. This is a direct computation. For concreteness, enumerate $E = \{e_1, \ldots, e_n\}$. Then we can compute

$$\left(\sum_{k=1}^n e_k\right)\left(\sum_{\ell=1}^n e_\ell\right) = \sum_{k,\ell=1}^n e_k e_\ell = \sum_{k=1}^n e_k e_k + \sum_{\substack{k,\ell=1 \\ k \neq \ell}}^n e_k e_\ell.$$

In particular, we note that $e_k^2 = e_k$ for each k because E is only made of idempotents. Further, $e_k e_\ell = 0$ for any $k \neq \ell$ because E is made of orthogonal idempotents. It follows that

$$\left(\sum_{k=1}^n e_k\right)^2 = \sum_{k=1}^n e_k,$$

which is what we wanted. ■

The above lemma is in fact detecting a larger ring decomposition, generalizing Lemma 5.59.

Lemma 5.63. Fix R a ring and $E \subseteq R$ a finite set of orthogonal idempotents such that

$$\sum_{e\in E} e = 1.$$

Then

$$\bigoplus_{e\in E} Re \cong R$$

by taking $(r_e e)_{e\in E}$ to $\sum_{e\in E} r_e e$.

Proof. Let $\varphi : (r_e e)_{e\in E} \mapsto \sum_{e\in E} r_e e$ be the map in question. We have the following checks on φ; let $(r_e e)_{e\in E}$ and $(s_e e)_{e\in E}$ be elements of $\bigoplus_{e\in E} Re$.

- Additive: we note that

$$\varphi\left((r_e e)_{e\in E} + (s_e e)_{e\in E}\right) = \varphi\left(((r_e + s_e)e)_{e\in E}\right) = \sum_{e\in E}(r_e + s_e)e = \varphi\left((r_e)_{e\in E}\right) + \varphi\left((s_e)_{e\in E}\right).$$

- Multiplicative: we note that

$$\varphi\left((r_e e)_{e\in E} \cdot (s_e e)_{e\in E}\right) = \varphi\left((r_e s_e e)_{e\in E}\right) = \sum_{e\in E} r_e s_e e.$$

  However,

$$\varphi\left((r_e)_{e\in E}\right)\varphi\left((s_e)_{e\in E}\right) = \left(\sum_{e\in E} r_e e\right)\left(\sum_{e'\in E} s_{e'} e'\right) = \sum_{e=e'\in E} r_e s_{e'} e' + \sum_{\substack{e,e'\in E\\ e\neq e'}} r_e s_{e'} ee'.$$

  The left sum here evaluates term-wise as $r_e s_e e^2 = r_e s_e e$, and the right sum here evaluates term-wise as $r_e s_{e'} ee' = 0$ because E is made of orthogonal idempotents (!). So we are done.

- Identity: we note that

$$\varphi\left((1e)_{e\in E}\right) = \sum_{e\in E} e = 1$$

  by hypothesis.

- Injective: if an element $(r_e e)_{e\in E} \in \ker\varphi$, then we see that

$$\sum_{e\in E} r_e e = 0$$

  by definition. Now, fixing any $e' \in E$, we note that $r_e ee' = 0$ for any $e \neq e'$ because E is made of orthogonal idempotents; however, when $e = e'$, we have $r_e ee' = r_e e^2 = r_e e$. As such, we see

$$r_{e'} e' = e' \cdot \sum_{e\in E} r_e e = e' \cdot 0 = 0,$$

  so $r_{e'} e' = 0$ for any $e' \in E$. Thus, $(r_e e)_{e\in E}$ is the zero element.

- Surjective: for any $r \in R$, we note that

$$\varphi\left((re)_{e\in E}\right) = \sum_{e\in E} re = r\sum_{e\in E} e = r \cdot 1 = r,$$

  so we are done.

The above checks finish showing that φ is an isomorphism of rings. ■

The condition that the orthogonal idempotents sum to 1 might look limiting, but it really is not so bad.

Lemma 5.64. Fix R a ring and $E \subseteq R$ a finite set of idempotents. Then

$$1 - \sum_{e \in E} e$$

is another idempotent, orthogonal from the rest of E.

Proof. By Lemma 5.62, $\sum_{e \in E} e$ is an idempotent. By Example 5.58, $1 - \sum_{e \in E} e$ is an idempotent.

It remains to show that this idempotent is orthogonal to E. Well, fixing any $e' \in E$, we note that

$$e' \cdot \sum_{e \in E} e = \sum_{e \in E} ee'.$$

If $e = e'$, then $ee' = (e')^2 = e'$; else if $e \neq e'$, then $ee' = 0$ because E consists of orthogonal idempotents. So the sum collapses to

$$e' \left(1 - \sum_{e \in E} e\right) = e' - e' \sum_{e \in E} e = e' - e' = 0.$$

This finishes. ■

As such, given any set of orthogonal idempotents, E, we can just add in the idempotent

$$1 - \sum_{e \in E} e$$

to get a new larger set of orthogonal idempotents, from which we can use Lemma 5.63.

5.3.2 Lifting Idempotents

With that definition out of the way, here is our main statement.

Proposition 5.65. Fix a Noetherian, local ring R complete with respect to its maximal ideal $\mathfrak{m}$. Further, take A to be a finite R-algebra (not necessarily commutative!), and pick up a finite set of orthogonal idempotents

$$\overline{E} \subseteq A/\mathfrak{m}A.$$

Then each idempotent $\overline{e} \in \overline{E}$ can be lifted to an idempotent $e \in E$ such that the set of lifts remains an orthogonal

Proof. We divide the proof into two cases. We start with the case where A is a commutative ring. Our starting step is to reduce to the case where $R = A$. Indeed, note that A is complete with respect to the ideal $\mathfrak{m}A$ because

$$\widehat{A}_{\mathfrak{m}A} \cong \widehat{R}_{\mathfrak{m}} \otimes_R A = R \otimes_R A = A,$$

where we are using the tensor-product characterization of the completion; notably, $\widehat{R}_{\mathfrak{m}} = R$ because R is complete with respect to $\mathfrak{m}$. Because A is now complete with respect to an ideal $\mathfrak{m}A$, we might as well ignore R. In particular, A is local with maximal ideal $\mathfrak{m}A$ and Noetherian as a finite algebra over a Noetherian ring.

Now, suppose that we have an idempotent $\overline{e} \in A/\mathfrak{m}A$, and let $e_0 \in A$ be any representative. Set $f(x) := x^2 - x$, and we will use Hensel lifting. In particular,

$$f(e_0) = e_0^2 - e_0 \equiv \overline{e}^2 - \overline{e} \equiv 0 \pmod{\mathfrak{m}},$$

and

$$(f'(e_0))^2 = (2e_0 - 1)^2 = 4\left(e_0^2 - e_0\right) + 1 \equiv 1 \pmod{\mathfrak{m}},$$

so we may use Hensel's lemma to lift $\overline{e}$ to an element $e \in A$ such that $e \equiv e_0 \equiv \overline{e} \pmod{\mathfrak{m}}$ and $f(e) = e^2 - e = 0$.

It remains to preserve orthogonality. For concreteness, enumerate $\overline{E}$ by $\{\overline{e_1}, \ldots, \overline{e_n}\} \subseteq A/\mathfrak{m}A$, which we lift to $\{e_1, \ldots, e_n\} \subseteq A$. Now, for $k \neq \ell$, we need to show that $e_k e_\ell = 0$. Well,

$$e_k e_\ell \equiv \overline{e_k} \cdot \overline{e_\ell} \equiv 0 \pmod{\mathfrak{m}}$$

because the $\overline{e_\bullet}$ are orthogonal. However, we can do better than this because we have idempotents: for any $d \in \mathbb{N}$, we see that

$$e_k e_\ell = e_k^d e_\ell^d = (e_k e_\ell)^d \in \mathfrak{m}^d.$$

Notably, this is the point where we are crucially using the fact that A is commutative: we need $e_k^d e_\ell^d = (e_k e_\ell)d$. Anyways, it follows that

$$e_k e_\ell \in \bigcap_{\mathfrak{m}} \mathfrak{m}^d.$$

By the Krull intersection theorem (recall A is a Noetherian local ring), we conclude that $e_k e_\ell = 0$.

We now add on the case where A is not commutative, by reducing to the commutative case. We proceed by induction on $\#E$. For example, if $\#\overline{E} = 1$, then we can still lift our idempotent from A upwards as discussed above, and the ring $R[e]$ is commutative, so we can directly reduce to the commutative case.

More generally, suppose that we have orthogonal idempotents $\{\overline{e_1}, \ldots, \overline{e_n}\} \subseteq A/\mathfrak{m}A$. By the inductive hypothesis, we can lift the first $n-1$ of these to orthogonal idempotents

$$\{e_1, \ldots, e_{n-1}\} \subseteq A.$$

Now, we add in the last idempotent by hand: set

$$f \coloneqq 1 - \sum_{i=1}^{n-1} e_i$$

so that $\{e_1, \ldots, e_{n-1}, f\}$ is a set of orthogonal idempotents. With this "auxiliary" idempotent, we finish by taking any representative $e_n' \in A$ of $\overline{e_n}$ and then lift $f e_n f$ in the commutative case $R[e_1, \ldots, e_{n-1}, f e_n' f]$. This lifted idempotent e_n will work. ■

Being able to lift idempotents gives us the following ring decomposition, akin to Lemma 5.59.

Lemma 5.66. Fix R a Noetherian local ring complete with respect to its maximal ideal $\mathfrak{m}$. Further, given a finite (commutative) R-algebra A, we have that A has only finitely many maximal ideals $\{\mathfrak{m}_1, \ldots, \mathfrak{m}_n\}$, and

$$A \cong \prod_{k=1}^{n} A_{\mathfrak{n}_k}$$

Notably, $A_{\mathfrak{m}_k}$ is a localization.

Proof. The point is to use the Artinian decomposition from our discussion of modules of finite length and then lift by appealing to idempotents. Namely, $A/\mathfrak{m}A$ is a finite-dimensional $R/\mathfrak{m}$-vector space, so $A/\mathfrak{m}A$ is an Artinian ring. In particular, we can write

$$A/\mathfrak{m}A \cong \prod_{i=1}^{n} \overline{A_i},$$

where we are writing A_i as our product of the various localizations of $A/\mathfrak{m}A$. Because we have expressed $A/\mathfrak{m}A$ as a product of rings, we can identify the inclusion maps

$$\overline{A_i} \hookrightarrow A/\mathfrak{m}A$$

as taking 1 to some idempotent of $A/\mathfrak{m}A$, which we will call $\overline{e_i}$. For psychological reasons, we will identify $\overline{A_i}$ with its image (via the above inclusion map) in $A/\mathfrak{m}A$ so that $\overline{A_i} = (A/\mathfrak{m}A)\overline{e_i}$.

We now lift. Our idempotents $\{\overline{e_1}, \ldots, \overline{e_n}\}$ are orthogonal, so we can use our lifting to give us a set of orthogonal idempotents

$$\{e_1, \ldots, e_n\} \subseteq A$$

such that $e_1 \equiv \overline{e_1} \pmod{\mathfrak{m}}$. Then these orthogonal idempotents give rise to the ring decomposition

$$A = \prod_{i=1}^{n} A_i,$$

where $A_i = Ae$.

To finish, we need to show that A_i is a localization of A with respect to a maximal ideal. To be explicit, we claim that A_i is local with maximal ideal $\mathfrak{n}_i := A_i \cap \mathfrak{m}A$. For this, we note

$$\frac{R}{\mathfrak{n}_i \cap R} \subseteq \frac{A_i}{\mathfrak{n}_i A_i}$$

is an integral extension (in particular, finite), where $R/(\mathfrak{n}_i \cap R)$ is a field (as an extension of $R/\mathfrak{m}$). From here, we can realize A_i as a localization by setting

$$\mathfrak{m}_i = \prod_{j=1}^{i-1} A_i \times \mathfrak{n}_i \times \prod_{j=i+1}^{n} A_i.$$

Thus, we have forced A to be a product of the localizations of A, from which we conclude that we have found all of our maximal ideals. ■

5.3.3 The Cohen Structure Theorem

We end our discussion of completions with a few works on the Cohen structure theorem. Here is the statement.

Theorem 5.67 (Cohen structure)**.** Fix a Noetherian local ring R complete with respect to its maximal ideal $\mathfrak{m}$. Further, let $\kappa := R/\mathfrak{m}$ be the residue field; if R contains a field, then

$$R \cong \kappa\left[\!\left[x_1, \ldots, x_n\right]\!\right]/I$$

for some ideal $I \subseteq \kappa\left[\!\left[x_1, \ldots, x_n\right]\!\right]$.

Note that the condition that R contains its residue field k is necessary.

Non-Example 5.68. Take $R = \mathbb{Z}_p$ to be the ring of p-adic integers, which has residue field $k = R/\mathfrak{m} = \mathbb{Z}_p/p\mathbb{Z}_p \cong \mathbb{F}_p$. However, R does not contain $\mathbb{F}_p$ because R has characteristic 0.

We'll show Theorem 5.67 in the case where κ is perfect.

Proof of Theorem 5.67 when κ is perfect. Note that, if R contains any field K which surjects onto κ, then we can give $\mathfrak{m}$ generators $\{f_1, \ldots, f_n\}$ over R and then surjecting

$$\pi : K\left[\!\left[x_1, \ldots, x_n\right]\!\right] \twoheadrightarrow R$$

by lifting $K \twoheadrightarrow R/\mathfrak{m}$ and then sending $x_\bullet \mapsto f_\bullet$. From here, we can mod out by the kernel to get an isomorphism of the form

$$R \cong \frac{K\left[\!\left[x_1, \ldots, x_n\right]\!\right]}{\ker \pi},$$

which gives the desired map.

So it suffices to show that, if R contains any field, then R contains a field isomorphic to κ. Well, by modding out by $\mathfrak{m}$, we can at least be sure that the field which R contains can be embedded into κ, so we can build the extension

$$K \subseteq K(\{t_i : i \in I\}) \subseteq \kappa,$$

where $K \subseteq K(\{t_i : i \in I\})$ is a purely transcendental extension and $K(t_i : i \in I) \subseteq \kappa$ is a purely algebraic extension.

Now, the transcendental elements $t_i \in \kappa = R/\mathfrak{m}$ can be lifted arbitrarily to R, which induces an embedding $F \hookrightarrow R$, where F is some very large field. As such, we let K' be the maximal subfield of R which contains F. We would like to show that K' surjects onto κ when taken modulo $\mathfrak{m}$, which will finish by choosing our lifts carefully.

Well, let $\alpha \in \kappa \setminus K'$ be an element of κ such that $\kappa = K'(\alpha)$. However, we can lift the root α up to the root of some polynomial in R, which produces a strictly larger field than K'. This is a contradiction, so we must instead have $K' \twoheadrightarrow R/\mathfrak{m}$. This finishes. ■

Remark 5.69. We used separability at the end of the proof during our use of the Primitive element theorem.

THEME 6
INTRODUCTION TO DIMENSION

In this sense the algebraic geometers have never left paradise: There is no snake (that is, Peano curve) in the garden.

—David Eisenbud

6.1 March 15

We continue today's lecture by transitioning over to dimension theory.

6.1.1 Krull Dimension

Let's talk about some properties that we want out of our dimension. Here's a starting example.

Definition 6.1 (Dimension, vector spaces)**.** The dimension of a (finite-dimensional) vector space V is the length of a maximal chain of distinct subspaces

$$0 = V_0 \subsetneq V_1 \subsetneq \cdots \subsetneq V_n = V.$$

Remark 6.2. To see that these align, suppose that V is finite-dimensional so that the definition makes sense. Then we can give V a basis by choosing a vector from each $V_k \setminus V_{k-1}$. We will not check formally that this works.

What's impressive about this definition is that we have even managed to remove the data of the ground field of our vector space!

In analogy with this, we have the following algebraic definition of dimension.

Definition 6.3 (Krull dimension)**.** The *Krull dimension* of a ring R, denoted $\dim R$, is the supremum of the length r of a chain of distinct primes

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

Here are some examples to get used to this definition.

Example 6.4. Fields have dimension 0.

Example 6.5. In general, if a Noetherian ring R has $\dim R = 0$, then all primes are maximal, so we know from our discussion of modules of finite length that R is Artinian. In fact, we know R is Artinian if and only if all primes are maximal and R is Noetherian.

Example 6.6. If R is a principal ideal domain which is not a field, then we showed in our proof that principal ideal domains are unique factorization domains that all nonzero prime ideals are maximal. Thus, the largest possible chain in R takes the form

$$(0) \subsetneq \mathfrak{p} \subsetneq R,$$

so R has dimension 1.

Example 6.7. The ring $k[x]$ is a principal ideal domain and not a field and therefore has dimension 1. More generally,

$$\dim k[x_1, \ldots, x_n] = n,$$

but we will not prove this yet.

6.1.2 Motivating Dimension

One way to be convinced that Definition 6.3 is the right definition of dimension is to write down some axioms that we want out of our dimension and try to use these to characterize dimension. Here are some axioms that Eisenbud provides.

- We want dimension to be a property determined locally; for example, the dimension of the union of a plane and a line should be 2 because of the plane. Because localization and completions are intended to be ways to look very locally at a point (geometrically speaking), we ask for

$$\dim R = \sup_{\mathfrak{p} \in \operatorname{Spec} R} \dim R_\mathfrak{p} \qquad \text{and} \qquad \dim R_\mathfrak{p} = \dim \widehat{R}_\mathfrak{p}.$$

- We don't want to have to deal with nilpotent elements. In some sense, nilpotent elements correspond to differentials, but they shouldn't affect the dimension of our space. As such, if $I \subseteq R$ is a nilpotent ideal, we will require that

$$\dim(R/I) = \dim R.$$

- Small changes in our base ring should not affect the dimension either. For example, the rings k and $k[x]/\left(x^2+1\right)$ should have the same dimension (they are, roughly speaking, just lines), even though the latter ring is certainly bigger in some sense. To codify this, if S is a finite R-algebra containing R, we will require that

$$\dim S = \dim R.$$

- We want the dimension of the coordinate ring of affine n-space to be n; additionally, the dimension should be uniform across all of n-space. So after taking completion at $(x_1, \ldots, x_n)$, this amounts to requiring

$$\dim k\llbracket x_1, \ldots, x_n \rrbracket = n.$$

It turns out that these properties completely characterize the dimension.

6.1.3 Other Characterizations

Here are some other characterizations of the dimension.

Theorem 6.8. Fix $R := k[x_1, \ldots, x_n]/\mathfrak{p}$ (i.e., R is a finitely generated k-algebra), where $\mathfrak{p} \subseteq k[x_1, \ldots, x_n]$ is a prime so that R is a domain. Then $\dim R$ is equal to the transcendence degree of $K(R)$ over k. In fact, in this case, $\dim R$ is the length of all maximal chains of distinct primes.

Note that the previous theorem is somewhat agnostic about the case where R is not an integral domain: for example, the ring

$$k[x] \times k[y, z],$$

which can be thought of the ring of functions of the (disjoint) union of a line and a plane. Indeed, in this disjoint union, we wouldn't even expect all maximal chains to have the same length because taking the union along the line should prevent us from being able to see the plane.

We can use the above result in a stronger sense to justify our axioms above.

Theorem 6.9 (Noether Normalization)**.** Fix $R := k[x_1, \ldots, x_n]/\mathfrak{p}$ (i.e., R is a finitely generated k-algebra), where $\mathfrak{p} \subseteq k[x_1, \ldots, x_n]$ is a prime so that R is a domain. Further, fix

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

a maximal chain of primes. Then there exists a subring $S \subseteq R$ such that $S \cong k[x_1, \ldots, x_n]$ and $\mathfrak{p}_k \cap S = (x_1, \ldots, x_k)$.

In particular, finitely generated k-algebras have their dimension intimately connected with some finite subring, akin to our third axiom.

We close with a more computational way to look at the dimension. Recall that if R is a local Noetherian ring with maximal ideal $\mathfrak{m}$, then we can define its Hilbert function by

$$H_R(n) := \dim_{R/\mathfrak{m}} \mathfrak{m}^n/\mathfrak{m}^{n+1},$$

which we know to be equal to a polynomial P_R for sufficiently large values of n. Then the following is true.

Theorem 6.10. Fix R a local Noetherian ring. Then $\dim R = 1 + \deg P_R$.

We can be convinced of this by running the example $R = k\llbracket x_1, \ldots, x_n \rrbracket$.

6.2 March 17

We're back, y'all.

6.2.1 A Quick Exercise

Let's start with an exercise, to review for the midterm. Recall the following result.

Lemma 6.11 (Eisenbud 6.4)**.** Fix R a ring and $S := R[x_1, \ldots, x_n]/(f)$, where f is some polynomial. Then S is a flat R-algebra if and only if $\operatorname{cont} f = R$.

Proof. This was on the homework. ■

And here is our exercise.

Exercise 6.12. Fix $R := k[x,y]$ with maximal ideal $\mathfrak{m} := (x,y)$, and we consider the blow-up ring

$$S := \mathrm{B}_{\mathfrak{m}} R := R \oplus \mathfrak{m} \oplus \mathfrak{m}^2 \oplus \cdots .$$

Now, we ask if S is a flat R-module.

Proof. Heuristically, the fiber at any point except for $(0,0)$ is a point, but the fiber over $(0,0)$ is the full projective line. So these fibers are pretty poorly behaved, so we expect this to not be a flat module.

Well, by staring hard at our grading, we see that

$$S \cong k[x,y,tx,ty] \cong \frac{k[x,y,z,w]}{(yz-xw)},$$

where the point is that we induce the right-hand isomorphism by $tx \mapsto z$ and $ty \mapsto w$. As such, we see that this module is not flat because the polynomial $f(z,w) = yz - xw$ has coefficients which generate $\operatorname{cont}(f) = (x,y) \neq R$. In particular, we have "detected" the fiber over the origin. ■

6.2.2 The Krull Dimension

Warning 6.13. For effectively the rest of the course, all of our rings will be Noetherian. This hypothesis will only occasionally be stated.

Recall the following definition.

Definition 6.3 (Krull dimension)**.** The *Krull dimension* of a ring R, denoted $\dim R$, is the supremum of the length r of a chain of distinct primes

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

This gives rise to the following definitions.

Definition 6.14 (Krull dimension, ideals)**.** Fix a ring R and an ideal $I \subseteq R$. Then we define the *dimension* of an ideal I to be $\dim I := \dim R/I$.

Definition 6.15 (Codimension)**.** Fix I a proper ideal of a ring R.

- If $I = \mathfrak{p}$ is a prime ideal of R, then we define the *codimension* as $\operatorname{codim} \mathfrak{p} := \dim R_{\mathfrak{p}}$.
- More generally, we define the *codimension* as

  $$\operatorname{codim} I := \min_{\mathfrak{p} \supseteq I} \operatorname{codim} \mathfrak{p},$$

  where the minimum is over all prime ideals $\mathfrak{p}$ containing I.

We quickly check the well-definedness of these definitions. To start, we give more hands-on characterizations of these definitions.

Lemma 6.16. Fix an ideal I of a ring R. Then $\dim I$ is equal to the length of the longest chain of primes

$$I \subseteq \mathfrak{p}_0 \subsetneq \mathfrak{p}_1 \subsetneq \cdots \subsetneq \mathfrak{p}_d$$

in R.

Proof. Let $\pi : R \twoheadrightarrow R/I$ be the natural projection. In one direction, suppose that

$$I \subseteq \mathfrak{p}_0 \subsetneq \mathfrak{p}_1 \subsetneq \cdots \subsetneq \mathfrak{p}_d$$

is the longest possible such chain of primes in R. Then, projecting down via π, we get a chain

$$\pi\mathfrak{p}_0 \subseteq \pi\mathfrak{p}_1 \subseteq \cdots \subseteq \pi\mathfrak{p}_d. \tag{1}$$

We have two checks.

- If $\mathfrak{p}$ is a prime ideal containing I, then we claim $\pi\mathfrak{p}$ is also a prime ideal. Indeed, if $(a+I)(b+I) \in \pi\mathfrak{p}$ implies $ab + I \in \pi\mathfrak{p}$ implies $ab + x \in \mathfrak{p}$ for some $x \in I$ implies $ab \in \mathfrak{p}$ because $I \subseteq \mathfrak{p}$.

  Thus, because $\mathfrak{p}$ is prime, $a \in \mathfrak{p}$ or $b \in \mathfrak{p}$, so $a + I \in \pi\mathfrak{p}$ or $b + I \in \pi\mathfrak{p}$.

- If $I_1 \subsetneq I_2$ are distinct ideals containing I, then we claim $\pi(I_1) \subsetneq \pi(I_2)$. Indeed, we claim that $\pi(I_1) = \pi(I_2)$ would imply $I_1 = I_2$; by symmetry, it suffices to show that $\pi(I_1) \subset \pi(I_2)$ implies $I_1 \subseteq I_2$.

  Well, fix any $a \in I_1$. Then $\pi(a) \in \pi(I_1) \subseteq \pi(I_2)$, so $a + I \in \pi(I_2)$, so there exists $b \in I_2$ such that

  $$a + I = b + I.$$

  Then $a - b \in I \subseteq I_2$, so $a \in b + I_2 = I_2 + I_2 = I_2$. Thus, $I_1 \subseteq I_2$.

  By symmetry, we see that $\pi(I_2) \subseteq \pi(I_1)$ implies $I_2 \subseteq I_1$ as well. Thus, $\pi(I_1) = \pi(I_2)$ implies both $\pi(I_1) \subseteq \pi(I_2)$ and $\pi(I_2) \subseteq \pi(I_1)$ and so $I_1 \subseteq I_2$ and $I_2 \subseteq I_1$, giving $I_1 = I_2$.

Thus, (1) provides a chain of distinct primes in R/I, so $d \le \dim R/I$.

In the other direction, suppose that we have chosen our largest possible chain of distinct primes

$$\mathfrak{p}_0 \subsetneq \mathfrak{p}_1 \subsetneq \cdots \subsetneq \mathfrak{p}_{\dim R/I}$$

in R/I. Pulling backwards, we get a chain of primes

$$\pi^{-1}\mathfrak{p}_0 \subseteq \pi^{-1}\mathfrak{p}_1 \subseteq \cdots \subseteq \pi^{-1}\mathfrak{p}_{\dim R/I}. \tag{2}$$

Notably, $(0) \subseteq \mathfrak{p}_k$ for each prime $\mathfrak{p}_k \subseteq R/I$ above, so $I = \pi^{-1}(0) \subseteq \pi^{-1}\mathfrak{p}_k$ for each prime $\pi^{-1}\mathfrak{p}_k$, so all these primes contain I.

Additionally, we check that distinct R/I-ideals $I_1 \ne I_2$ will have $\pi^{-1}(I_1) \ne \pi^{-1}(I_2)$. Indeed, we claim that $\pi^{-1}(I_1) = \pi^{-1}(I_2)$ implies $I_1 = I_2$. To see this, we show $\pi^{-1}(I_1) \subseteq \pi^{-1}(I_2)$ implies $I_1 \subseteq I_2$. Well, pick up $a + I \in I_1$ so that $\pi(a) \in I_1$, implying

$$a \in \pi^{-1}(I_1) \subseteq \pi^{-1}(I_2)$$

and hence $a + I = \pi(a) \in I_2$ as well.

Now, by symmetry, we see that $\pi^{-1}(I_2) \subseteq \pi^{-1}(I_1)$ will also imply $I_2 \subseteq I_1$, so when we have both in the equality $\pi^{-1}(I_1) = \pi^{-1}(I_2)$, we will have both $I_1 \subseteq I_2$ and $I_2 \subseteq I_1$. Thus, $I_2 = I_2$.

In total, (2) now provides us with a chain of $\dim R/I$ distinct primes above I in R, showing that $\dim R/I \le d$. This finishes the proof, for we now have $d = \dim R/I$. ■

Lemma 6.17. Fix a prime ideal $\mathfrak{p}$ of a ring R. Then $\operatorname{codim}\mathfrak{p}$ is equal to the length of the longest chain of primes

$$\mathfrak{p}_0 \subsetneq \mathfrak{p}_1 \subsetneq \cdots \subsetneq \mathfrak{p}_d = \mathfrak{p},$$

where $\mathfrak{p}$ is included in the chain; i.e., $\operatorname{codim}\mathfrak{p} = d$ here.

Proof. Let $\iota : R \to R_\mathfrak{p}$ denote the natural inclusion. In one direction, suppose that

$$\mathfrak{p}_0 \subsetneq \mathfrak{p}_1 \subsetneq \cdots \subsetneq \mathfrak{p}_d = \mathfrak{p}$$

is the longest possible chain of distinct prime ideals below $\mathfrak{p}$. Notably, none of these primes have intersection with $R \setminus \mathfrak{p}$ because they are contained in $\mathfrak{p}$, so Theorem 2.29 (combined with Lemma 2.27 to give the inverse map) tells us that we have a chain of primes

$$\mathfrak{p}_0 R_\mathfrak{p} \subsetneq \mathfrak{p}_1 R_\mathfrak{p} \subsetneq \cdots \subsetneq \mathfrak{p}_d R_\mathfrak{p} = \mathfrak{p} R_\mathfrak{p}.$$

By the bijection of Theorem 2.29, we are getting an ascending chain of distinct primes, so we see $\dim R_\mathfrak{p} \ge d$, as needed

In the other direction, suppose that we have chain of distinct primes

$$\mathfrak{q}_0 \subsetneq \mathfrak{q}_1 \subsetneq \cdots \subsetneq \mathfrak{q}_{\operatorname{codim}\mathfrak{p}}.$$

Notably, $R_\mathfrak{p}$ is a local ring with maximal ideal $\mathfrak{p}R_\mathfrak{p}$, so if the prime $\mathfrak{q}_{\operatorname{codim}\mathfrak{p}}$ is not equal to $\mathfrak{p}R_\mathfrak{p}$, then $\mathfrak{q}_{\operatorname{codim}\mathfrak{p}} \subsetneq \mathfrak{p}R_\mathfrak{p}$, allowing us to add an extra prime to the list and violating the definition of $\operatorname{codim}\mathfrak{p} = \dim R_\mathfrak{p}$. So we must have $\mathfrak{q}_{\operatorname{codim}\mathfrak{p}} = \mathfrak{p}R_\mathfrak{p}$.

Now, applying Theorem 2.29 once more, we get a chain of primes

$$\iota^{-1}\mathfrak{q}_0 \subsetneq \iota^{-1}\mathfrak{q}_1 \subsetneq \cdots \subsetneq \iota^{-1}\mathfrak{q}_{\operatorname{codim}\mathfrak{p}} = \iota^{-1}(\mathfrak{p}R_\mathfrak{p}),$$

which remain distinct by our bijection. In particular, $\iota^{-1}\mathfrak{q}_{\operatorname{codim}\mathfrak{p}} = \iota^{-1}(\mathfrak{p}R_\mathfrak{p}) = \mathfrak{p}$ because $\iota^{-1} : I \mapsto \iota^{-1}I$ is inverse to $I \mapsto IR_\mathfrak{p}$ by Lemma 2.27.

Thus, we see that we have exhibited a chain of $\operatorname{codim}\mathfrak{p}$ primes below $\mathfrak{p}$, so we see that $\dim R_\mathfrak{p} \le d$ as well. Combining with our previous inequality, we are done. ■

Lemma 6.18. Fix an ideal I of a ring R. The two definitions of codimension of an ideal coincide when I is a prime ideal.

Proof. For this proof, we will ignore the second definition when discussing codimension of a prime ideal. We need to show that

$$\operatorname{codim} I = \min_{\mathfrak{p}\supseteq I} \operatorname{codim}\mathfrak{p}$$

and in particular that one is finite when the other is finite.

In one direction, note that $I \supseteq I$ implies that

$$\operatorname{codim} I \ge \min_{\mathfrak{p}\supseteq I} \operatorname{codim}\mathfrak{p}$$

because the ideal I is contained in the ideal. In the other direction, we note that we can find a chain of primes

$$\mathfrak{p}_0 \subsetneq \mathfrak{p}_1 \subsetneq \cdots \subseteq \mathfrak{p}_{\operatorname{codim} I - 1} \subsetneq I$$

by Lemma 6.17. As such, by tacking on the prime $\mathfrak{p} \supseteq I$ to the end, we get a chain of length at least $\operatorname{codim} I$ distinct primes descending from $\mathfrak{p}$, so Lemma 6.17 again tells us that

$$\operatorname{codim}\mathfrak{p} \ge \operatorname{codim} I.$$

It follows that $\min_{\mathfrak{p}\supseteq I}\mathfrak{p} \ge \operatorname{codim} I$, and this inequality finishes the proof. ■

These results give us the following proposition, which finishes our well-definedness checks.

Proposition 6.19. Fix a ring R such that $\dim R$ is finite. Then, for any proper ideal I, both $\dim I$ and $\operatorname{codim} I$ are finite.

Proof. We prove the statements in steps.

- We show that $\dim I$ is finite. Well, by Lemma 6.16, we note that $\dim I$ is equal to the length of the longest possible chain of distinct primes
$$I \subseteq \mathfrak{p}_0 \subsetneq \mathfrak{p}_1 \subsetneq \cdots \subsetneq \mathfrak{p}_d.$$
However, ignoring the I and viewing this as a chain of distinct primes in R, we see that $d \leq \dim R$ is forced, and in particular, $\dim I$ must be finite.

- We show that $\operatorname{codim} \mathfrak{p}$ is finite when $\mathfrak{p}$ is a prime ideal. By Lemma 6.17, we note that $\operatorname{codim} \mathfrak{p}$ is equal to the length of the longest possible chain of distinct primes
$$\mathfrak{p}_0 \subsetneq \mathfrak{p}_1 \subsetneq \cdots \subsetneq \mathfrak{p}_d = \mathfrak{p}.$$
Again ignoring the $\mathfrak{p}$ at the end and viewing this as a chain of distinct primes in R, we see that $d \leq \dim R$ is forced, and in particular, $\operatorname{codim} \mathfrak{p}$ must be finite.

- We show that $\operatorname{codim} I$ is finite when I is any ideal. Well, we note that I is contained in some maximal and hence prime ideal because I is proper, so
$$\{\operatorname{codim} \mathfrak{p} : \mathfrak{p} \supseteq I\}$$
is nonempty and only contains natural numbers by our previous checks. So the well-ordering of $\mathbb{N}$ promises us that we have a minimum, finishing. ■

As a reward for all of our hard work, we note that we have the following nice result: dimension can be computed locally.

Theorem 6.20. Fix a ring R. Then
$$\dim R = \max_{\mathfrak{p} \in \operatorname{Spec} R} \dim R_{\mathfrak{p}}.$$

Proof. The point is to use Lemma 6.17.

By Lemma 6.17, we see that $\dim R_{\mathfrak{p}} = \operatorname{codim} \mathfrak{p}$ is equal to the length of the largest chain of distinct primes below $\mathfrak{p}$ in R. Because such a chain of primes below $\mathfrak{p}$ is still a chain of primes in R, we conclude $\operatorname{codim} \mathfrak{p} \leq \dim R$ for each prime $\mathfrak{p}$. Thus,
$$\max_{\mathfrak{p} \in \operatorname{Spec} R} \dim R_{\mathfrak{p}} \leq \dim R.$$
In the other direction, we know that we have a chain of distinct primes
$$\mathfrak{p}_0 \subsetneq \mathfrak{p}_1 \subsetneq \cdots \subsetneq \mathfrak{p}_{\dim R}$$
in R. But this is a chain of distinct primes below $\mathfrak{p}_{\dim R}$, so we conclude $\operatorname{codim} \mathfrak{p}_{\dim R} \geq \dim R$ by Lemma 6.17. Thus,
$$\max_{\mathfrak{p} \in \operatorname{Spec} R} \dim R_{\mathfrak{p}} \geq \operatorname{codim} \mathfrak{p}_{\dim R} \geq \dim R.$$
Combining with the previous inequality, we are done. ■

6.2.3 Bounds on Dimension

With our checks out of the way, here are some examples.

Example 6.21. Fix $R := \mathbb{Z}$, which has $\dim \mathbb{Z} = 1$. Then $\operatorname{codim}(0) = \dim \mathbb{Z}_{(0)} = \dim \mathbb{Q} = 0$; in fact, $\dim(0) = 1$.

Example 6.22. Similarly, if p is a positive prime, one can show that

$$\operatorname{codim}(p) = \dim \mathbb{Z}_p = 1$$

by showing that $\mathbb{Z}_p$ is a principal ideal domain whose principal ideals take the form $(p^\bullet)$. On the other hand, $\dim(p) = \dim \mathbb{Z}/p\mathbb{Z} = 0$ because $\mathbb{Z}/p\mathbb{Z}$ is a field.

In all these examples, we see that

$$\dim \mathfrak{p} + \operatorname{codim} \mathfrak{p} \stackrel{?}{=} \dim R.$$

This equality need not hold in general, as we will show in a second, but we do have the following.

Proposition 6.23. Fix $\mathfrak{p}$ a prime ideal of a ring R. Then

$$\dim \mathfrak{p} + \operatorname{codim} \mathfrak{p} \le \dim R.$$

Proof. By Lemma 6.17, we have a chain of distinct primes

$$\mathfrak{p}_0 \subsetneq \mathfrak{p}_1 \subsetneq \cdots \subsetneq \mathfrak{p}_{\operatorname{codim} \mathfrak{p}} = \mathfrak{p}.$$

Similarly, by Lemma 6.16, we have a chain of distinct primes

$$\mathfrak{p} \subseteq \mathfrak{q}_0 \subsetneq \mathfrak{q}_1 \subsetneq \cdots \subseteq \mathfrak{q}_{\dim \mathfrak{p}}.$$

By maximality, we note that we need $\mathfrak{p} = \mathfrak{q}_0$, lest we be able to make this chain longer by taking on $\mathfrak{p} \subsetneq \mathfrak{q}_0$ at the front. As such, we can zipper our two chains together into a long chain

$$\mathfrak{p}_0 \subsetneq \mathfrak{p}_1 \subsetneq \cdots \subsetneq \mathfrak{p}_{\operatorname{codim} \mathfrak{p}} = \mathfrak{p} = \mathfrak{q}_0 \subsetneq \mathfrak{q}_1 \subsetneq \mathfrak{q}_2 \subsetneq \cdots \subsetneq \mathfrak{q}_{\dim \mathfrak{p}}.$$

This chain has length $\operatorname{codim} \mathfrak{p} + \dim \mathfrak{p}$, which must be less than or equal to $\dim R$ because we have constructed a chain of distinct primes in R. This finishes. ■

Remark 6.24. Equality in Proposition 6.23 holds for affine domains (i.e., the ring of functions over a reduced variety).

Here is another useful lemma.

Lemma 6.25. Fix ideals I and J in a ring R. If $I \subseteq J$, then

$$\dim I \ge \dim J \qquad \text{and} \qquad \operatorname{codim} I \le \operatorname{codim} J.$$

Similarly, if $\mathfrak{p}$ and $\mathfrak{q}$ are primes with $\mathfrak{p} \subseteq \mathfrak{q}$, then $\operatorname{codim} \mathfrak{p} \le \operatorname{codim} \mathfrak{q}$, with equality if and only if $\mathfrak{p} = \mathfrak{q}$.

Proof. Roughly speaking, these follow directly from Lemma 6.16 and Lemma 6.17. We show them separately.

- From Lemma 6.16, we can find a chain of distinct primes
$$J \subseteq \mathfrak{p}_0 \subsetneq \mathfrak{p}_1 \subsetneq \cdots \subsetneq \mathfrak{p}_{\dim J}.$$
However, $I \subseteq J$, so replacing the J at the end I implies $\dim I$ is at least $\dim J$ by Lemma 6.16.

- We need to show that
$$\min_{\mathfrak{p}\supseteq I} \operatorname{codim} \mathfrak{p} \stackrel{?}{\leq} \min_{\mathfrak{p}\supseteq J} \operatorname{codim} \mathfrak{p}.$$
Well, there will exist some $\mathfrak{p}_0 \supseteq J$ for which $\operatorname{codim} I = \operatorname{codim} \mathfrak{p}_0$. But this prime $\mathfrak{p}_0$ also contains $I \subseteq J$, so
$$\min_{\mathfrak{p}\supseteq I} \operatorname{codim} \mathfrak{p} \leq \operatorname{codim} \mathfrak{p}_0 = \operatorname{codim} J,$$
finishing.

- Lastly, let $\mathfrak{p}$ and $\mathfrak{q}$ be primes with $\mathfrak{p} \subsetneq \mathfrak{q}$. By Lemma 6.17, we are promised a chain
$$\mathfrak{p}_0 \subsetneq \mathfrak{p}_1 \subsetneq \cdots \subsetneq \mathfrak{p}_{\operatorname{codim} \mathfrak{p}} = \mathfrak{p}.$$
Placing $\subsetneq \mathfrak{q}$ at the end of this chain gives $\operatorname{codim} \mathfrak{p} + 1 \leq \operatorname{codim} \mathfrak{q}$, finishing.

Thus, we have shown the desired inequalities. ■

For the sake of examples, we pick up the following computation.

Lemma 6.26. Fix rings R_1 and R_2, and let $\pi_1 : R_1 \times R_2 \to R_1$ and $\pi_1 : R_1 \times R_2 \to R_2$ be the natural projections. If $\mathfrak{p} \subseteq R_1 \times R_2$ is a prime ideal, then one of the following is true.

- $\mathfrak{p} = \pi_1\mathfrak{p} \times R_2$, and $\pi_1\mathfrak{p}$ is prime.
- $\mathfrak{p} = R_1 \times \pi_2\mathfrak{p}$, and $\pi_2\mathfrak{p}$ is prime.

Conversely, if $\mathfrak{p}_1 \subseteq R_1$ is prime, then $\mathfrak{p}_1 \times R_2 \subseteq R_1 \times R_2$ is a prime. Similarly, if $\mathfrak{p}_2 \subseteq R_2$ is prime, then $R_1 \times \mathfrak{p}_2 \subseteq R_1 \times R_2$ is prime.

Proof. We start with the first statement; let $\mathfrak{p} \subseteq R_1 \times R_2$ be prime. Note that $(0,1)\cdot(1,0) = (0,0) \in \mathfrak{p}$, so primality forces $(0,1) \in \mathfrak{p}$ or $(1,0) \in \mathfrak{p}$. By swapping R_1 and R_2, we may say (without loss of generality) that $(0,1) \in \mathfrak{p}$ and show that $\mathfrak{p} = \pi_1\mathfrak{p} \times R_2$. We will show the inclusions separately.

- We show $\mathfrak{p} \subseteq \pi_1\mathfrak{p} \times R_2$. Indeed, pick up $(a,b) \in \mathfrak{p}$. Then $a = \pi_1(a,b) \in \pi_1\mathfrak{p}$, so $(a,b) \in \pi_1\mathfrak{p} \times R_2$.

- We show $\pi_1\mathfrak{p} \times R_2 \subseteq \mathfrak{p}$. Indeed, pick up any $(a,b) \in \pi_1\mathfrak{p} \times R_2$. Because $a \in \pi_1\mathfrak{p}$, pulling back along π_1 promises some $b' \in R_2$ such that $(a,b') \in \mathfrak{p}$. But then we note that $(0,1) \in \mathfrak{p}$ implies that
$$(a,b') + (b-b')\cdot(0,1) = (a,b) \in \mathfrak{p}$$
as well, finishing.

Thus, $\mathfrak{p} = \pi_1\mathfrak{p} \times R_2$. It remains to show that $\pi_1\mathfrak{p}$ is prime. Well, if $a_1a_2 \in \pi_1\mathfrak{p}$, then $(a_1a_2, 0) \in \mathfrak{p}_1 \times R_2 = \mathfrak{p}$, so
$$(a_1,0)\cdot(a_2,0) \in \mathfrak{p}.$$
Thus, $(a_1,0) \in \mathfrak{p}$ or $(a_2,0) \in \mathfrak{p}$, so $a_1 \in \pi_1\mathfrak{p}$ or $a_2 \in \pi_1\mathfrak{p}$.

We now show the second part of the statement. On one hand, if $\mathfrak{p}_1 \subseteq R_1$ is prime, then we see immediately that $\pi_1^{-1}\mathfrak{p}_1 = \mathfrak{p}_1 \times R_2$ is prime. Similarly, if $\mathfrak{p}_2 \subseteq R_2$ is prime, then again we have that $\pi_2^{-1}\mathfrak{p}_2 = R_1 \times \mathfrak{p}_2$ is prime. ■

Corollary 6.27. Fix rings R_1 and R_2 with finite dimension. Then

$$\dim(R_1 \times R_2) = \max\{\dim R_1, \dim R_2\}.$$

Proof. We show the inequalities separately.

- We show $\dim(R_1 \times R_2) \geq \max\{\dim R_1, \dim R_2\}$. Indeed, we will show that $\dim(R_1 \times R_2) \geq \dim R_1$, and then swapping the roles of R_1 and R_2 will show that $\dim(R_1 \times R_2) \geq \dim R_2$ as well, finishing.

  Well, set $d := \dim R_1$, and suppose that we have a chain of primes

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

  in R_1. Then Lemma 6.26 gives us the chain of primes

  $$(\mathfrak{p}_0 \times R_2) \subseteq (\mathfrak{p}_1 \times R_2) \subseteq \cdots \subseteq (\mathfrak{p}_d \times R_2).$$

  Notably, these primes are still distinct because $a \in \mathfrak{p}_{k+1} \setminus \mathfrak{p}_k$ has $(a, 0) \in (\mathfrak{p}_{k+1} \times R_2) \setminus (\mathfrak{p}_k \times R_2)$. Thus, we have a chain of $\dim R_1$ distinct primes in $\dim(R_1 \times R_2)$, so $\dim(R_1 \times R_2) \geq \dim R_1$ follows.

- We show $\dim(R_1 \times R_2) \leq \max\{\dim R_1, \dim R_2\}$. Suppose that we have a chain of distinct primes

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

  in $R_1 \times R_2$. Our goal is to show that $d \leq \max\{\dim R_1, \dim R_2\}$. Now, Lemma 6.26 $\mathfrak{p}_0 \in \{\pi_1\mathfrak{p}_0 \times R_2, R_1 \times \pi_2\mathfrak{p}_0\}$, so without loss of generality, we will assume that $\mathfrak{p}_0 = \pi_1\mathfrak{p}_0 \times R_2$; otherwise, we can swap the roles of R_1 and R_2 everywhere. Notably, the quantity $\max\{\dim R_1, \dim R_2\}$ is symmetric in R_1 and R_2.

  However, this implies that $(0, 1) \in \pi_1\mathfrak{p}_0 \times R_2 = \mathfrak{p}_0$, so

  $$(0, 1) \in \pi_1\mathfrak{p}_k$$

  for each $\mathfrak{p}_k$. So, using the proof of Lemma 6.26, we see that this implies $\mathfrak{p}_k = \pi_1\mathfrak{p}_k \times R_2$ for all k. Thus, our chain of primes now looks like

  $$(\pi_1\mathfrak{p}_0 \times R_2) \subsetneq (\pi_1\mathfrak{p}_1 \times R_2) \subsetneq \cdots \subsetneq (\pi_1\mathfrak{p}_d \times R_2).$$

  In particular, applying π_1 gives us a chain of primes (by Lemma 6.26)

  $$\mathfrak{p}_0 \subseteq \mathfrak{p}_1 \subseteq \cdots \subseteq \mathfrak{p}_d$$

  in R_1. Now, we note distinctness: for any k, we see $(a, 0) \in (\pi_1\mathfrak{p}_{k+1} \times R_2) \setminus (\pi_2\mathfrak{p}_k \times R_2)$ implies that $a \in \pi_1\mathfrak{p}_{k+1}$. However, $a \in \pi_1\mathfrak{p}_k$ would imply that $(a, 0) \in \pi_1\mathfrak{p}_k \times R_2$, which is false, so instead we must have $a \in \mathfrak{p}_{k+1} \setminus \mathfrak{p}_k$, so the above chain is indeed made of distinct primes.

  Thus, $d \leq \dim R_1 \leq \max\{\dim R_1, \dim R_2\}$. This finishes.

Having shown both inequalities, we conclude $\dim(R_1 \times R_2) = \max\{\dim R_1, \dim R_2\}$. So we are done. ■

Remark 6.28. By induction, we see that any $n \in \mathbb{N}$ and rings $\{R_k\}_{k=1}^n$ will have

$$\dim \prod_{k=1}^n R_k = \max\{\dim R_k : 1 \leq k \leq n\}.$$

We won't talk about infinite products because they should mostly be infinite-dimensional. I don't think we have the machinery to talk about this here, but we refer to mo90980.

And here is an example computation.

Example 6.29. Let $R_1 := k[x]$ and $R_2 := k[x, y]$ and consider $R := k[x] \times k[y, z]$, which is the coordinate ring of the disjoint union of a line and a plane.

- Note $\dim R = \max\{1, 2\} = 2$ by Corollary 6.27.
- Any prime below $(x) \times R_2$ needs to have the form $\mathfrak{p} \times R_2$ (essentially by the argument above), but the only prime $\mathfrak{p}$ below (x) is (0) because $k[x]$ is a principal ideal domain, so all nonzero primes are maximal. Thus, $\operatorname{codim}((x) \times R_2) = 1$.
- Again, any prime above $(x) \times R_2$ needs to have the form $\mathfrak{p} \times R_2$, but (x) is a maximal ideal, so there is no such prime, so $\dim((x) \times R_2) = 0$.

Computing, we see that $\dim R = 2 > 1 + 0 = \operatorname{codim}((x) \times R_2) + \dim((x) \times R_2)$, manifesting the lack of equality in Proposition 6.23.

To close out our examples, we study the most basic affine sets: sets of points.

Proposition 6.30. Fix a nonzero Noetherian ring R.

(a) We have $\dim R = 0$ if and only if R is Artinian. In this case, R is the product of finitely many Artinian local rings.

(b) If X is an algebraic set, then $\dim A(X) = 0$ if and only if X is finite.

Proof. We go one at a time.

(a) A ring R is Artinian if and only if R is Noetherian and all primes are maximal by Theorem 2.126. As such, under the hypothesis that R is Noetherian, we see that R is Artinian if and only if all primes are maximal.

Now, all primes being maximal implies that we cannot build a chain of two distinct primes

$$\mathfrak{p} \subsetneq \mathfrak{q}$$

because $\mathfrak{p}$ would need to be prime and hence maximal; thus, we have $\dim R = 0$. (Note that R does have dimension 0 because R is nonzero and hence has a maximal ideal.)

And conversely, if $\dim R = 0$, then any prime $\mathfrak{p}$ must be maximal: we can put $\mathfrak{p}$ inside a maximal ideal $\mathfrak{m}$, which makes the chain

$$\mathfrak{p} \subseteq \mathfrak{m}.$$

If $\mathfrak{p} \neq \mathfrak{m}$, then $\dim R \geq 1$, which is false. So instead we have $\mathfrak{p} = \mathfrak{m}$, making $\mathfrak{p}$ maximal.

Lastly, it remains to show that R is the product of finitely many Artinian local rings. This follows directly from Proposition 2.136.

(b) By Proposition 2.137, we see that $\dim A(X) = 0$ is equivalent to $A(X)$ being Artinian, which is equivalent to X being finite. ■

6.2.4 Dimension in Families

In algebraic geometry, we are interested in families of varieties, which in our algebraic context means morphisms of algebras. A helpful case to consider will be when we take an integral extension; this corresponds to the notion of a finite morphism of algebraic sets.

Proposition 6.31. Fix a ring homomorphism $\varphi : R \to S$ which makes S into an integral R-algebra. Then, for any $\mathfrak{p} \in \operatorname{Spec} R$ such that $\ker\varphi \subseteq \mathfrak{p}$, there exists $\mathfrak{q} \in \operatorname{Spec} S$ such that

$$\mathfrak{p} = \varphi^{-1}(\mathfrak{q}).$$

In fact, for any ideal $I \subseteq S$, we have $\dim S/I = \dim R/\varphi^{-1}(I)$.

Proof. We show the two sentences separately.

- To start, we claim that S is still integral over $R/\ker\varphi$ by the induced map $\overline{\varphi} : R/\ker\varphi \to S$. Indeed, any $s \in S$ has some monic polynomial

  $$s^n + \sum_{k=0}^{n-1} \varphi(a_k)s^k = 0$$

  for $\{a_0, \ldots, a_{n-1}\} \subseteq R$. However, $\varphi(a_k) = \overline{\varphi}([a_k]_{\ker\varphi})$, so we conclude

  $$s^n + \sum_{k=0}^{n-1} \overline{\varphi}([a_k]_{\ker\varphi})s^k = 0,$$

  making s still integral over $R/\ker\varphi$.

  Now, $\overline{\varphi} : R/\ker\varphi \to S$ has trivial kernel. Further, because $\ker\varphi \subseteq \mathfrak{p}$, we see that $\mathfrak{p} + \ker\varphi \subseteq R/\ker\varphi$ is still a prime: if $(a + \ker\varphi)(b + \ker\varphi) \in \mathfrak{p} + \ker\varphi$, then $ab \in \mathfrak{p} + \ker\varphi = \mathfrak{p}$, so $a \in \mathfrak{p}$ or $b \in \mathfrak{p}$, so $a + \ker\varphi \in \mathfrak{p} + \ker\varphi$ or $b + \ker\varphi \in \mathfrak{p} + \ker\varphi$.

  Thus, we can invoke Proposition 3.77 (notably, $\overline{\varphi}$ is injective!) so that we have a prime $\mathfrak{q} \subseteq S$ such that

  $$\overline{\varphi}^{-1}(\mathfrak{q}) = \mathfrak{p} + \ker\varphi.$$

  In particular, we can compute

  $$\begin{aligned}\varphi^{-1}(\mathfrak{q}) &= \{a \in R : \varphi(a) \in \mathfrak{q}\} \\ &= \{a \in R : \overline{\varphi}([a]_{\ker\varphi}) \in \mathfrak{q}\} \\ &= \{a \in R : [a]_{\ker\varphi} \in \overline{\varphi}^{-1}(\mathfrak{q})\} \\ &= \{a \in R : [a]_{\ker\varphi} \in \mathfrak{p} + \ker\varphi\} \\ &= \{a \in R : a \in \mathfrak{p} + \ker\varphi\} \\ &= \mathfrak{p} + \ker\varphi \\ &= \mathfrak{p},\end{aligned}$$

  which is what we wanted.

- Fix any ideal $I \subseteq S$. We claim that S/I is integral over $R/\varphi^{-1}(I)$ by the induced map $\overline{\varphi} : R/\varphi^{-1}(I) \to S/I$. The argument is the same as before: any $s \in S$ has some monic polynomial

  $$s^n + \sum_{k=0}^{n-1} \varphi(a_k)s^k = 0$$

  for $\{a_0, \ldots, a_{n-1}\} \subseteq R$. However, $\varphi(a_k) = \overline{\varphi}([a_k]_I)$, so we conclude

  $$s^n + \sum_{k=0}^{n-1} \overline{\varphi}([a_k]_I)s^k = 0,$$

  making s still integral over $R/\varphi^{-1}(I)$.

Thus, we replace R with $R/\varphi^{-1}(I)$, replace S with S/I, and replace φ with $\overline{\varphi}$. In total, we have an integral extension $\varphi : R \to S$, but in fact φ is injective because we modded out by its kernel.

We now compute dimensions. In one direction, suppose that we have a chain of distinct primes

$$\mathfrak{p}_0 \subsetneq \mathfrak{p}_1 \subsetneq \cdots \subsetneq \mathfrak{p}_{\dim R}$$

in R. Then we can use Proposition 3.77 to lift these to a chain of primes

$$\mathfrak{q}_0 \subseteq \mathfrak{q}_1 \subseteq \cdots \subseteq \mathfrak{q}_{\dim R}$$

in S. Notably, $a \in \mathfrak{p}_{k+1} \setminus \mathfrak{p}_k$ implies that $\varphi(a) \in \mathfrak{q}_{k+1} \setminus \mathfrak{q}_k$ because φ is injective, so we do indeed have a chain of $\dim R$ distinct primes in S. Thus, $\dim R \le \dim S$.

Conversely, suppose that we have a chain of distinct primes

$$\mathfrak{q}_0 \subsetneq \mathfrak{q}_1 \subsetneq \cdots \subsetneq \mathfrak{q}_{\dim S}$$

in S. Pulling these back to R, we have a chain of primes

$$\mathfrak{p}_0 \subseteq \mathfrak{p}_1 \subseteq \cdots \subseteq \mathfrak{p}_{\dim S}$$

in R. Now, if any prime $\mathfrak{p} \subseteq R$ appears more than once in the above chain, then there are two primes $\mathfrak{q}_k \subsetneq \mathfrak{q}_\ell$ of S lying over $\mathfrak{p}$. However, this is illegal by Lemma 3.87, so instead we have a chain of $\dim S$ distinct primes in S, so we conclude $\dim R \ge \dim S$.

Combining our arguments, we see that $\dim R = \dim S$, which is what we wanted.

The above statements finish the proof. ■

Remark 6.32 (Nir). Here is a nice application: let K be a finite extension of $\mathbb{Q}$, and let $\mathcal{O}_K$ be the integral closure of $\mathbb{Z}$ in K. Then $\mathcal{O}_K$ is integral over $\mathbb{Z}$ by construction, so Proposition 6.31 promises us that

$$\dim \mathcal{O}_K = \dim \mathbb{Z} = 1.$$

Thus, we have verified that all nonzero primes of $\mathcal{O}_K$ are maximal.

And here is the geometric application.

Corollary 6.33. Fix a morphism of varieties $\varphi : X \to Y$ and let $\varphi^* : A(Y) \to A(X)$ be the induced map on coordinate rings. Further, suppose $A(X)$ is finitely generated as an $A(Y)$-module. Then the following are true.

(a) The fibers of φ are finite.

(b) If φ^* is an injection, then φ is surjective.

(c) If $Z \subseteq X$ is Zariski closed, then $\varphi(Z) \subseteq Y$ is also Zariski closed.

Proof. We go one at a time. For brevity, we set $R \coloneqq A(Y)$ and $S \coloneqq A(X)$ so that $\varphi^* : R \to S$ makes S into an R-algebra. We quickly note that $A(X)$ being finite over $A(Y)$ implies that S is an integral R algebra by Lemma 3.48.

(a) Fix a maximal ideal $\mathfrak{m} \subseteq R$. Noting the coordinate ring of the fiber over $\mathfrak{m}$ is $S/\mathfrak{m}S$, so we compute

$$\dim S/\mathfrak{m}S = \dim R/\varphi^{-1}(\mathfrak{m}S) = \dim R/\mathfrak{m} = 0,$$

where we have used Proposition 6.31; notably, S is indeed an integral R-algebra.

(b) Because points correspond to maximal ideals, we will show that

$$(\varphi^*)^{-1} : \operatorname{Spec} S \to \operatorname{Spec} R$$

surjects onto maximal ideals from maximal ideals. Indeed, pick up some maximal ideal $\mathfrak{m} \subseteq R$ and use Proposition 3.77 to get a prime $\mathfrak{p}$ lying over $\mathfrak{m}$. Note that we have used the fact that φ^* is injective here.

However, we can place $\mathfrak{p}$ inside a maximal ideal $\mathfrak{p}'$, so $(\varphi^*)^{-1}(\mathfrak{p}')$ is a prime of R containing $(\varphi^*)^{-1}(\mathfrak{p}) = \mathfrak{m}$ and hence will equal $\mathfrak{m}$. Thus, we have a maximal ideal $\mathfrak{p} \subseteq S$ lying over $\mathfrak{m}$, as required.

To finish, we claim $\varphi((a_1, \ldots, a_n)) = (b_1, \ldots, b_m)$ only if

$$(\varphi^*)^{-1}\left((x_1 - a_1, \ldots, x_n - a_n)\right) = (y_1 - b_1, \ldots, y_m - b_m),$$

where $A(X) = k[x_1, \ldots, x_n]/I$ and $A(Y) = k[y_1, \ldots, y_m]/J$. This will be enough because we showed that there will be a maximal ideal $(x_1 - a_1, \ldots, x_n - a_n)$ in $A(X)$ to hit the maximal ideal $(y_1 - b_1, \ldots, y_m - b_m)$ of $A(Y)$ above.

Well, observe that any $f \in (y_1 - b_1, \ldots, y_m - b_m)$ has $f\varphi \in (x_1 - a_1, \ldots, x_n - a_n)$, so $f\varphi(a_1, \ldots, a_n) = 0$. In particular,

$$\varphi(a_1, \ldots, a_n) \in Z((y_1 - b_1, \ldots, y_m - b_m)) = \{(b_1, \ldots, b_m)\},$$

so we are done.

(c) Note that φ restricts to a morphism $\varphi : Z \to \overline{\varphi(Z)}$ (which we conveniently rename to φ), where $\overline{\varphi(Z)} = Z(I(\overline{\varphi(Z)}))$ is the Zariski closure of $\varphi(Z)$. We would like to show that φ is surjective, for which it suffices by (b) to show that φ^* is injective.

This is a matter of computation. We show that φ^* has trivial kernel. Let $A(Z) = k[x_1, \ldots, x_n]/I$ (so that $Z = Z(I)$), which forces

$$A(\overline{\varphi(Z)}) = k[x_1, \ldots, x_n]/I(Z(I(\varphi(Z)))) = I(\varphi(Z)).$$

In particular, having $f \in k[y_1, \ldots, y_m]$ with $[f]_{I(\varphi(Z))} \in \ker \varphi^*$ means that $f\varphi \in I(Z)$ so that $f\varphi(p) = 0$ for all $p \in Z$. But then f vanishes on $I(\varphi(Z))$, so $f \in I(\varphi(Z))$, which is what we wanted. ■

Remark 6.34 (Nir)**.** The statement (b) above is an instance of "geometry is the opposite of algebra."

Example 6.35. Fix $S := k[x, y]/\left(x - y^2\right)$ and $R := k[x]$ so that we have a mapping $R \hookrightarrow S$. The mapping between the algebraic curves is in fact surjective, though this is not apparent from the image in $\mathbb{R}$.

6.2.5 Local Dimension

As an intermission, we quickly discuss how dimension behaves locally.

Lemma 6.36. Fix a ring R and a multiplicatively closed subset $U \subseteq R$. Further, set $S := R\left[U^{-1}\right]$ with the natural map $\varphi : R \to S$. Then, for any prime $\mathfrak{p} \subseteq R\left[U^{-1}\right]$, we have

$$\operatorname{codim} \varphi^{-1}(\mathfrak{p}) = \operatorname{codim} \mathfrak{p}.$$

Proof. We use Lemma 6.17. As such, we split the proof into two inequalities.

- We show $\operatorname{codim} \varphi^{-1}(\mathfrak{p}) \leq \operatorname{codim} \mathfrak{p}$. Indeed, set $d := \operatorname{codim} \varphi^{-1}(\mathfrak{p})$ so that we have a chain of distinct primes

$$\mathfrak{p}_0 \subsetneq \mathfrak{p}_1 \subsetneq \cdots \mathfrak{p}_d = \varphi^{-1}(\mathfrak{p}).$$

Note $\mathfrak{p}_k R\left[U^{-1}\right] \subseteq \varphi^{-1}(\mathfrak{p}) R\left[U^{-1}\right]$ for each $\mathfrak{p}_k$, but $\varphi^{-1}(\mathfrak{p}) R\left[U^{-1}\right]=\mathfrak{p}$ by Lemma 2.27, so $\mathfrak{p}_k R\left[U^{-1}\right]$ is a proper ideal, so $\mathfrak{p}_k \cap U=\varnothing$, lest we have a unit.

It follows from Theorem 2.29 that

$$\mathfrak{p}_0 R\left[U^{-1}\right] \subsetneq \mathfrak{p}_1 R\left[U^{-1}\right] \subsetneq \cdots \mathfrak{p}_d R\left[U^{-1}\right]=\mathfrak{p}$$

is a chain of primes in $R\left[U^{-1}\right]$. Notably, the map $\mathfrak{p}_k \mapsto \mathfrak{p}_k R\left[U^{-1}\right]$ is injective (with inverse φ^{-1}) by combining with Lemma 2.28.

Thus, we have a chain d distinct primes below $\mathfrak{p}$, so $\operatorname{codim} \mathfrak{p} \geq d$, as desired.

- We show $\operatorname{codim} \mathfrak{p} \leq \operatorname{codim} \varphi^{-1}(\mathfrak{p})$. Indeed, set $d:=\operatorname{codim} \mathfrak{p}$ so that we have a chain of distinct primes

$$\mathfrak{p}_0 \subsetneq \mathfrak{p}_1 \subsetneq \cdots \subsetneq \mathfrak{p}_d=\mathfrak{p} .$$

In particular, pulling back along φ^{-1} gives us a chain of primes

$$\varphi^{-1} \mathfrak{p}_0 \subsetneq \varphi^{-1} \mathfrak{p}_1 \subsetneq \cdots \subsetneq \varphi^{-1} \mathfrak{p}_d=\varphi^{-1} \mathfrak{p},$$

which are distinct by using the bijectivity of Theorem 2.29. Thus, we have a chain of d distinct primes below $\varphi^{-1} \mathfrak{p}$, so it follows $\operatorname{codim} \varphi^{-1} \mathfrak{p} \geq d$, as desired.

Combining the above results gives $\operatorname{codim} \varphi^{-1} \mathfrak{p}=\operatorname{codim} \mathfrak{p}$, which is what we wanted. ■

Remark 6.37. In fact, one can show that $R_{\varphi^{-1} \mathfrak{p}} \cong R\left[U^{-1}\right]_{\mathfrak{p}}$ by using the universal property of localization a bunch of times.

6.2.6 The Principal Ideal Theorem

Here is our statement.

Theorem 6.38 (Principal ideal). Fix a Noetherian ring R. Given $x \in R$, suppose $\mathfrak{p}$ is a minimal prime over (x). Then

$$\operatorname{codim} \mathfrak{p} \leq 1 .$$

Proof. We start by localizing. The key is the following lemma.

Lemma 6.39. Fix an ideal I of a ring R. If the prime $\mathfrak{p}$ of R is minimal over I, then $\mathfrak{p} R_{\mathfrak{p}}$ is minimal over $I R_{\mathfrak{p}}$.

Proof. Indeed, if we can find a prime $\mathfrak{q} \subseteq R_{\mathfrak{p}}$ such that

$$I R_{\mathfrak{p}} \subseteq \mathfrak{q} \subseteq \mathfrak{p} R_{\mathfrak{p}},$$

then pulling back along the localization map $\psi: R \rightarrow R_{\mathfrak{p}}$ gives us the chain

$$I \subseteq \psi^{-1}(\mathfrak{q}) \subseteq \psi^{-1}\left(\mathfrak{p} R_{\mathfrak{p}}\right)$$

because $I \subseteq \psi^{-1}\left(I R_{\mathfrak{p}}\right)$. As such, minimality forces $\psi^{-1}(\mathfrak{q})$ to be equal to $\psi^{-1}\left(\mathfrak{p} R_{\mathfrak{p}}\right)=\mathfrak{p}$ (here we are using Theorem 2.29), so Lemma 2.27 tells us

$$\mathfrak{q}=\psi^{-1}(\mathfrak{q}) R_{\mathfrak{p}}=\mathfrak{p} R_{\mathfrak{p}},$$

thus finishing. ■

In particular, $\mathfrak{p}R_\mathfrak{p}$ is minimal over $(x)R_\mathfrak{p}$.

So at this point, we fully replace R with $R_\mathfrak{p}$ (which is still Noetherian by Corollary 2.30), $\mathfrak{p}$ with $R_\mathfrak{p}$, and (x) with $(x)R_\mathfrak{p}$. Thus, R is a local ring with maximal ring $\mathfrak{p}$, and $\mathfrak{p}$ is a minimal prime over (x). Before the replacement, we wanted to show that $\dim R_\mathfrak{p} \le 1$, so we see that now we want to show $\dim R \le 1$. In other words, we want to show that any chain of distinct primes

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

must have $d \le 1$. Note that if $\mathfrak{p}_d \ne \mathfrak{p}$, then we can tack on $\subsetneq \mathfrak{p}$ to the end of chain because $\mathfrak{p}$ is the unique maximal ideal, so we may in fact assume that $\mathfrak{p}_d = \mathfrak{p}$. Thus, we are essentially showing that the chain

$$\mathfrak{p}_0 \subsetneq \mathfrak{p}_1 \subsetneq \cdots \subsetneq \underbrace{\mathfrak{p}_{d-1}}_{\mathfrak{q}:=} \subsetneq \mathfrak{p}$$

has $d \le 1$. If $d = 0$, then there is nothing to say.

Otherwise, we want $\mathfrak{q} = \mathfrak{p}_{d-1}$ to have no primes strictly below it, which means (from Lemma 6.17) we want to show $\dim R_\mathfrak{q} = \operatorname{codim} \mathfrak{q} = 0$. Noting that $R_\mathfrak{q}$ is still Noetherian, we see that showing $\dim R_\mathfrak{q} = 0$ is equivalent to showing $R_\mathfrak{q}$ is Artinian by Proposition 6.30. Thus, we will imitate the discussion in Theorem 2.126 and show that the ideal $\mathfrak{q}$ is nilpotent.

As a starting step, we claim that $R/(x)$ is Artinian. We have the following stronger statement.

Lemma 6.40. Fix a proper ideal I of a ring local ring R with maximal ideal $\mathfrak{p}$. Then the following are equivalent.

(a) $\mathfrak{p}$ is minimal over I.

(b) R/I is Artinian.

(c) $\mathfrak{p}^n \subseteq I$ for some positive integer n.

Proof. We have the following implications. Let $\pi : R \to R/I$ be the natural projection.

- We show (a) implies (b). In particular, we claim $\dim I = \dim R/I = 0$, for which we use Lemma 6.16. Well, if we have some chain
$$I \subseteq \mathfrak{p}_0 \subsetneq \mathfrak{p}_1 \subsetneq \cdots \subsetneq \mathfrak{p}_d,$$
then because R is local, we can place $\subseteq \mathfrak{p}_d$ at the end, thus allowing us to assume $\mathfrak{p}_d = \mathfrak{p}$. But then $\mathfrak{p}$ is minimal over I, so the entire chain collapses to $\mathfrak{p}_0 = \mathfrak{p}$. It follows $d = 0$, finishing.

- We show (b) implies (c). By Lemma 3.89, we see that $\pi(\mathfrak{p})$ is the unique maximal ideal of R/I, so $\pi(\mathfrak{p})$ is the Jacobson radical of R/I. Because R/I is Artinian, this Jacobson radical is nilpotent by Lemma 2.134, so there exists a positive integer n for which
$$\pi(\mathfrak{p})^n = (0) + I.$$
As such, any generating element $x_1 \cdot \ldots \cdot x_n \in \mathfrak{p}^n$ will have its projection go to $0 \pmod I$, meaning that $x_1 \cdot \ldots \cdot x_n \in I$, which verifies $\mathfrak{p}^n \subseteq I$ for our n.

- We show (c) implies (a). Indeed, suppose that we have a prime $\mathfrak{q}$ such that
$$I \subseteq \mathfrak{q} \subseteq \mathfrak{p}.$$
We need $\mathfrak{q} = \mathfrak{p}$, for which it suffices to show $\mathfrak{p} \subseteq \mathfrak{q}$ because $\mathfrak{p}$ is the unique maximal ideal. Well, any $x \in \mathfrak{p}$ has $x^n \in \mathfrak{p}^n \subseteq I \subseteq \mathfrak{q}$, so $x \in \mathfrak{q}$ follows.

The above implications finish the proof. ■

So indeed, $R/(x)$ is Artinian by Lemma 6.40.

Continuing, to measure how close $\mathfrak{q}$ is to being nilpotent, we let $\varphi : R \to R_{\mathfrak{q}}$ be the localization map and set

$$\mathfrak{q}^{(n)} := \varphi^{-1}\left((\mathfrak{q}R_{\mathfrak{q}})^n\right).$$

In particular, $\frac{r}{1} \in (\mathfrak{q}R_{\mathfrak{q}})^n$ if and only if $\frac{r}{1} = \frac{r'}{s'}$ for some $r' \in \mathfrak{q}^n$ and $s' \notin \mathfrak{q}$,[1] or equivalently, $rs'' \in \mathfrak{q}^n$ for some $s'' \notin \mathfrak{q}$, where we are implicitly using the fact $R \setminus \mathfrak{q}$ is multiplicative. Thus,

$$\mathfrak{q}^{(n)} = \{r \in R : rs \in \mathfrak{q}^n \text{ for some } s \notin \mathfrak{q}\}.$$

Now, using the fact that $R/(x)$ is Artinian, we see that the chain

$$\mathfrak{q}^{(1)} + (x) \supseteq \mathfrak{q}^{(2)} + (x) \supseteq \mathfrak{q}^{(3)} + (x) \supseteq \cdots$$

must stabilize, so we are promised some n for which $\mathfrak{q}^{(n)} + (x) = \mathfrak{q}^{(n+1)} + (x)$. It follows $\mathfrak{q}^{(n)} \subseteq \mathfrak{q}^{(n+1)} + (x)$. Quickly, this means that any element of $\mathfrak{q}^{(n)}$ can be written as $a + bx$ with $a \in \mathfrak{q}^{(n+1)}$ and $b \in R$. But then $bx \in \mathfrak{q}^{(n)}$, so $b(sx) \in \mathfrak{q}^n$ for some $s \notin \mathfrak{q}$, but $x \notin \mathfrak{q}$ (otherwise $(x) \subseteq \mathfrak{q} \subseteq \mathfrak{p}$ forces $\mathfrak{q} = \mathfrak{p}$ by minimality), so in fact $b \in \mathfrak{q}^{(n)}$. So actually

$$\mathfrak{q}^{(n)} \subseteq \mathfrak{q}^{(n+1)} + (x)\mathfrak{q}^{(n)},$$

and we get a full equality because $\mathfrak{q}^{(n+1)}, (x)\mathfrak{q}^{(n)} \subseteq \mathfrak{q}^{(n)}$ individually. In other words, looking in $R/\mathfrak{q}^{(n+1)}$, we find

$$\left(\mathfrak{q}^{(n)} + \mathfrak{q}^{(n+1)}\right) = (x) \cdot \left(\mathfrak{q}^{(n)} + \mathfrak{q}^{(n+1)}\right),$$

so we can apply Nakayama's lemma: the fact that $(x) \subseteq \mathfrak{p}$ lives in the Jacobson radical, forces by Theorem 3.33 that $\mathfrak{q}^{(n)} + \mathfrak{q}^{(n+1)} = 0 + \mathfrak{q}^{(n+1)}$. Thus, $\mathfrak{q}^{(n)} = \mathfrak{q}^{(n+1)}$, so

$$(\mathfrak{q}R_{\mathfrak{q}})^n = \varphi^{-1}\left((\mathfrak{q}R_{\mathfrak{q}})^n\right)R_{\mathfrak{q}} = \mathfrak{q}^{(n)}R_{\mathfrak{q}} = \mathfrak{q}^{(n+1)}R_{\mathfrak{q}} = \varphi^{-1}\left((\mathfrak{q}R_{\mathfrak{q}})^{n+1}\right)R_{\mathfrak{q}} = (\mathfrak{q}R_{\mathfrak{q}})^{n+1}$$

using Lemma 2.27. In particular, noting that the Jacobson radical in $R_{\mathfrak{q}}$ is $\mathfrak{q}R_{\mathfrak{q}}$, applying Theorem 3.33 to the above equation gives

$$(\mathfrak{q}R_{\mathfrak{q}})^n = 0.$$

So indeed, our maximal ideal $\mathfrak{q}R_{\mathfrak{q}}$ is nilpotent, so it follows that $R_{\mathfrak{q}}$ has dimension 1, which is what we wanted. One could track through the proof of Theorem 2.126 to see this. Alternatively, one could note more directly that, $R_{\mathfrak{q}}$ has only one prime: if $\mathfrak{q}' \subseteq R_{\mathfrak{q}}$ is a prime, then of course $\mathfrak{q}' \subseteq \mathfrak{q}R_{\mathfrak{q}}$ by maximality; conversely, any element $a \in \mathfrak{q}R_{\mathfrak{q}}$ has $a^n = 0 \in \mathfrak{q}'$, so $a \in \mathfrak{q}'$ follows, giving $\mathfrak{q}' = \mathfrak{q}R_{\mathfrak{q}}$. So we get $\dim R_{\mathfrak{q}} = 0$. ■

Remark 6.41 (Nir)**.** Theorem 6.38 provides a silly way to see that principal ideal domains R which are not fields have dimension 1: all primes $\mathfrak{p}$ is principal and hence minimal over a prime, so $\operatorname{codim} \mathfrak{p} \le 1$. But Theorem 6.20 then gives

$$\dim R \le 1.$$

On the other hand, R is not a field, we conclude that R has a nonzero prime $\mathfrak{p} \supsetneq (0)$, so $\dim R > 0$.

Remark 6.42. The analogous statement in the affine case is that the dimension of the intersection between a one-dimensional curve $f = 0$ and the space cut out by $\mathfrak{p}$ is either going to be 0 (if we intersect at points) or 1 (if a nontrivial part of the curve $f = 0$ lives in the region cut out by $\mathfrak{p}$).

More rigorously, by the implicit function theorem in differential geometry, having one equation in a tangent space will have a solution set with either the same dimension or one fewer dimension.

We can extend this result to any finitely generated ideal by an induction.

[1] To see $(\mathfrak{q}R_{\mathfrak{q}})^n = \mathfrak{q}^n R_{\mathfrak{q}}$, certainly $\mathfrak{q}^n R_{\mathfrak{q}} \subseteq (\mathfrak{q}R_{\mathfrak{q}})^n$ by directly localizing. On the other hand, any product $\frac{r_1}{s_1} \cdot \ldots \cdot \frac{r_n}{s_n}$ generating $(\mathfrak{q}^n R_{\mathfrak{q}})$ must live in $\mathfrak{q}^n R_{\mathfrak{q}}$ by multiplying through.

Theorem 6.43. Fix a Noetherian ring R. Given an ideal $(x_1, \ldots, x_s) \in R$, suppose $\mathfrak{p}$ is a minimal prime over $(x_1, \ldots, x_s)$. Then
$$\operatorname{codim} \mathfrak{p} \le s.$$

Proof. We proceed by induction on s; the case of $s = 0$ is merely saying that a minimal prime $\mathfrak{p}$ (over (0)) has $\operatorname{codim} \mathfrak{p} = 0$, which is true by Lemma 6.17. The case of $s = 1$ is Theorem 6.38.

So now we discuss the inductive step. As before, we begin by localizing. By Lemma 6.39, we see that $\mathfrak{p}R_\mathfrak{p}$ remains minimal over $(x_1, \ldots, x_s)R_\mathfrak{p}$, and we are trying to show that $\dim R_\mathfrak{p} = \operatorname{codim} \mathfrak{p} = s$. In particular, replacing R with $R_\mathfrak{p}$, $\mathfrak{p}$ with $R_\mathfrak{p}$, and $(x_1, \ldots, x_s)$ with $(x_1, \ldots, x_s)R_\mathfrak{p}$, we see that R is local with maximal ideal $\mathfrak{p}$, which is minimal over $(x_1, \ldots, x_s)$, and we want to show that
$$\dim R \le s.$$
We now proceed with the proof. In particular, we would like to show that any chain of distinct primes
$$\mathfrak{p}_0 \subsetneq \mathfrak{p}_1 \subsetneq \cdots \subsetneq \mathfrak{p}_d$$
must have $d \le s$. If $d = 0$, there is nothing to say.

Otherwise, note that $\mathfrak{p}$ is the unique maximal ideal, so we can tack on $\subseteq \mathfrak{p}$ to the end of this chain, allowing us to assume $\mathfrak{p} = \mathfrak{p}_d$. Similarly, we can replace $\mathfrak{p}_{d-1}$ with the largest prime $\mathfrak{q}$ containing $\mathfrak{p}_{d-1}$ while strictly below $\mathfrak{p}$ so that we have the chain
$$\mathfrak{p}_0 \subsetneq \mathfrak{p}_1 \subsetneq \cdots \subsetneq \mathfrak{p}_{d-2} \subsetneq \mathfrak{q} \subsetneq \mathfrak{p}.$$
As such, we would like to show that there at most $s-1$ primes below $\mathfrak{q}$, which means we want $\operatorname{codim} \mathfrak{q} \le s-1$ by Lemma 6.17. By the inductive hypothesis, it will suffice to show that $\mathfrak{q}$ is minimal over an ideal generated by $s-1$ elements.

Note that, if $\mathfrak{q}$ contains the $x_\bullet$, then $(x_1, \ldots, x_s) \subseteq \mathfrak{q} \subsetneq \mathfrak{p}$, violating the minimality of $\mathfrak{p}$. So $\mathfrak{q}$ does not contain at least one of the $x_\bullet$; by rearranging, suppose $x_s \notin \mathfrak{q}$. Now, imitating the previous proof, we note that $\mathfrak{p}$ is a minimal prime over $\mathfrak{q}$ and contains (x_s), so actually $\mathfrak{p}$ is a minimal prime over $\mathfrak{q} + (x_s)$. So Lemma 6.40 tells us
$$\mathfrak{p}^n = \mathfrak{q} + (x_s)$$
for some positive integer n. In particular, each x_i has $x_i^n \in \mathfrak{p}^n = \mathfrak{q} + (x_s)$, so there exists a corresponding $y_i \in \mathfrak{q}$ and $r_i \in R$ such that
$$x_i^n = y_i + r_i x_s. \qquad (*)$$
We now claim that $\mathfrak{q}$ is minimal over $(y_1, \ldots, y_{s-1})$, which will of course finish. To see this, we proceed in steps.

1. Note that $\mathfrak{p} + (y_1, \ldots, y_{s-1}, x_s)$ is nilpotent in $R/(y_1, \ldots, y_{s-1}, x_s)$ by Lemma 6.40: taking $\mathfrak{p}$ to a sufficiently large power places $\mathfrak{p}^\bullet$ in $(x_1, \ldots, x_s)$, but then taking any generator x_i to a sufficiently large power places it into $(y_1, \ldots, y_{s-1}, x_s)$ by $(*)$.

2. Reading the previous step backwards, it follows that the image of $\mathfrak{p}$ in $(R/(y_1, \ldots, y_{s-1}))/(x_s)$ nilpotent, so the image of $\mathfrak{p}$ in $R/(y_1, \ldots, y_{s-1})$ is minimal over (x_s) by Lemma 6.40. In particular, Theorem 6.38 enforces
$$\operatorname{codim}(\mathfrak{p} + (y_1, \ldots, y_{s-1})) \le 1.$$

3. We now track through $\mathfrak{q}$. To show that $\mathfrak{q}$ is minimal over $(y_1, \ldots, y_{s-1})$ we are showing that there are no primes strictly between $(y_1, \ldots, y_{s-1})$ and $\mathfrak{q}$. Modding out by $(y_1, \ldots, y_{s-1})$, we are showing that there are no primes strictly between (0) and $\mathfrak{q} + (y_1, \ldots, y_{s-1})$ in $R/(y_1, \ldots, y_{s-1})$. (The fact that the modding process preserves inclusions of primes is discussed in Lemma 6.16.) As such, we need
$$\operatorname{codim}(\mathfrak{q} + (y_1, \ldots, y_{s-1})) = 0$$
in $R/(y_1, \ldots, y_{s-1})$. Well, note that x_s is not in $\mathfrak{q}$ and hence not in $(y_1, \ldots, y_{s-1})$, so we have
$$\mathfrak{q} + (y_1, \ldots, y_{s-1}) \subsetneq (\mathfrak{q} + (x_s)) + (y_1, \ldots, y_{s-1}) \subseteq \mathfrak{p} + (y_1, \ldots, y_{s-1}),$$

in $R/(y_1, \ldots, y_{s-1})$. Thus, the previous step forces $\mathfrak{q} + (y_1, \ldots, y_{s-1})$ to in fact have no primes strictly smaller (and hence have codimension 0), lest we be able to add more primes below $\mathfrak{p} + (y_1, \ldots, y_{s-1})$.

So $\mathfrak{q}$ is minimal over $(y_1, \ldots, y_{s-1})$, which is what we wanted. ■

Remark 6.44. As in Remark 6.42, the analogous statement in linear algebra is that the solution set to s equations (carved out by $(x_1, \ldots, x_s)$) will have at most dimension codimension s when living inside an affine variety.

We close class by discussing the sharpness of Theorem 6.43. As an example, the equality case is in fact achievable, for any s.

Example 6.45. Fix $R := k[x_1, \ldots, x_n]$. Then the codimension of the prime $\mathfrak{p} := (x_1, \ldots, x_r)$ is upper-bounded by r by Theorem 6.43, but we also have a chain of distinct primes

$$(0) \subsetneq (x_1) \subsetneq (x_1, x_2) \subsetneq \cdots \subsetneq (x_1, \ldots, x_r) = \mathfrak{p},$$

so $\operatorname{codim} \mathfrak{p} = r$ follows.

And here is a full converse to Theorem 6.43.

Corollary 6.46. Fix a prime ideal $\mathfrak{p}$ of a Noetherian ring R with codimension r. Then there are elements $x_1, \ldots, x_r$ such that $\mathfrak{p}$ is minimal over $(x_1, \ldots, x_r)$, and in fact $\operatorname{codim}(x_1, \ldots, x_r) = r$.

Proof. We induct. If $\mathfrak{p}$ has codimension 0, then by Lemma 6.17, we see that there is no prime strictly smaller than $\mathfrak{p}$. In other words, $\mathfrak{p}$ is minimal over (0), the ideal generated by 0 elements.

We now proceed with the induction. Because $\mathfrak{p}$ has codimension $r > 0$, we can build a chain of primes

$$\mathfrak{p}_0 \subsetneq \mathfrak{p}_1 \subsetneq \cdots \subsetneq \mathfrak{p}_{r-1} \subsetneq \mathfrak{p}$$

by Lemma 6.17. In particular, $\operatorname{codim} \mathfrak{p}_{r-1} = r - 1$ (it is at least $r - 1$ by this construction and cannot exceed $r - 1$ by Lemma 6.25), so the induction promises us that $\mathfrak{p}_{r-1}$ is minimal over some ideal $(x_1, \ldots, x_{r-1})$ of codimension $r - 1$.

We now just need to choose x_r to make our codimension a little bigger. Indeed, the set of primes minimal over $(x_1, \ldots, x_{r-1})$ is finite by Proposition 2.175 have codimension at most $r-1$ by the inductive hypothesis, so $\mathfrak{p}$ is not contained in of them by Lemma 6.25. So Lemma 2.165 promises that we can find an element x_r which lives in $\mathfrak{p}$ but in none of the primes minimal over $(x_1, \ldots, x_{r-1})$, so we claim that $\mathfrak{p}$ is minimal over

$$(x_1, \ldots, x_r).$$

Indeed, fix any prime $\mathfrak{q}$ such that

$$(x_1, \ldots, x_r) \subseteq \mathfrak{q} \subseteq \mathfrak{p}.$$

So to finish, we claim that any prime $\mathfrak{q}$ containing $(x_1, \ldots, x_r)$ has codimension at least r. By Lemma 6.25, this will force $\mathfrak{p} = \mathfrak{q}$ in the above case because $\mathfrak{q} \subseteq \mathfrak{p}$ already.

On one hand, we get $\operatorname{codim} \mathfrak{q} \le \operatorname{codim} \mathfrak{p} = r$ by Lemma 6.25 automatically, so we want $\operatorname{codim} \mathfrak{q} \ge r$. Well, $\mathfrak{q}$ contains $(x_1, \ldots, x_{r-1})$ and hence have codimension at least

$$\operatorname{codim}(x_1, \ldots, x_{r-1}) = r - 1.$$

However, if we did have $\operatorname{codim} \mathfrak{q} = r - 1$, then there could be no prime strictly between $\mathfrak{q}$ and $(x_1, \ldots, x_{r-1})$ because such a prime would have codimension strictly less than $\operatorname{codim} \mathfrak{q} = r - 1 = \operatorname{codim}(x_1, \ldots, x_{r-1})$ by Lemma 6.25. So in this case, $\mathfrak{q}$ is minimal over $(x_1, \ldots, x_{r-1})$, which is a contradiction because $x_r \in \mathfrak{q}$.

Lastly, we finish the induction by showing $\operatorname{codim}(x_1, \ldots, x_r) = r$. Certainly $\mathfrak{p} \supseteq \operatorname{codim}(x_1, \ldots, x_r)$ shows that $\operatorname{codim}(x_1, \ldots, x_r) \le r$ by Lemma 6.25. However, the argument of the previous paragraph showed that any prime $\mathfrak{q}$ containing $(x_1, \ldots, x_r)$ has codimension at least r, so the equality follows. ■

6.3 March 29

There was no lecture today because there was a midterm.

6.4 March 31

Welcome back from spring break.

6.4.1 More Local Dimension

In light of Theorem 6.20, we can compute dimension via localizations, so we will focus on local rings.

Lemma 6.47. Fix a local ring R with unique maximal ideal $\mathfrak{m}$. Then $\dim R = \operatorname{codim} \mathfrak{m}$.

Proof. Certainly $\operatorname{codim} \mathfrak{m} \le \dim R$ by Proposition 6.23, so we need to show $\dim R \le \operatorname{codim} \mathfrak{m}$. Well, fix any chain of distinct primes

$$\mathfrak{p}_0 \subsetneq \mathfrak{p}_1 \subsetneq \cdots \subsetneq \mathfrak{p}_{d-1} \subsetneq \mathfrak{p}_d$$

in R, we claim that $d \le \operatorname{codim} \mathfrak{m}$, which will finish by setting $d = \dim R$. Note that $\mathfrak{m}$ is the unique maximal ideal, so $\mathfrak{p}_d \subseteq \mathfrak{m}$. As such, we can replace $\mathfrak{p}_d$ at the end with $\mathfrak{m}$ (namely, if $\mathfrak{p}_{d-1}$ exists and is strictly contained in $\mathfrak{p}_d \subseteq \mathfrak{m}$, then $\mathfrak{p}_{d-1} \subsetneq \mathfrak{m}$ as well), so we have a chain

$$\mathfrak{p}_0 \subsetneq \mathfrak{p}_1 \subsetneq \cdots \subsetneq \mathfrak{p}_{d-1} \subsetneq \mathfrak{m}$$

of length d descending from $\mathfrak{m}$. As such, $d \le \operatorname{codim} \mathfrak{m}$ by Lemma 6.17. ■

Proposition 6.48. Fix a local ring R with maximal ideal $\mathfrak{m}$. Then $\dim R$ is the minimal $d \in \mathbb{N}$ such that there exist generators $f_1, \ldots, f_d$ so that

$$\mathfrak{m}^n \subseteq (f_1, \ldots, f_d) \subseteq \mathfrak{m}$$

for some n.

Proof. The point is to use the Principal ideal theorem to use the number of generators. By Lemma 6.47, we have $\dim R = \operatorname{codim} \mathfrak{m}$. We now take our implications separately.

- Suppose that we have some d generators $f_1, \ldots, f_d$ and some $n \in \mathbb{N}$ so that

  $$\mathfrak{m}^n \subseteq (f_1, \ldots, f_d) \subseteq \mathfrak{m}.$$

  We show $d \ge \dim R = \operatorname{codim} \mathfrak{m}$. By Theorem 6.43, it suffices to show $\mathfrak{m}$ is minimal over $(f_1, \ldots, f_d)$. Well, by Lemma 6.40, we note that $\mathfrak{m}^n \subseteq (f_1, \ldots, f_d)$ provides this for free.

- In the other direction, we note that Corollary 6.46 provides us with $d := \operatorname{codim} \mathfrak{m} = \dim R$ generators $f_1, \ldots, f_d$ such that $\mathfrak{m}$ is minimal over $(f_1, \ldots, f_d)$. But then Lemma 6.40 tells us that there exists some n such that

  $$\mathfrak{m}^n \subseteq (f_1, \ldots, f_d).$$

  Noting $\mathfrak{m}$ contains $(f_1, \ldots, f_d)$ because $\mathfrak{m}$ is minimal over $(f_1, \ldots, f_d)$, we are done.

From the above two points, we see that the minimal number d such that there exist elements $f_1, \ldots, f_d \in R$ such that

$$\mathfrak{m}^n \subseteq (f_1, \ldots, f_d) \subseteq \mathfrak{m}$$

is at least $\operatorname{codim} \mathfrak{m}$ by the first point above, but $\operatorname{codim} \mathfrak{m}$ is achievable by the second point above, so we conclude $d = \operatorname{codim} \mathfrak{m} = \dim R$. ■

Remark 6.49. There is a geometric meaning to the discovered $\{f_1, \ldots, f_d\}$. Namely, if X is an algebraic set, and $P \in X$ is a point, then we can set $R := A(X)$ to be our coordinate ring and $\mathfrak{m}$ the maximal ideal corresponding to P.

Here, the functions $\{f_1, \ldots, f_d\}$ from Proposition 6.48 will be "local coordinates" in a neighborhood of P. In other words, these elements f_k have powers which go to 0, so they are approximately providing an infinitesimal (i.e., "differential") basis of some small region around P, which indeed what we feel the dimension at P should be.

6.4.2 The Rank–Nullity Theorem

Working in Vec_k, our notion of dimension has its usual geometric meaning. One important result in linear algebra is the Rank–nullity theorem, which says that a map of vector spaces $\varphi : X \to B$ (thinking of this as giving a "family" of vector spaces over B) will give

$$\dim X = \dim \operatorname{im} \varphi + \dim \ker \varphi.$$

We would like to remove the data of φ from this equation, which we do in two steps.

- Certainly $\operatorname{im} \varphi \subseteq B$, so we callously bound $\dim \operatorname{im} \varphi \leq \dim B$.
- We would like to think of dimension as a local quantity, so instead of looking at $\ker \varphi$ as the pre-image of specifically $0 \in B$, we choose any $p \in B$ and note that we are looking at $\dim \varphi^{-1}(p)$, roughly speaking.

So in total, we are getting

$$\dim X \leq \dim B + \dim \varphi^{-1}(p).$$

Now, translating this into the algebraic context, we set $R = A(B)$ and $S = A(X)$ so that we have the map $\varphi^* : R \to S$, which makes S into an R-algebra. Choosing some $p \in B$ with corresponding maximal ideal $\mathfrak{m} \subseteq R$, we note that the coordinate ring of $\varphi^{-1}(p)$ is $S/\mathfrak{m}S$, so we can fully translate the above inequality as asking for

$$\dim S \stackrel{?}{\leq} \dim R + \dim S/\mathfrak{m}S.$$

Because we no longer expect dimension to be so uniform in a general algebraic variety, we will not expect the above inequality to hold whole-sale. However, if we do look locally at some point in S which is going to p, we are expecting something like a linear transformation between these, so perhaps we can salvage this.

We could either manually localize S to get this effect, but we will just force S and R to be local, say with maximal ideals $\mathfrak{n}$ and $\mathfrak{m}$ respectively. Then looking at a point in $q \in X$ which goes to $p \in B$ is really just asking for $\varphi(q) = p$, which translates into $(\varphi^*)^{-1}(\mathfrak{n}) = \mathfrak{m}$ on the algebraic side. As such, we have the following.

Proposition 6.50 (Rank–nullity)**.** Fix two local rings R and S with maximal ideals $\mathfrak{m}$ and $\mathfrak{n}$, respectively. Given a map $\varphi : R \to S$ of local rings so that $\varphi(\mathfrak{m}) \subseteq \mathfrak{n}$, we have

$$\dim S \leq \dim R + \dim S/\mathfrak{m}S$$

In fact, if S is a flat as an R-module, then we have equality.

Proof. We use Proposition 6.48. For brevity, set $r := \dim R$ and $s := \dim S/\mathfrak{m}S$. As such, Proposition 6.48 promises us elements $\{f_1, \ldots, f_r\} \subseteq \mathfrak{m}$ and some $p \in \mathbb{N}$ such that

$$\mathfrak{m}^p \subseteq (f_1, \ldots, f_r) \subseteq \mathfrak{m}.$$

On the other hand, let $\pi : S \to S/\mathfrak{m}S$ be the natural projection and note that Lemma 3.89 implies that the only maximal ideal of $S/\mathfrak{m}S$ is $\pi\mathfrak{n}$ because this is the only maximal ideal of S containing $\mathfrak{m}S$. (Note $\mathfrak{n} \supseteq \mathfrak{m}S$ follows from $\varphi(\mathfrak{m}) \subseteq \mathfrak{n}$.) As such, Proposition 6.48 promises $\{\pi g_1, \ldots, \pi g_s\} \subseteq \pi\mathfrak{n}$ and $q \in \mathbb{N}$ so that

$$(\pi\mathfrak{n})^q \subseteq (\pi g_1, \ldots, \pi g_s) \subseteq \pi\mathfrak{n}.$$

Pulling back along π, we see that

$$\mathfrak{n}^q = (\mathfrak{n} + \mathfrak{m}S)^q \subseteq (g_1, \ldots, g_s) + \mathfrak{m}S \subseteq \mathfrak{n} + \mathfrak{m}S = \mathfrak{n}$$

because π^{-1} preserves inclusions.

We thus compute

$$\begin{aligned}
\mathfrak{n}^{pq} &= (\mathfrak{n}^q)^p \\
&\subseteq \big((g_1, \ldots, g_s) + \mathfrak{m}S\big)^p \\
&= \sum_{k=0}^{p} (g_1, \ldots, g_s)^k \cdot (\mathfrak{m}S)^{p-k} \\
&\subseteq (g_1, \ldots, g_s) + (\mathfrak{m}S)^p.
\end{aligned}$$

Now, $\mathfrak{m}S$ is generated by elements of the form $\varphi(x)$ for $x \in \mathfrak{m}$, so $(\mathfrak{m}S)^p$ is generated by elements of the form $\varphi(x_1) \cdot \ldots \cdot \varphi(x_p) = \varphi(x_1 \cdot \ldots \cdot x_p)$, which are exactly the generators of $\mathfrak{m}^p S$. As such, we can compute

$$\mathfrak{n}^{pq} \subseteq (g_1, \ldots, g_s) + (\mathfrak{m}S)^p \subseteq (g_1, \ldots, g_s) + (\varphi f_1, \ldots, \varphi f_d),$$

which is still contained in $\mathfrak{n}$ because all the generators are contained in $\mathfrak{n}$ by construction or in $\varphi\mathfrak{m} \subseteq \mathfrak{n}$ by construction. Thus, $\dim S \le r + s$ by Proposition 6.48, which is what we wanted. ■

We can even give an equality case to our Rank–nullity theorem. In particular, if we force S to be flat, then we expect to have "continuously varying" fibers, so we should not have any of the disruption of local problems that forced us to localize S. As such, we have the following.

Proposition 6.51. Fix two local rings R and S with maximal ideals $\mathfrak{m}$ and $\mathfrak{n}$, respectively. Given a map $\varphi : R \to S$ of local rings so that $\varphi(\mathfrak{m}) \subseteq \mathfrak{n}$ and S is flat as an R-module, we have

$$\dim S = \dim R + \dim S/\mathfrak{m}S.$$

Proof. Proposition 6.50 promises

$$\dim S \le \dim R + \dim S/\mathfrak{m}S,$$

so we need $\dim S \ge \dim R + \dim S/\mathfrak{m}S$. As before, set $r := \dim R$ and $s := \dim S/\mathfrak{m}S$ for brevity. By Lemma 6.16, we can pick up some chain of primes

$$\mathfrak{m}S \subseteq \mathfrak{p}_0 \subsetneq \mathfrak{p}_1 \subsetneq \cdots \subsetneq \mathfrak{p}_s,$$

so we set $\mathfrak{q} := \mathfrak{p}_0$. As such, we see $\dim \mathfrak{q} = \dim S/\mathfrak{m}S = s$ by Lemma 6.16 because being able to make any chain longer ascending from $\mathfrak{q}$ would make both $\dim \mathfrak{q}$ and $\dim S/\mathfrak{m}S$ larger. Notably, $\mathfrak{q}$ is a minimal prime over $\mathfrak{m}S$, lest we be able to insert a prime between $\mathfrak{m}S$ and $\mathfrak{p}_0$ in the above chain.

Now, Proposition 6.23 tells us that

$$\dim S \ge \dim \mathfrak{q} + \operatorname{codim} \mathfrak{q} = s + \operatorname{codim} \mathfrak{q},$$

so to get $\dim S \ge \dim R + \dim S/\mathfrak{m}S$, we need $\operatorname{codim} \mathfrak{q} \ge r$. We will show this by hand, taking chains of primes down in R up to S, so we pick up the following lemma.

Lemma 6.52 (Going down)**.** Fix a flat R-algebra S with $\varphi\colon R \to S$. Further, pick up prime ideals $\mathfrak{p}' \subseteq \mathfrak{p}$ in R such that we have a lift prime $\mathfrak{q}$ in S with $\mathfrak{p} = \varphi^{-1}\mathfrak{q}$. Then there is a $\mathfrak{q}' \subseteq \mathfrak{q}$ in S such that $\mathfrak{p}' = \varphi^{-1}\mathfrak{q}'$.

Proof. Pictorially, we are building $\mathfrak{q}'$ in the following diagram.

$$\begin{tikzcd}
\mathfrak{q}' \arrow[r, phantom, "\subseteq"] \arrow[d, dash] & \mathfrak{q} \arrow[r, phantom, "\subseteq"] \arrow[d, dash] & S \\
\mathfrak{p}' \arrow[r, phantom, "\subseteq"] & \mathfrak{p} \arrow[r, phantom, "\subseteq"] & R \arrow[u, "\varphi"']
\end{tikzcd}$$

For psychological reasons, we mod out by $\mathfrak{p}'$. Let $\alpha\colon R \twoheadrightarrow R/\mathfrak{p}'$ and $\beta\colon S \twoheadrightarrow S/\mathfrak{p}'S$ be the canonical projections. We have the following reduction checks.

- Note that $S/\mathfrak{p}'S \cong S \otimes_R R/\mathfrak{p}'$ (Proposition 2.96) is still flat as an $R/\mathfrak{p}'$-algebra by the composite

  $$R/\mathfrak{p}' \to S \otimes_R R/\mathfrak{p}' \cong S/\mathfrak{p}'S.$$

  Namely, the coset $r + \mathfrak{p}'$ goes to $\varphi(r) \otimes (1 + \mathfrak{p}') = 1_S \otimes (r + \mathfrak{p}')$ goes to $r1_S + \mathfrak{p}'S$; we call this map $\overline{\varphi}$. A direct explanation for the flatness was given on the homework, but the fastest way to see this is that, for any $R/\mathfrak{p}'$-module N, we have

  $$\operatorname{Tor}_1^{R/\mathfrak{p}'}(N, S \otimes_R R/\mathfrak{p}') \cong \operatorname{Tor}_1^{R/\mathfrak{p}'}(N \otimes_R R/\mathfrak{p}', S \otimes_R R/\mathfrak{p}') \cong R/\mathfrak{p}' \otimes_R \operatorname{Tor}_1^R(N, S) = 0,$$

  where we are using Theorem 4.133 and Lemma 4.128. It follows $S \otimes_R R/\mathfrak{p}'$ is indeed flat.

- Now, as noted in Lemma 6.16, modding out by $\mathfrak{p}'$ preserves primality, so $\beta\mathfrak{q}$ and $\alpha\mathfrak{p}$ and $\alpha\mathfrak{p}' = (0)$ are all still primes.

- We check that $\beta\mathfrak{q}$ still lies over $\alpha\mathfrak{p}$. We compute

  $$\overline{\varphi}^{-1}(\beta\mathfrak{q}) = \{r + \mathfrak{p}' : \overline{\varphi}(r + \mathfrak{p}') \in \beta\mathfrak{q}\} = \{r + \mathfrak{p}' : \varphi(r) + \mathfrak{p}'S \in \beta\mathfrak{q}\}.$$

  Now, because $\mathfrak{p}'S \subseteq \mathfrak{p}S \subseteq \mathfrak{q}$, we see that $\varphi(r) + \mathfrak{p}'S \in \beta\mathfrak{q}$ is equivalent to $\varphi(r) \equiv x \pmod{\mathfrak{p}'S}$ for some $x \in \mathfrak{q}$ is equivalent to $\varphi(r) \in \mathfrak{q}$. But this is equivalent to $r \in \varphi^{-1}\mathfrak{q} = \mathfrak{p}$, so we conclude

  $$\overline{\varphi}^{-1}(\beta\mathfrak{q}) = \{r + \mathfrak{p}' : r \in \mathfrak{p}\} = \alpha\mathfrak{p}.$$

- Lastly, we cover the conclusion. If we can find some prime $\beta\mathfrak{q}' \subseteq \beta\mathfrak{q}$ in $S/\mathfrak{p}'S$ lying over $\alpha\mathfrak{p}' = (0)$, then pulling back to S gives us a prime $\mathfrak{q}' = \beta\mathfrak{q}' + \mathfrak{p}'S$. Note $\mathfrak{p}'S \subseteq \mathfrak{q}'$ by construction, and because pre-images preserve inclusion, we get $\mathfrak{q}' \subseteq \mathfrak{q}$ as well.

  It remains to check that we will actually have $\mathfrak{q}'$ lying over $\mathfrak{p}'$. Certainly $\mathfrak{p}' \subseteq \varphi^{-1}\mathfrak{q}'$ because $\varphi\mathfrak{p}' \subseteq \mathfrak{p}'S \subseteq \mathfrak{q}'$ by construction.

  On the other hand, if $a \in \varphi^{-1}\mathfrak{q}'$, then $\varphi a \in \mathfrak{q}'$, so $\overline{\varphi}(a + \mathfrak{p}') = \varphi a + \mathfrak{p}'S \in \beta\mathfrak{q}'$. But $\beta\mathfrak{q}'$ lies over $\alpha\mathfrak{p}' = (0)$, so we conclude $a + \mathfrak{p}' = (0)$, so $a \in \mathfrak{p}'$. This finishes.

Thus, we may replace R with $R/\mathfrak{p}$, replace S with $S/\mathfrak{p}'S$, replace $\mathfrak{p}'$ and $\mathfrak{p}$ with $\alpha\mathfrak{p}' = (0)$ and $\alpha\mathfrak{p}$, and replace $\mathfrak{q}$ with $\beta\mathfrak{q}$. We have checked that S is still a flat R-algebra and that $\mathfrak{q}$ still lies over $\mathfrak{p}$, and we know that it will suffice to construct a prime $\mathfrak{q}' \subseteq \mathfrak{q}$ lying over $\mathfrak{p}'$.

However, we now know that $\mathfrak{p}' = (0)$ and that R is an integral domain. As such, here is our new diagram.

$$\begin{tikzcd}
\mathfrak{q}' \arrow[r, phantom, "\subseteq"] \arrow[d, dash] & \mathfrak{q} \arrow[r, phantom, "\subseteq"] \arrow[d, dash] & S \\
(0) \arrow[r, phantom, "\subseteq"] & \mathfrak{p} \arrow[r, phantom, "\subseteq"] & R \arrow[u, "\varphi"']
\end{tikzcd}$$

With this in mind, we define $\mathfrak{q}'$ to be a minimal prime (over (0)) contained in $\mathfrak{q}$, which certainly exists by saying something about Zorn's lemma.[2] Notably, $\mathfrak{q}' \subseteq \mathfrak{q}'$ is free, so it remains to show that

$$\varphi^{-1}(\mathfrak{q}) \stackrel{?}{=} (0).$$

Certainly $(0) \subseteq \varphi^{-1}(\mathfrak{q})$. On the other hand, fix any $a \in R \setminus \{0\}$, and we show $\varphi(a) \notin \mathfrak{q}'$. Indeed, because S is flat (!), we see

$$0 = \operatorname{Tor}_1^R(R/(a), S) \cong \{s \in S : \varphi(a)s = a \cdot s = 0\}$$

by Theorem 4.133 and Exercise 4.131.

In particular, $\varphi(a)$ is a non-zero-divisor in S, so $a \notin \mathfrak{q}'$ by minimality: viewing S as an S-module, we see $\operatorname{Ann}_S S = (0)$, so $\mathfrak{q}'$ being minimal over (0) implies that $\mathfrak{q}'$ is associated to S by Proposition 2.166 and so $\mathfrak{q}' = \operatorname{Ann} s$ for some $s \in S$, meaning that $\mathfrak{q}'$ only contains 0 and zero-divisors. This finishes. ■

Now, our lemma makes quick work of the theorem. From Lemma 6.47, we note that $r = \dim R = \operatorname{codim} \mathfrak{m}$, so Lemma 6.17 promises us a descending chain as follows.

$$\mathfrak{p}_0 \subsetneq \mathfrak{p}_1 \subsetneq \cdots \subsetneq \mathfrak{p}_{r-1} \subsetneq \mathfrak{p}_r = \mathfrak{m}.$$

Very quickly, we check that $\mathfrak{q}$ lies over $\mathfrak{m}$: by construction, $\mathfrak{q}$ is minimal over $\mathfrak{m}S$, so we get $\mathfrak{m} \subseteq \varphi^{-1}(\mathfrak{q})$ for free. But $\varphi^{-1}(\mathfrak{q})$ is prime and hence proper, so $\varphi^{-1}(\mathfrak{q}) \subseteq \mathfrak{m}$ follows because R is local.

As such, we may inductively apply Lemma 6.52 to build a chain of primes descending from $\mathfrak{q} := \mathfrak{q}_r$ as follows.

$$\begin{tikzcd}
\mathfrak{q}_0 \arrow[r, phantom, "\subseteq"] \arrow[d, dash] & \mathfrak{q}_1 \arrow[r, phantom, "\subseteq"] \arrow[d, dash] & \cdots \arrow[r, phantom, "\subseteq"] & \mathfrak{q}_{r-1} \arrow[r, phantom, "\subseteq"] \arrow[d, dash] & \mathfrak{q}_r \arrow[r, phantom, "\subseteq"] \arrow[d, dash] & S \arrow[d, dash, "\varphi"] \\
\mathfrak{p}_0 \arrow[r, phantom, "\subsetneq"] & \mathfrak{p}_1 \arrow[r, phantom, "\subsetneq"] & \cdots \arrow[r, phantom, "\subsetneq"] & \mathfrak{p}_{r-1} \arrow[r, phantom, "\subsetneq"] & \mathfrak{p}_r \arrow[r, phantom, "\subsetneq"] & R
\end{tikzcd}$$

Notably, all the $\mathfrak{q}_i$ are distinct because $\varphi^{-1}\mathfrak{q}_i = \mathfrak{p}_i$ are all distinct. Because we have exhibited a chain of distinct primes descending from $\mathfrak{q}$ of length r, Lemma 6.17 promises $\operatorname{codim} \mathfrak{q} \geq r$. This finishes. ■

Remark 6.53. At a high level, we have codified the notion that flat means continuously varying fibers: the dimension of the fiber $S/\mathfrak{m}S$ over the "point" $\mathfrak{m} \in \operatorname{Spec} R$ must be $\dim S - \dim R$ and therefore is constant!

Let's see an example of failed equality.

Exercise 6.54. Consider $S := k[x, y, z, w]/(xw - yz)$ to be the ring of singular matrices, as an algebra over $R := k[x, y]$. Further, set $\mathfrak{n} := (x, y, z, w) \subseteq S$ (which is maximal by Lemma 3.89) so that we take $\mathfrak{m} = (x, y) \subseteq R$. We track through the dimensions of Proposition 6.50 at $\mathfrak{n}$.

Proof. Let $\varphi : R \to S$ be the natural map by lifting id_k via $x \mapsto x$ and $y \mapsto y$. Very quickly, note that $\varphi^{-1}\mathfrak{n} = \mathfrak{m}$, as claimed: if we have some element map into $\mathfrak{n}$ as

$$\varphi\left(\sum_{i,j=0}^{\infty} a_{i,j} x^i y^j\right) = \sum_{i,j=0}^{\infty} a_{i,j} x^i y^j \in \mathfrak{n} = (x, y, z, w),$$

then we see $a_{0,0} \in \mathfrak{n}$ because all higher terms certainly live in $\mathfrak{n}$. But the only constant in $\mathfrak{n}$ is 0 because all nonzero constants are units, and $\mathfrak{n}$ is a proper ideal.

We now run the following computations.

[2] Set $\mathcal{S} := \{\mathfrak{q}' \in \operatorname{Spec} S : \mathfrak{q}' \subseteq \mathfrak{q}\}$. This is nonempty because $\mathfrak{q} \in \mathcal{S}$. All descending chains have a lower bound because primes are closed under intersection in chains.

- Using Lemma 6.47, we see $\dim R_\mathfrak{m} = \operatorname{codim} \mathfrak{m}R_\mathfrak{m}$, which equals $\operatorname{codim} \mathfrak{m} = 2$ by Lemma 6.36: notably, $\mathfrak{m}$ is the minimal prime over the principal ideal (x, y), so $\operatorname{codim} \mathfrak{m} \le 2$ by Theorem 6.43. But we also have the chain of primes
$$(0) \subseteq (x) \subseteq (x, y)$$
to witness $\operatorname{codim} \mathfrak{m} \ge 2$ by Lemma 6.17.

- Note that
$$\frac{S}{\mathfrak{m}S} = \frac{k[x, y, z, w]/(xw - yz)}{(x, y)k[x, y, z, w]/(xw - yz)} \cong \frac{k[x, y, z, w]}{(x, y) + (xw - yz)} = \frac{k[x, y, z, w]}{(x, y)} \cong k[w, z].$$
Now, localizing at $\mathfrak{n}$ preserves quotients because localization is flat, so
$$\frac{S_\mathfrak{n}}{\mathfrak{m}S_\mathfrak{n}} \cong \frac{S}{\mathfrak{m}S} \otimes_S S_\mathfrak{n} \cong k[w, z] \otimes_S S_\mathfrak{n} = k[w, z]_\mathfrak{n}.$$
Now, the S-action on $k[w, z]$ descends into an action by $k[x, y, z, w]/(x, y) = k[z, w]$, so localizing at $\mathfrak{n}$ is essentially localizing at (x, y). However, we now see that $\dim S_\mathfrak{n}/\mathfrak{m}S_\mathfrak{n} = \dim k[z, w]_{(z,w)} = 2$ by exactly the computation of the previous point.

- Note that $xw - yz \in k[x, y, z, w]$ is an irreducible by Example 3.104, so $(xw - yz)$ is a prime ideal because $k[x, y, z, w]$ is a unique factorization domain. In particular,
$$(0) \subseteq (xw - yz)$$
forces $\operatorname{codim}(xw - yz) \ge 1$ by Lemma 6.17 while $\operatorname{codim}(xw - yz) \le 1$ by Theorem 6.38 (note $(xw - yz)$ is the minimal prime over $(xw - yz)$). Thus, $\operatorname{codim}(xw - yz) = 1$, so Proposition 6.23 gives
$$\dim(xw - yz) + \operatorname{codim}(xw - yz) \le \dim k[x, y, z, w] = 4,$$
forcing $\dim S = \dim(xw - yz) \le 4 - 1 = 3$. In particular, using Proposition 6.23 tells us
$$\dim S_\mathfrak{n} = \operatorname{codim} \mathfrak{n} \le \dim S = 3.$$

In total, we see that
$$\dim S_\mathfrak{n} \le 3 < 2 + 2 = \dim R_\mathfrak{m} + \dim S_\mathfrak{n}/\mathfrak{m}S_\mathfrak{n},$$
which is what we wanted. ■

Remark 6.55. The above showed that the dimension of the fiber of S over $(x, y) = (0, 0)$ is 2, but "in general" the dimension over a fiber should be 1. Indeed, if $(a, b) \ne (0, 0)$, then
$$\frac{S}{(x - a, y - b)S} \cong \frac{k[x, y, z, w]}{(x - a, y - b) + (xw - yz)} \cong \frac{k[x, y, z, w]}{(x - a, y - b, aw - bz)} \cong k[w],$$
where in the last step we send $x \mapsto a$, send $y \mapsto b$, and send $w \mapsto b/a \cdot z$ if $a \ne 0$ or $z \mapsto a/b \cdot w$ if $b \ne 0$. So indeed, our fibers do not vary continuously, so we see that S should not be flat.

6.4.3 Consequences of the Rank–Nullity Theorem

As a quick corollary, we show the other side of "dimension is a local property": dimension is preserved by completion.

Corollary 6.56. Fix a Noetherian local ring R with maximal ideal $\mathfrak{m}$. Then $\dim R = \dim \widehat{R}$.

Proof. To start, we set $\iota : R \to \widehat{R}$ to be the natural inclusion. Note that $\widehat{R}$ is local with maximal ideal $\widehat{\mathfrak{m}}$ by Corollary 5.27, and we note that

$$\iota\mathfrak{m} \subseteq \mathfrak{m}\widehat{R} = \widehat{\mathfrak{m}},$$

where the last equality is by Proposition 5.33. So we see that ι is indeed a good map of local rings.

Continuing, we note that $\widehat{R}$ is flat as an R-algebra by Theorem 5.38, so Proposition 6.51 promises

$$\dim \widehat{R} = \dim R + \dim \widehat{R}/\widehat{\mathfrak{m}}.$$

However, $\widehat{R}/\widehat{\mathfrak{m}} \cong R/\mathfrak{m}$ by definition of $\widehat{\mathfrak{m}}$, so we conclude $\dim \widehat{R}/\widehat{\mathfrak{m}} = \dim R/\mathfrak{m} = 0$ because $R/\mathfrak{m}$ is a field (all primes are maximal because all proper ideals are (0)). It follows

$$\dim \widehat{R} = \dim R,$$

which is what we wanted. ■

And here is another corollary: we are finally able to compute the dimension of polynomial rings.

Proposition 6.57. Fix a Noetherian ring R with finite dimension. Then $\dim R[x] = \dim R + 1$.

Proof. We split the proof into two parts. For brevity, set $r := \dim R$.

- We start by showing $\dim R[x] \ge r+1$; we do this by manually constructing a chain of primes of length $r+1$. Well, because $r = \dim R$, we may pick up a chain

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

  Lifting these to $R[x]$, we get the chain

$$\mathfrak{p}_0 R[x] \subseteq \mathfrak{p}_1 R[x] \subseteq \cdots \subseteq \mathfrak{p}_r R[x].$$

  The point is to show that this is a distinct chain of primes in $R[x]$, and then we'll add $\mathfrak{p}_r R[x] + (x)$ to the end.

  Note that these ideals $\mathfrak{p}_i R[x]$ are prime because, for any prime $\mathfrak{p} \subseteq R$, we have

$$\frac{R[x]}{\mathfrak{p}R[x]} \cong (R/\mathfrak{p})[x],$$

  where the isomorphism is by lifting the natural projection map $R \twoheadrightarrow R/\mathfrak{p}$ via $x \mapsto x$. (Surjectivity of this morphism $R[x] \to (R/\mathfrak{p})[x]$ is clear. The kernel consists of all elements of $R[x]$ all of whose coefficients live in $\mathfrak{p}$, which is $\mathfrak{p}R[x]$.) Now, $(R/\mathfrak{p})[x]$ is a polynomial ring over an integral domain and hence is an integral domain, so we conclude $\mathfrak{p}R[x]$ is indeed prime.

  Further, the primes $\mathfrak{p}_i R[x]$ are distinct because passing $\mathfrak{p}_i R[x]$ through the map $R[x] \to R$ evaluating $x \mapsto 0$ recovers the constant terms in $\mathfrak{p}_i R[x]$, which is simply $\mathfrak{p}_i$. So the map $\mathfrak{p} \mapsto \mathfrak{p}R[x]$ has a left inverse and hence must be injective. So we indeed have the chain of distinct primes

$$\mathfrak{p}_0 R[x] \subsetneq \mathfrak{p}_1 R[x] \subsetneq \cdots \subsetneq \mathfrak{p}_r R[x]$$

  of length r in $R[x]$.

  Lastly, we note that $\mathfrak{p}_r R[x] + (x)$ is a prime ideal because

$$\frac{R[x]}{\mathfrak{p}_r R[x] + (x)} \cong R/\mathfrak{p}_r,$$

where the isomorphism is by lifting $R \mapsto R/\mathfrak{p}_r$ with $x \mapsto 0$; in other words, we extract the constant term and take it $\pmod{\mathfrak{p}_r}$. Certainly this map is surjective (everyone in R is eligible to be a constant term), and $\mathfrak{p}_r R[x] + (x)$ lives in its kernel; conversely, the kernel consists exactly of the elements with constant term in $\mathfrak{p}_r$, which is $\mathfrak{p}_r + (x) = \mathfrak{p}_r R[x] + (x)$.

However, note $\mathfrak{p}_r R[x] \subsetneq \mathfrak{p}_r R[x] + (x)$ because $x \notin \mathfrak{p}_r R[x]$ (the coefficient of x is 1, which is not in $\mathfrak{p}_r$) while $x \in \mathfrak{p}_r R[x] + (x)$. As such, we have a chain of distinct primes

$$\mathfrak{p}_0 R[x] \subsetneq \mathfrak{p}_1 R[x] \subsetneq \cdots \subsetneq \mathfrak{p}_r R[x] \subsetneq \mathfrak{p}_r R[x] + (x)$$

of length $r+1$ in $R[x]$. Thus, $\dim R[x] \geq r + 1 = \dim R + 1$.

- We show $\dim R[x] \leq \dim R + 1$ by Proposition 6.50. Well, suppose that we have a chain of primes

$$\mathfrak{q}_0 \subsetneq \mathfrak{q}_1 \subsetneq \cdots \subsetneq \mathfrak{q}_d \qquad (*)$$

for some d; we will show that $d \leq r+1$, which will be enough. Note that, if $\mathfrak{q}_d$ is not a maximal ideal, then we can place $\mathfrak{q}_d$ inside a maximal ideal $\mathfrak{n}$ and then replace $\mathfrak{q}_d$ with $\mathfrak{n}$ because we still have $\mathfrak{q}_{d-1} \subsetneq \mathfrak{q}_d \subseteq \mathfrak{n}$. Notably, we still have a chain of distinct primes of length d, and we'll still show $d \leq r + 1$.

As such, we can assume that $\mathfrak{n} := \mathfrak{q}_d$ is a maximal ideal. Very quickly, note that we have the natural map $\iota : R \hookrightarrow R[x]$, and we note $\iota^{-1}\mathfrak{n}$ (i.e., $\mathfrak{n} \cap R$) is a maximal ideal: certainly $\iota^{-1}\mathfrak{n}$ is prime and hence proper. On the other hand, if

$$\iota^{-1}\mathfrak{n} \subseteq I \subsetneq R,$$

then $I = \iota^{-1}\mathfrak{n} + I$ still does not contain 1_R, so $\mathfrak{n} + IR[x]$ still cannot 1_R because the constant terms of $\mathfrak{n} + IR[x]$ are precisely $\iota^{-1}\mathfrak{n} + I$. So $\mathfrak{n} + IR[x]$ is a proper ideal containing $\mathfrak{m}fn$, so $\mathfrak{n} + IR[x] = \mathfrak{n}$, so $IR[x] \subseteq \mathfrak{n}$, so $I \subseteq \iota^{-1}\mathfrak{n}$, so $\iota^{-1}\mathfrak{n} = I$.

Thus, we set $\mathfrak{m} := \iota^{-1}\mathfrak{n}$ and so $\iota\mathfrak{m} \subseteq \mathfrak{n}$. Localizing, we see that Proposition 6.50 promises

$$\dim R[x]_{\mathfrak{n}} \leq \dim R_{\mathfrak{m}} + \dim R[x]_{\mathfrak{n}}/(\mathfrak{m}R_{\mathfrak{m}})R[x]_{\mathfrak{n}}.$$

We now compute each of these terms.

  - Note that $\dim R[x]_{\mathfrak{n}} = \operatorname{codim} \mathfrak{n} = \operatorname{codim} \mathfrak{q}_d \geq d$ from $(*)$.
  - Note that $\dim R_{\mathfrak{m}} = \operatorname{codim} \mathfrak{m} \leq \dim R = r$ by Proposition 6.23.
  - Lastly, we compute $\dim R[x]_{\mathfrak{n}}/(\mathfrak{m}R_{\mathfrak{m}})R[x]_{\mathfrak{n}}$. Intuitively, this is a localization of $R[x]/\mathfrak{m}R[x]$, which is $(R/\mathfrak{m})[x]$, which is a polynomial ring over a field and hence a principal ideal domain (while not a field) and therefore has dimension 1.

    Rigorizing this computation is quite annoying, so we will be a little terse. Note that $\mathfrak{n}/\mathfrak{m}R[x]$ is a maximal ideal of $R[x]/\mathfrak{m}R[x]$ by Lemma 3.89, and so $\mathfrak{n}/\mathfrak{m}R[x]$ will go to a maximal ideal $\mathfrak{n}'$ under the isomorphism

$$\frac{R[x]}{\mathfrak{m}R[x]} \cong (R/\mathfrak{m})[x],$$

    induced by $R \twoheadrightarrow R/\mathfrak{m}$ and $x \mapsto x$. Thus, we compute

$$\dim \left(\frac{R[x]}{\mathfrak{m}R[x]}\right)_{\mathfrak{n}/\mathfrak{m}R[x]} = \dim \left((R/\mathfrak{m})[x]\right)_{\mathfrak{n}'} = 1,$$

    where the last equality is because $\mathfrak{n}'$ is a nonzero prime of the principal ideal domain $(R/\mathfrak{m})[x]$. So to finish, we claim that

$$\frac{R[x]_{\mathfrak{n}}}{(\mathfrak{m}R_{\mathfrak{m}})R[x]_{\mathfrak{n}}} \cong \left(\frac{R[x]}{\mathfrak{m}R[x]}\right)_{\mathfrak{n}/\mathfrak{m}R[x]}.$$

    This will finish because it shows that $\dim R[x]_{\mathfrak{n}}/(\mathfrak{m}R_{\mathfrak{m}})R[x]_{\mathfrak{n}} = 1$.

We manually exhibit maps in both directions. In one direction, we have a map

$$R[x] \to \frac{R[x]}{\mathfrak{m}R[x]} \to \left(\frac{R[x]}{\mathfrak{m}R[x]}\right)_{\mathfrak{n}/\mathfrak{m}R[x]}$$

sending $p(x)$ to $\frac{[p(x)]_{\mathfrak{m}R[x]}}{1}$ and in particular all elements of $R[x] \setminus \mathfrak{n}$ to a unit (notably, $\mathfrak{m}R[x] \subseteq \mathfrak{n}$, so this localization is legal), so we get an induced map from $R[x]_{\mathfrak{n}}$ by the universal property. By definition, we can see that $(\mathfrak{m}R_{\mathfrak{m}})R[x]_{\mathfrak{n}}$ will end up in the kernel, so we get an induced map

$$\varphi : \frac{R[x]_{\mathfrak{n}}}{(\mathfrak{m}R_{\mathfrak{m}})R[x]_{\mathfrak{n}}} \to \left(\frac{R[x]}{\mathfrak{m}R[x]}\right)_{\mathfrak{n}/\mathfrak{m}R[x]}$$

by sending

$$\varphi : \left[\frac{p(x)}{q(x)}\right]_{\mathfrak{m}R_{\mathfrak{m}}R[x]_{\mathfrak{n}}} \mapsto \frac{[p(x)]_{\mathfrak{m}R[x]}}{[q(x)]_{\mathfrak{m}R[x]}}.$$

In the other direction, we note that we have a map

$$R[x] \to R[x]_{\mathfrak{n}} \to \frac{R[x]_{\mathfrak{n}}}{(\mathfrak{m}R_{\mathfrak{m}})R[x]_{\mathfrak{n}}}$$

sending $p(x)$ to $\left[\frac{p(x)}{1}\right]_{(\mathfrak{m}R_{\mathfrak{m}})R[x]_{\mathfrak{n}}}$. In particular, we can see that any element of $\mathfrak{m}R[x]$ goes to 0 immediately, so we get an induced map from $R[x]/\mathfrak{m}R[x]$. However, we see further that any $[p] \notin \mathfrak{n}/\mathfrak{m}R[x]$ will go to a unit because it's mapping to $\frac{p(x)}{1}$, which is a unit in $R[x]_{\mathfrak{n}}$ with inverse $\frac{1}{p(x)}$. As such, we get an induced map

$$\psi : \left(\frac{R[x]}{\mathfrak{m}R[x]}\right)_{\mathfrak{n}/\mathfrak{m}R[x]} \to \frac{R[x]_{\mathfrak{n}}}{(\mathfrak{m}R_{\mathfrak{m}})R[x]_{\mathfrak{n}}}$$

by sending

$$\psi : \frac{[p(x)]_{\mathfrak{m}R[x]}}{[q(x)]_{\mathfrak{m}R[x]}} \mapsto \left[\frac{p(x)}{q(x)}\right]_{\mathfrak{m}R_{\mathfrak{m}}R[x]_{\mathfrak{n}}}$$

Tracking through φ and ψ shows that they are inverse essentially immediately, so we get our isomorphism.

Plugging in, we see that

$$d \leq r + 1,$$

which is what we wanted.

The above inequalities finish the proof. ■

Corollary 6.58. For a field k, we have $k[x_1, \ldots, x_n] = n$.

Proof. This follows by induction on n. For $n = 0$, we are showing that $\dim k = 0$, which follows because all prime ideals are maximal because all proper ideals are (0) in a field. Then the inductive step is Proposition 6.57 because we compute

$$\dim k[x_1, \ldots, x_{n+1}] = \dim k[x_1, \ldots, x_n] + 1 = n + 1$$

by induction. ■

6.4.4 Dimension for Modules

We now add a notion of Krull dimension for modules.

Definition 6.59 (Krull dimension, modules)**.** Given an R-module M, we define the *dimension* of M as $\dim M := \dim R/\operatorname{Ann} M$.

As in the case of Artinian rings, it will be useful to be more closely monitor the dimension-0 case.

Definition 6.60 (Colength)**.** Fix an ideal $\mathfrak{q} \subseteq R$. Then $\mathfrak{q}$ *has finite colength* on a module M if and only if $M/\mathfrak{q}M$ has finite length. We might also say that $\mathfrak{q}$ is a *parameter ideal.*

We have the following check.

Lemma 6.61. Fix a Noetherian local ring R with maximal ideal $\mathfrak{m}$, and let M be a finitely generated R-module. Then an R-ideal $\mathfrak{q} \subseteq R$ has finite colength if and only if there exists an integer n so that

$$\mathfrak{m}^n \subseteq \mathfrak{q} + \operatorname{Ann} M.$$

Proof. For motivation, we quickly check that $M' := M/\mathfrak{m}^n M$ has finite length for all n. The main intermediate claim is that $R/\operatorname{Ann} M'$ is Artinian; by Theorem 2.126, it suffices to show that all primes of R containing $\operatorname{Ann} M'$ are maximal. However, a prime $\mathfrak{p}$ containing $\operatorname{Ann} M'$ contains $\mathfrak{m}^n$ and hence contains $\mathfrak{m}$ and hence $\mathfrak{p} = \mathfrak{m}$ is maximal.

But now, again using Theorem 2.126, we note that $R/\operatorname{Ann} M'$ has finite length as a ring but also as an R-module because the $R/\operatorname{Ann} M'$-action is the same as the R-action. So because M' is finitely generated as an R-module but really as an $R/\operatorname{Ann} M'$-module (again, the actions match, so we might as well mod out by $\operatorname{Ann} M'$), we have a surjection of R-modules

$$(R/\operatorname{Ann} M')^n \twoheadrightarrow M'$$

for some n. It follows from Proposition 2.117 that M' has finite length.

We now show the two directions independently.

- Suppose there exists some n for which $\mathfrak{m}^n \subseteq \mathfrak{q} + \operatorname{Ann} M$. Then we have the surjection

$$M/\mathfrak{m}^n M \twoheadrightarrow \frac{M}{(\mathfrak{q} + \operatorname{Ann} M)M} \to 0.$$

  It follows by Proposition 2.117 that $M/(\mathfrak{q} + \operatorname{Ann} M)M = M/\mathfrak{q}M$ has finite length; notably, $(\mathfrak{q} + \operatorname{Ann} M)M = \mathfrak{q}M$ because $\operatorname{Ann} M$ merely annihilates all of M.

- Conversely, suppose that $M/\mathfrak{q}M$ has finite length; the idea is to use the Krull intersection theorem. In particular, Theorem 4.41 grants us $r \in \mathfrak{m}$ such that

$$(1-r) \cdot \left(\bigcap_{s \geq 0} \mathfrak{m}^s (M/\mathfrak{q}M) \right) = 0.$$

  However, $1 - r$ is a unit because R is local and $\mathfrak{m}$ is its unique maximal ideal, so we conclude

$$\bigcap_{s \geq 0} \mathfrak{m}^s (M/\mathfrak{q}M) = 0.$$

  Now, $\mathfrak{m}^s(M/\mathfrak{q}M)$ is a descending chain of submodules, which must stabilize because $M/\mathfrak{q}M$ has finite length. But this stabilization must be 0 because of the above intersection, so we conclude that there exists some $n \in \mathbb{N}$ for which

$$\mathfrak{m}^n \cdot (M/\mathfrak{q}M) = 0.$$

  So we are done upon noting that the annihilator of $M/\mathfrak{q}M$ is $\mathfrak{q} + \operatorname{Ann} M$, so $\mathfrak{m}^n \subseteq \mathfrak{q} + \operatorname{Ann} M$.

The above implications complete the proof. ■

As usual, our notion of size behaves in short exact sequences.

Proposition 6.62. Fix a Noetherian ring R and pick up a short exact sequence of R-modules

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

If $\mathfrak{q}$ has finite colength on A and C, then $\mathfrak{q}$ has finite colength on B.

Proof. Tensoring the given short exact sequence with $R/\mathfrak{q}$, we get the right-exact sequence

$$A/\mathfrak{q}A \to B/\mathfrak{q}B \to C/\mathfrak{q}C \to 0.$$

For concreteness, let the last map be $\pi\colon B/\mathfrak{q}B \to C/\mathfrak{q}C$. Then $A/\mathfrak{q}A$ surjects onto $\ker\pi$ by the exactness above, so because $A/\mathfrak{q}A$ has finite length, Proposition 2.117 tells us that $\ker\pi$ has finite length. But then the short exact sequence

$$0 \to \ker\pi \to B/\mathfrak{q}B \xrightarrow{\pi} C/\mathfrak{q}C$$

tells us that $B/\mathfrak{q}B$ has finite length by Proposition 2.117 again. ■

The punchline of defining finite colength is the following result.

Proposition 6.63. Fix a Noetherian local ring R with maximal ideal $\mathfrak{m}$ and an R-module M. Then $\dim M$ is equal to the minimal d such that there is some proper ideal $(f_1, \ldots, f_d) \subseteq R$ with finite colength on M.

Proof. The point is to use Proposition 6.48. Namely, the dimension of the module M is equal to the dimension of the ring $R/\operatorname{Ann} M$. Now, $R/\operatorname{Ann} M$ is still local with maximal ideal $\mathfrak{m}/\operatorname{Ann} M$, so its dimension by Proposition 6.48 is the smallest d for which there is a proper R-ideal with

$$\mathfrak{m}^n/\operatorname{Ann} M \subseteq (f_1, \ldots, f_d) \subseteq \mathfrak{m}$$

for some n. Equivalently, we are asking for

$$\mathfrak{m}^n \subseteq (f_1, \ldots, f_d) + \operatorname{Ann} M,$$

which by Lemma 6.61 is equivalent to $(f_1, \ldots, f_d)$ having finite colength on M. ■

Proposition 6.64. Fix a local ring R with maximal ideal $\mathfrak{m}$ and an R-module M. Given $x \in \mathfrak{m}$, we have

$$\dim M/xM \geq \dim M - 1.$$

Proof. The point is to use Proposition 6.63 twice. Set $d := \dim M/xM$ and will show

$$\dim M \overset{?}{\leq} d + 1.$$

Now, Proposition 6.63 grants us a proper ideal $(f_1, \ldots, f_d)$ with finite colength on M/xM. Namely,

$$\frac{M/xM}{(f_1, \ldots, f_d) \cdot M/xM} \cong \frac{M}{((f_1, \ldots, f_d) + (x))M} = \frac{M}{(f_1, \ldots, f_d, x)M}$$

has finite length. However, using Proposition 6.63 again, we see that $\dim M$ is then at most $d + 1$. This finishes. ■

6.4.5 Regular Rings

We close class by defining regular.

Definition 6.65 (Regular)**.** Fix a local ring R of dimension $d := \dim R$. Further, let $\mathfrak{m}$ be the maximal ideal of R. Then R is *regular* if and only if there exist elements $\{f_1, \ldots, f_d\} \subseteq R$ such that

$$\mathfrak{m} = (f_1, \ldots, f_d).$$

In particular, because R is local, $\operatorname{codim} \mathfrak{m} = \dim R$ (see Lemma 6.47), so Corollary 6.46 tells us that $\mathfrak{m}$ is at least a minimal prime over some ideal generated by d elements. The regularity condition strengthens being minimal over to having a full equality.

Here are some examples.

Example 6.66. Fix $R := k[x_1, \ldots, x_d]_{\mathfrak{m}}$, where $\mathfrak{m} = (x_1, \ldots, x_d)$. Then R is regular because $\dim R = d$. To see that $\dim R = d$, note on one hand that

$$\dim R = \operatorname{codim} \mathfrak{m} \le \dim k[x_1, \ldots, x_d] = d.$$

On the other hand,

$$(0) \subsetneq (x_1) \subsetneq (x_1, x_2) \subsetneq \cdots \subsetneq (x_1, \ldots, x_d)$$

is a chain of distinct primes in R by Theorem 2.29, so $\dim R \ge d$.

Example 6.67. The completion $R := k[\![x_1, \ldots, x_n]\!]$ is regular. Here, $\dim R = d$ by Corollary 6.56 and Corollary 6.58, and our maximal ideal is

$$(x_1, \ldots, x_d),$$

which is indeed generated by d elements.

Example 6.68. Any local principal ideal domain R which is not a field has dimension 1, and the maximal ideal also is generated by one element (because the ring is principal), so R is regular.

Let's get some practice with this definition.

Proposition 6.69. Let R be a Noetherian regular local ring with maximal ideal $\mathfrak{m}$. Then

$$\dim_{R/\mathfrak{m}} \mathfrak{m}/\mathfrak{m}^2 = \dim R.$$

Proof. As some quick type-checking, note that $\mathfrak{m}/\mathfrak{m}^2$ is in fact annihilated by $\mathfrak{m}$ (namely, $\mathfrak{m} \cdot \mathfrak{m}/\mathfrak{m}^2 = 0$), so it is an $R/\mathfrak{m}$-vector space. We now show two inequalities to finish the proof.

- We show $\dim_{R/\mathfrak{m}} \mathfrak{m}/\mathfrak{m}^2 \le \dim R$. For brevity, set $d := \dim R$. Here we use the fact that R is regular: by definition, we can find $f_1, \ldots, f_d \in \mathfrak{m}$ so that

  $$\mathfrak{m} = (f_1, \ldots, f_d).$$

  In particular, the $f_\bullet$ generate $\mathfrak{m}$ as an R-module, so it follows that they span $\mathfrak{m}/\mathfrak{m}^2$ as an R-module as well. But the R-action descends to an $R/\mathfrak{m}$-action, so the $f_\bullet$ provide a spanning set of d elements.

- We show $\dim_{R/\mathfrak{m}} \mathfrak{m}/\mathfrak{m}^2 \ge \dim R$. For brevity, set $d' := \dim_{R/\mathfrak{m}} \mathfrak{m}/\mathfrak{m}^2$ so that we can find a basis

  $$\left\{f_1 + \mathfrak{m}^2, \ldots, f_{d'} + \mathfrak{m}^2\right\}$$

for $\mathfrak{m}/\mathfrak{m}^2$. Thus, Corollary 3.36 (applied to the R-module $\mathfrak{m}$) tells us that these elements $f_1, \ldots, f_{d'}$ will generate $\mathfrak{m}$, giving

$$\mathfrak{m} = (f_1, \ldots, f_{d'}),$$

It follows from Theorem 6.43 that $\dim R = \operatorname{codim} \mathfrak{m} \le d'$, which is what we wanted.

The above inequalities establish that $\dim_{R/\mathfrak{m}} \mathfrak{m}/\mathfrak{m}^2 = \dim R$, finishing the proof. ■

And here is a last result.

Proposition 6.70. A Noetherian regular local ring is an integral domain.

Proof. Let R be a regular local ring with maximal ideal $\mathfrak{m}$. We proceed by induction on $\dim R$. If $\dim R = 0$, then $\mathfrak{m}$ is generated by zero elements, so $\mathfrak{m} = (0)$, so (0) is maximal and hence prime, so R is an integral domain.

Now, for the inductive step, suppose that $d := \dim R > 0$. The idea is to reduce to use the inductive hypothesis on some suitable quotient $R/(x)$. We do this construction and application in steps.

1. Because $\operatorname{codim} \mathfrak{m} = d > 0$ (see Lemma 6.47), we see that $\mathfrak{m}$ is not a minimal prime (over (0)).

   We now use prime avoidance to conjure our desired $x \in R$: by Proposition 2.175, we see that there are finitely many minimal primes, and $\mathfrak{m}$ strictly contains all of these. Additionally, $\mathfrak{m}^2 \ne \mathfrak{m}$ because $\mathfrak{m}^2 = \mathfrak{m}$ would imply $\mathfrak{m} = 0$ by Theorem 3.33 and hence $\dim R = 0$. In total, Lemma 2.165 promises us some $xin\mathfrak{m}$ which does not live in any minimal prime nor in $\mathfrak{m}^2$.

2. As such, $\dim(x) < d$ (using Lemma 6.16) because any chain of primes

$$(x) \subseteq \mathfrak{p}_0 \subsetneq \mathfrak{p}_1 \subsetneq \cdots \subsetneq \mathfrak{p}_{d'}$$

   cannot have $\mathfrak{p}_0$ a minimal prime, so there is some prime $\mathfrak{p}_{-1}$ strictly contained in $\mathfrak{p}_0$. This gives us a chain of distinct primes of length $d'+1$ in R, so $d' \le d-1 < d$, so $\dim(x) < d$ follows.

3. Thus, $\dim R/(x) < \dim R$. We would therefore like to apply the inductive hypothesis to $R/(x)$, but we need to know that $R/(x)$ is regular. To start, we note that $R/(x)$ is local with maximal ideal $\mathfrak{m}/(x)$, which we need to provide generators for. How many generators? Well, we note Proposition 6.64 tells us that

$$\dim R/(x) \ge \dim R - 1$$

   where dimension is as R-modules, but $R/(x)$-ideals are the same as the R-submodules of $R/(x)$, so we might as well compute these dimensions as rings. As such, we get that $\dim R/(x) = \dim R - 1$.

4. To show R is regular, we now need to generate $\mathfrak{m}/(x)$ by $d-1$ elements. To get our generators, we cheat by using Nakayama's lemma. In particular, by Corollary 3.36, it suffices to generate

$$\frac{\mathfrak{m}/(x)}{\mathfrak{m}/(x) \cdot \mathfrak{m}/(x)} = \frac{\mathfrak{m}/(x)}{\mathfrak{m} \cdot \mathfrak{m}/(x)} = \frac{\mathfrak{m}/(x)}{\mathfrak{m}^2/(x)} \cong \frac{\mathfrak{m}}{\mathfrak{m}^2 + (x)}$$

   by $d-1$ elements. However, $\dim_{R/\mathfrak{m}} \mathfrak{m}^2/\mathfrak{m} = d$ by Proposition 6.69, and

$$\frac{\mathfrak{m}}{\mathfrak{m}^2} \twoheadrightarrow \frac{\mathfrak{m}}{\mathfrak{m}^2 + (x)}$$

   is a map with nontrivial kernel—namely, $x + \mathfrak{m}^2$ lives in the kernel, and $x \notin \mathfrak{m}^2$ by construction (!). Thus,

$$\dim_{R/\mathfrak{m}} \frac{\mathfrak{m}}{\mathfrak{m}^2 + (x)} < \dim \frac{\mathfrak{m}}{\mathfrak{m}^2} = d,$$

   so we can in fact generate $\mathfrak{m}/\left((x) + \mathfrak{m}^2\right)$ by strictly fewer than d elements and hence by $d-1$ elements (by just choosing some large spanning set).

From the above construction, $R/(x)$ is in fact a regular local ring of dimension $d-1$ and hence an integral domain by the inductive hypothesis. We now show that R is an integral domain by showing that $(0) \subseteq R$ is prime. Certainly (x) contains some minimal prime $\mathfrak{q}$ because x was chosen outside all minimal primes. As such, we claim that

$$\mathfrak{q} \stackrel{?}{=} (x) \cdot \mathfrak{q},$$

which will show $\mathfrak{q} = (0)$ by Theorem 3.33 finishing. Certainly $(x)\cdot\mathfrak{q} \subseteq \mathfrak{q}$. In the other direction, any $y \in \mathfrak{q} \subseteq (x)$ can be written as $y = ax$ for some $a \in R$, but $ax \in \mathfrak{q}$ with $x \notin \mathfrak{q}$ (recall x is outside all minimal primes), we conclude $a \in \mathfrak{q}$, so $y \in (x)\mathfrak{q}$. ■

6.5 April 5

Welcome back.

6.5.1 Discrete Valuation Rings

This subsection will focus on regular local rings R of dimension 1, which turn out to be "discrete valuation rings." For example, Proposition 6.70 tells us that such rings R must be integral domains, so we have some inkling that such rings must be nice. Further, the maximal ideal $\mathfrak{m} \subseteq R$ must be principal because R is regular, so we set

$$\mathfrak{m} = (\pi)$$

for some $\pi \in R$. This turns out to make R very nice.

Proposition 6.71. Fix a Noetherian regular local ring R of dimension 1, with maximal ideal $\mathfrak{m} := (\pi)$. Then all nonzero ideals of R are of the form $\left(\pi^k\right)$ for some natural number k. In particular, R is a principal ideal domain.

Proof. The key is to show that any $r \in R \setminus \{0\}$ can be written as $u\pi^n$ for some $n \in \mathbb{N}$ and $u \in R^\times = R \setminus (\pi)$. For this, we use the Krull intersection theorem: by Corollary 4.43, we see that

$$\bigcap_{n\geq 0} (\pi^n) = \bigcap_{n\geq 0} (\pi)^n = 0.$$

Thus, $r \neq 0$ is not in the intersection of all the π^n even though certainly $r \in \left(\pi^0\right) = R$, so there exists some least $n \geq 1$ such that $r \notin \left(\pi^{n+1}\right)$. Notably, because n is the least such, we have

$$r \in (\pi^n) \setminus \left(\pi^{n+1}\right).$$

As such, we can write $r = u\pi^n$, but $u \notin (\pi)$ because this would imply $r \in \left(\pi^{n+1}\right)$. This is what we wanted.

We take a moment to note that representation as $u\pi^n$ is in fact unique: suppose $u\pi^a = v\pi^b$ for $u, v \notin (\pi)$ and $a, b \in \mathbb{N}$. Without loss of generality, take $a \geq b$ so that R being an integral domain (by Proposition 6.70) gives

$$u\pi^{a-b} = v \notin (\pi).$$

Thus, $a - b < 1$, so $a = b$ follows. In this case, the above equation reads $a = b$.

In total, we have written all elements $r \in R \setminus \{0\}$ uniquely in the form $u\pi^n$ for some $u \notin (\pi)$ and $n \in \mathbb{N}$. As such, we may define the function $\nu\colon R \setminus \{0\} \to \mathbb{N}$ by

$$\nu(r) := n.$$

In particular, $r/\pi^{\nu(r)} = u \in R^\times$ implies that $(r) = \left(\pi^{\nu(r)}\right)$.

We are now ready to attack the proof directly. Suppose that $I \subseteq R$ is a nonzero ideal. Then we set

$$\nu := \min\{\nu(a) : a \in I \setminus \{0\}\},$$

where the minimum is well-defined because $I \neq (0)$; in particular, this is some $x \in I$ with $\nu(x) = \nu$. Now, $a \geq b$ implies that $(\pi^a) \subseteq (\pi^b)$, so we write

$$I = \bigcup_{r \in I \setminus \{0\}} (r) = \bigcup_{r \in I \setminus \{0\}} \left(\pi^{\nu(r)}\right) \subseteq \bigcup_{r \in I} (\pi^\nu) = (\pi^\nu) = (x) \subseteq I.$$

Thus, equalities follow, and we get $I = (x) = (\pi^\nu)$, which finishes the proof. ■

As mentioned above, these rings are actually called discrete valuation rings. Let's explain this.

Definition 6.72 (Totally ordered group)**.** A group Γ endowed with a total order $\geq$ is a *totally ordered group* if and only if $a \geq b$ for $a, b \in G$ implies

$$ac \geq bc \qquad \text{and} \qquad ca \geq cb$$

for any $c \in G$.

Example 6.73. The group $(\mathbb{Z}, +)$ is an ordered group under the usual ordering $\geq$. The coherence check is that $a \geq b$ implies $a + c \geq b + c$.

Example 6.74. Exactly analogously to Example 6.73, $(\mathbb{R}, +)$ is an ordered group under the usual ordering $\geq$; the coherence check is the same.

The reason we have defined totally ordered groups is to be able to define valuations.

Definition 6.75 (Valuation)**.** Fix a domain R and totally ordered group Γ. A *valuation* ν is a group homomorphism $\nu \colon K(R)^\times \to \Gamma$ satisfying the following.

- We have $\nu(a + b) \geq \min\{\nu(a), \nu(b)\}$.
- We have $R = \{x \in K(R)^\times : \nu(x) \geq 0\} \cup \{0\}$.

When the codomain of our valuation is $\mathbb{Z}$, these rings have a special name.

Definition 6.76 (Discrete valuation ring)**.** A *discrete valuation ring* is an integral domain R equipped with a valuation $\nu \colon K(R)^\times \to \mathbb{Z}$.

Example 6.77. Suppose that R is a field. Then we claim R is a discrete valuation ring. Indeed, set $\nu \colon K(R)^\times \to \mathbb{Z}$ by $\nu(x) = 0$ always. We have the following checks.

- Homomorphism: note $\nu(a) + \nu(b) = 0 = \nu(a + b)$ for any $a, b \in K(R)^\times$.
- Note $\nu(a + b) = 0 \geq 0 = \min\{\nu(a), \nu(b)\}$ for any $a, b \in K(R)^\times$.
- Lastly, note $\nu(x) = 0 \geq 0$ for all $x \in K(R)^\times$, so

  $$\{x \in K(R)^\times : \nu(x) \geq 0\} \cup \{0\} = K(R)^\times \cup \{0\} = K(R) = R,$$

  where the last equality is because R is a field.

We are now ready for our main result.

Proposition 6.78. Fix a Noetherian ring R. The following are equivalent.

- R is a discrete valuation ring.
- R is a field or regular local ring of dimension 1.

Proof. We show the directions independently.

- In one direction, suppose R is a regular local ring of dimension 1 or a field. If R is a field, then R is a discrete valuation ring by Example 6.77.

  Otherwise, take R to be a regular local ring of dimension 1; as such, suppose (π) is maximal. Then most of the heavy lifting is done by Proposition 6.71, in which we defined a function $\nu\colon R\setminus\{0\}\to\mathbb{N}$ such that $\nu(r)$ is the unique nonnegative integer such that

  $$r/\pi^{\nu(r)}\in R^\times.$$

  Quickly, we check ν is additive: taking $r,s\in R$, we see that $r/\pi^{\nu(r)},s/\pi^{\nu(s)}\in R^\times$ so that

  $$\frac{rs}{\pi^{\nu(r)+\nu(s)}}\in R^\times$$

  so that uniqueness of ν forces $\nu(r+s)=\nu(r)-\nu(s)$. Now, to extend this to all of $K(R)^\times$, we simply define

  $$\nu(r/s)\coloneqq\nu(r)-\nu(s)$$

  for $r/s\in K(R)^\times$ (note $r,s\neq 0$). Observe that each $r\in R$ has $\nu(r/1)=\nu(r)-\nu(1)=\nu(r)$, so ν does indeed extend ν.

  Now, to see that ν is well-defined, note $\frac{r}{s}=\frac{r'}{s'}$ implies $rs'=r's$ because R is an integral domain, so

  $$\nu(r)-\nu(s)=\nu(r')-\nu(s').$$

  As such, we have a well-defined function $\nu\colon K(R)^\times\to\mathbb{Z}$. To check that this is a homomorphism, set $\frac{a}{b},\frac{c}{d}\in K(R)^\times$. Then, because we already showed that ν is additive on R, we see

  $$\nu\left(\frac{a}{b}\cdot\frac{c}{d}\right)=\nu\left(\frac{ac}{bd}\right)=\nu(ac)-\nu(bd)=\big(\nu(a)-\nu(b)\big)+\big(\nu(c)-\nu(d)\big)=\nu\left(\frac{a}{b}\right)+\nu\left(\frac{c}{d}\right).$$

  So we do have a homomorphism $\nu\colon K(R)^\times\to\mathbb{Z}$.

  Before continuing, observe that some $\frac{a}{b}\in K(R)^\times$ will have $a=u\pi^{\nu(a)}$ and $b=v\pi^{\nu(b)}$ for $u,v\in R^\times$, so

  $$\frac{a}{b}=\frac{u\pi^{\nu(a)}}{v\pi^{\nu(b)}}=uv^{-1}\pi^{\nu(a)-\nu(b)}=uv^{-1}\cdot\pi^{\nu(a/b)}\in R^\times.$$

  In particular, $\nu(a/b)$ is the correct power in $\mathbb{Z}$ to divide out from $\frac{a}{b}$ by to get into $R^\times$. As usual, this is unique: if $u\pi^m=v\pi^n$ for $u,v\in R^\times$ and $m\geq n$ (without loss of generality), then $\pi^{m-n}=u^{-1}v\in R^\times$, so $0\leq m-n<1$, so $m=n$.

  We now have the following remaining checks.

  – Given $\frac{a}{b},\frac{c}{d}\in K(R)^\times$, and suppose that $\nu(c/d)\geq\nu(a/b)$ without loss of generality. Then

    $$\frac{a/b}{\pi^{\nu(a/b)}}\in R\qquad\text{and}\qquad\frac{c/d}{\pi^{\nu(a/b)}}=\pi^{\nu(c/d)-\nu(a/b)}\cdot\frac{c/d}{\pi^{\nu(c/d)}}\in R,$$

    so it follows

    $$\frac{a/b+c/d}{\pi^{\nu(a/b)}}\in R,$$

    so $\nu(a/b+c/d)\geq\nu(a/b)$.

    $$\nu\left(\frac{a}{b}+\frac{c}{d}\right)=\nu\left(\frac{ad+bc}{bd}\right)=\nu(ad+bc)-\nu(bd).$$

  - Certainly $r \in R \setminus \{0\}$ has $\nu(r) \geq 0$ by definition of ν, so
$$R \subseteq \{x \in K(R)^\times : \nu(x) \geq 0\} \cup \{0\}.$$
Conversely, of course $0 \in R$, and any $\frac{r}{s} \in K(R)^\times$ with $\nu(r/s) = \nu(r) - \nu(s) \geq 0$ has $r = u\pi^{\nu(r)}$ and $s = v\pi^{\nu(s)}$ for some $u, v \in R^\times$. As such,
$$\frac{r}{s} = \frac{u\pi^{\nu(r)}}{v\pi^{\nu(s)}} = \frac{uv^{-1}\pi^{\nu(r)-\nu(s)}}{1} \in R,$$
so we also get
$$\{x \in K(R)^\times : \nu(x) \geq 0\} \cup \{0\} \subseteq R.$$

The above checks verify that R is in fact a discrete valuation ring with valuation ν.

- Suppose R is a discrete valuation ring, so pick up our valuation $\nu\colon K(R)^\times \to \mathbb{Z}$. If $\operatorname{im}\nu = \{0\}$, then
$$R = \{x \in K(R)^\times : \nu(x) \geq 0\} \cup \{0\} = K(R),$$
so R is a field.

Otherwise, suppose R is not a field and that $\operatorname{im}\nu \subseteq \mathbb{Z}$ has a nonzero element and hence a positive element by signing, so suppose d is the least such positive element. As such, find any
$$\pi \in \nu^{-1}(\{d\}).$$
We now proceed with the following steps.

  - We claim $R^\times = \nu^{-1}(\{0\})$. In one direction, if $r \in R^\times$, find $s \in R$ with $rs = 1$ so that certainly $r, s \neq 0$ and
$$\nu(r) + \nu(s) = \nu(rs) = \nu(1) = 0,$$
so $\nu(s) \geq 0$ (from $s \in R$) implies $\nu(r) \leq 0$. But still $\nu(r) \geq 0$, so we conclude $\nu(r) = 0$.
Conversely, if $x \in K(R)^\times$ has $\nu(x) = 0$, then $\nu\left(x^{-1}\right) = -\nu(x) = 0 \geq 0$ as well, so we see that both x and x^{-1} live in R, so $x \cdot x^{-1} = 1$ witnesses that x is a unit in R.
  - We claim that
$$(\pi) = \{0\} \cup \{x \in K(R)^\times : \nu(x) > 0\}.$$
Certainly any $\pi r \in (\pi)$ has $r = 0$ or $\nu(\pi r) = \nu(\pi) + \nu(r) \geq d + 0 > 0$. Conversely, if $x \in K(R)^\times$ has $\nu(x) > 0$, then of course $x \in R$. Also, $\nu(\pi) = d$ is as small as possible, so $\nu(x) \geq \nu(\pi)$, so $\nu(x/\pi) \geq 0$ gives $x/\pi \in R$ as well. Thus,
$$x = (x/\pi) \cdot \pi$$
witnesses $x \in (\pi)$.

The above two claims show that
$$\begin{aligned} R &= \{0\} \cup \{x \in K(R)^\times : \nu(x) \geq 0\} \\ &= \big(\{0\} \cup \{x \in K(R)^\times : \nu(x) > 0\}\big) \sqcup \{x \in K(R)^\times : \nu(x) = 0\} \\ &= (\pi) \sqcup R^\times, \end{aligned}$$
so R is local with unique maximal ideal (π). Further, note that $\dim R = \operatorname{codim}(\pi) \leq 1$ by Theorem 6.38, but $\dim R > 0$ because of the chain of primes $(0) \subsetneq (\pi)$. Thus, R is a regular local ring with dimension 1, regular because its maximal ideal is principal.

The above directions complete the proof. ■

As such, here is another example.

Example 6.79. The ring $\mathbb{Z}_p = \widehat{\mathbb{Z}}_{(p)}$ is a discrete valuation ring. Indeed, $\mathbb{Z}_p$ is local with maximal ideal $\widehat{(p)}$ by Corollary 5.27, and $\widehat{(p)} = p\mathbb{Z}_p$ by Proposition 5.33. Further, $\dim \mathbb{Z}_p = 1$ because $\dim \mathbb{Z}_p \geq 1$ because of the chain of primes $(0) \subsetneq p\mathbb{Z}_p$ while

$$\dim \mathbb{Z}_p = \operatorname{codim} p\mathbb{Z}_p \leq 1$$

by Theorem 6.38. Thus, $\mathbb{Z}_p$ is a regular local ring with dimension 1, so we finish by Proposition 6.78.

Remark 6.80. Tracking Proposition 6.78 through, we see that our valuation $\nu\colon \mathbb{Q}_p \to \mathbb{Z}$ takes $q \in \mathbb{Q}_p$ to the value n such that $q = u\pi^n$ with $u \in \mathbb{Z}_p^\times$. In fact, we can see that the function

$$d(a,b) := p^{-\nu(a-b)}$$

is exactly the metric defined in Lemma 5.20, so $\mathbb{Z}_p$ is a metric space defined by this valuation, actually complete by Proposition 5.24.

6.5.2 Normal Domains

Just for fun, let's provide a criterion to have a normal domain. To set up our discussion, recall that unique factorization domains are normal by Proposition 3.62. As such, we will imitate the following result.

Proposition 2.199. Fix R a Noetherian domain. Then R is a unique factorization domain if and only if every minimal prime ideal over a principal ideal is principal.

The idea is to weaken this condition to give us normality. In particular, recall that a prime $\mathfrak{p}$ is associated to the ideal I if and only if $\mathfrak{p} \in \operatorname{Ass} R/I$ if and only if there exists $x \in R$ such that

$$\mathfrak{p} = \operatorname{Ann}_R[x]_I = \{r : rx \in I\}.$$

Notably, we this would imply that $x \notin I$ and hence $[x]_I \neq [0]_I$.

Anyway, here is our statement.

Theorem 6.81. Fix a Noetherian domain R. Then R is normal if and only if either of the following conditions hold.

(a) For each prime $\mathfrak{p}$ associated to a principal ideal, the ideal $\mathfrak{p}R_\mathfrak{p} \subseteq R_\mathfrak{p}$ is a principal ideal.

(b) For each codimension-1 prime $\mathfrak{p}$, the localization $R_\mathfrak{p}$ is a discrete valuation ring. Further, each nonzero prime $\mathfrak{p}$ associated to a principal ideal has codimension 1.

Proof. We start by showing that each of the conditions (a) and (b) are equivalent.

- We show (a) implies (b). There are two sentences to check.
  - Given a codimension-1 prime $\mathfrak{p}$, Corollary 6.46 tells us that $\mathfrak{p}$ is minimal over some principal ideal (a). But $(a) = \operatorname{Ann} R/(a)$, so Proposition 2.166 shows that $\mathfrak{p}$ is associated to the R-module $R/(a)$, which means that $\mathfrak{p}$ is associated to the principal ideal (a).

    As such, by (a), we see that $\mathfrak{p}R_\mathfrak{p}$ is a principal ideal. This implies that $R_\mathfrak{p}$ is a regular local ring of dimension 1: note $R_\mathfrak{p}$ is local with maximal ideal $\mathfrak{p}R_\mathfrak{p}$, and we have $\dim R_\mathfrak{p} = \operatorname{codim} \mathfrak{p} = 1$ by construction of $\mathfrak{p}$. Thus, $\mathfrak{p}R_\mathfrak{p}$ being principal verifies that $R_\mathfrak{p}$ is regular. It follows $R_\mathfrak{p}$ is a discrete valuation ring by Proposition 6.78.

  - Pick up a nonzero prime $\mathfrak{p}$ associated to a principal ideal. By (a), we see $\mathfrak{p}R_\mathfrak{p} \subseteq R_\mathfrak{p}$ is a principal ideal and hence minimal over a principal ideal (namely, itself), so

$$\operatorname{codim} \mathfrak{p}R_\mathfrak{p} \leq 1$$

  by Theorem 6.38. But certainly $\mathfrak{p} \supsetneq (0)$ in R because $\mathfrak{p}$ is nonzero, and (0) is prime in the integral domain R, so $\operatorname{codim} \mathfrak{p} \geq 1$ by Lemma 6.17.
  Thus, Lemma 6.47 grants the inequalities

$$1 \leq \operatorname{codim} \mathfrak{p} = \dim R_\mathfrak{p} = \operatorname{codim} \mathfrak{p}R_\mathfrak{p} \leq 1$$

  because $R_\mathfrak{p}$ is local with maximal ideal $\mathfrak{p}R_\mathfrak{p}$. So indeed, $\operatorname{codim} \mathfrak{p} = 1$, which is what we wanted.

- We show (b) implies (a). Fix a prime $\mathfrak{p}$ associated to a principal ideal, and we check that $\mathfrak{p}R_\mathfrak{p}$ is principal. If $\mathfrak{p} = (0)$, then $\mathfrak{p}R_\mathfrak{p} = (0)$ is principal.
  Otherwise, $\mathfrak{p}$ is nonzero, so the second sentence of (b) tells us that $\mathfrak{p}$ has codimension 1, from which the first sentence tells us that $R_\mathfrak{p}$ is a discrete valuation ring. But then $R_\mathfrak{p}$ is a regular local ring of dimension 1 by Proposition 6.78, so the maximal ideal $\mathfrak{p}R_\mathfrak{p}$ must be principal, which is what we wanted.

We now show that (a) is equivalent to R being normal. We start with the backwards direction: suppose (a) holds, and we'll show R is normal. To start, we pick up the following lemma.

Lemma 6.82. Fix a Noetherian domain R. Given $x \in K(R)$, then $x \in R$ if and only if $x \in R_\mathfrak{p}$ for all primes $\mathfrak{p}$ associated to a principal ideal. In other words,

$$R = \bigcap_\mathfrak{p} R_\mathfrak{p},$$

where $\mathfrak{p}$ varies over primes associated to a principal ideal.

Proof. Of course, $x \in R$ implies that $x = x/1 \in R_\mathfrak{p}$ for each prime $\mathfrak{p}$ and therefore for each prime $\mathfrak{p}$ associated to a principal ideal.

Conversely, suppose $x \notin R$ has $x = \frac{a}{b}$. Then we are given $a \notin (b)$. Now, we showed a while ago that, in an R-module M, we have $m = 0$ if and only if $\frac{m}{1} = \frac{0}{1}$ in $R_\mathfrak{p}$ for all $\mathfrak{p} \in \operatorname{Ass} M$. As such, working with $M := R/(x)$, we see that $[a]_{(x)} \neq [0]_{(x)}$, so there exists a prime $\mathfrak{p}$ associated to $R/(b)$ (i.e., associated to the ideal (b)) with $a \notin (b)_\mathfrak{p}$, so $x \notin R_\mathfrak{p}$. ■

Thus, the hypothesis tells us that each $R_\mathfrak{p}$ is a discrete valuation ring and hence a principal ideal domain and hence a unique factorization domain and hence normal.[3] Thus, because the intersection of normal domains is normal, we deduce that R is normal.

We now show the forwards direction. Suppose that R is normal, and let $\mathfrak{p}$ be some prime associated to a principal ideal (a). We would like to show that $\mathfrak{p}R_\mathfrak{p}$ is principal; because $\mathfrak{p}R_\mathfrak{p}$ is still associated to $(a)R_\mathfrak{p}$, we see that we may replace R and $\mathfrak{p}$ with $R_\mathfrak{p}$ and $\mathfrak{p}R_\mathfrak{p}$ so that R is local with maximal ideal $\mathfrak{p}$.

To continue, we pick up the following definition.

Definition 6.83. A *fractional ideal* is an R-submodule of $K(R)$.

As such, we set

$$\mathfrak{p}^{-1} := \{x \in K(R) : x\mathfrak{p} \subseteq R\}.$$

Our goal is to show that $\mathfrak{p}\mathfrak{p}^{-1} = R$. Certainly $\mathfrak{p}^{-1}\mathfrak{p} \subseteq R$ by definition, and we can see that $\mathfrak{p}^{-1} \supseteq R$ implies $\mathfrak{p}\mathfrak{p}^{-1} \subseteq R$. Now, $\mathfrak{p}\mathfrak{p}^{-1}$ can be checked to be an R-ideal, so because $\mathfrak{p}$ is currently maximal, $\mathfrak{p}\mathfrak{p}^{-1} \in \{\mathfrak{p}, R\}$.

[3] One can show this somewhat more directly by building a monic polynomial with some $u\pi^m$ as a root and then arguing about the maximal ideal, but we won't bother.

Now, suppose for the sake of contradiction that $\mathfrak{p}^{-1}\mathfrak{p} = \mathfrak{p}$. Well, any $x \in \mathfrak{p}^{-1}$ is integral by the Cayley–Hamilton theorem, so $x \in R$, so we have shown $\mathfrak{p}^{-1} \subseteq R$. But this does not make sense: $\mathfrak{p}$ is associated to (a) by some element $[b]_{(a)}$, but then $b\mathfrak{p} \subseteq (a)$, so $a^{-1}b\mathfrak{p} \subseteq R$, so $a^{-1}b \in R \setminus \mathfrak{p}$.

But now $\mathfrak{p}^{-1}\mathfrak{p} = R$ shows that there exists $\frac{a}{b}$ such that $\frac{x}{y}\mathfrak{p} = R$ for some unit x, so $\frac{1}{y}\mathfrak{p} = R$, so $\mathfrak{p} = (y)$. This finishes the proof. ■

Remark 6.84. It is possible for $\mathfrak{p}$ in the proof to not be principal but still have $\mathfrak{p}R_\mathfrak{o}$ be principal.

As a corollary of the proof, we get the following results.

Corollary 6.85. Fix a Noetherian domain R. If R is normal, then

$$R = \bigcap_{\mathfrak{p}} R_\mathfrak{p},$$

where the intersection is over all primes $\mathfrak{p}$ of codimension 1.

Corollary 6.86. Fix X an affine algebraic variety such that $A(X)$ is a normal domain. If we have a subvariety $Y \subseteq X$ is such that $A(Y)$ is of codimension at least 2, then $A(X - Y) = A(X)$.

Proof. Suppose that $\mathfrak{q}$ is the prime ideal corresponding to the variety Y. Then $A(X - Y) = A(X)_\mathfrak{q}$, so taking the intersection finishes. ■

6.5.3 Invertible Modules

For the following discussion, we will take R to be a Noetherian domain, for intuition. We have the following definition.

Definition 6.87 (Invertible module)**.** An R-module M is *invertible* if and only if all prime ideals $\mathfrak{p} \subseteq R$ has $M_\mathfrak{p} \cong R_\mathfrak{p}$.

It turns out that these are all fractional ideals in the case where R is a Noetherian domain. Before that, here are some examples.

Example 6.88. A principal ideal $(f) \subseteq R$ is invertible.

Example 6.89. If M and N are invertible R-modules, then any prime $\mathfrak{p}$ will have

$$(M \otimes_R N)_\mathfrak{p} \cong M_\mathfrak{p} \otimes_{R_\mathfrak{p}} N_\mathfrak{p} \cong R_\mathfrak{p} \otimes_{R_\mathfrak{p}} R_\mathfrak{p} \cong R_\mathfrak{p},$$

so $M \otimes_R N$ is also invertible.

Example 6.90. If M is an invertible, finitely generated R-module, then $M^* := \operatorname{Hom}_R(M, R)$ is also invertible. In particular, because R is Noetherian, M is finitely presented, so

$$R_\mathfrak{p} \cong \operatorname{Hom}_{R_\mathfrak{p}}(R_\mathfrak{p}, R_\mathfrak{p}) \cong \operatorname{Hom}_{R_\mathfrak{p}}(M_\mathfrak{p}, R_\mathfrak{p}) \cong \operatorname{Hom}_R(M, R)_\mathfrak{p}.$$

To start our discussion, here is a lemma.

Lemma 6.91. Fix a Noetherian domain R. An R-module M is invertible if and only if the map

$$\mu : M^* \otimes_R M \to R$$

by $\varphi \otimes m \mapsto \varphi(m)$ is an isomorphism.

Proof. It suffices to work with the case that $\mu_\mathfrak{p}$ is an isomorphism for all primes $\mathfrak{p}$. By running through the isomorphisms in the examples, we see that we are asking for

$$\mu_\mathfrak{p} : (M_\mathfrak{p})^* \otimes_{R_\mathfrak{p}} M_\mathfrak{p} \to R_\mathfrak{p}$$

is an isomorphism for all primes $\mathfrak{p}$.

In particular, we are allowed to assume that R is local with maximal ideal $\mathfrak{p}$. In one direction, suppose that μ is an isomorphism. By surjectivity, we are promised some

$$\mu\left(\sum_{i=1}^n \varphi_i \otimes a_i\right) = 1.$$

In particular, there exists i such that $\varphi_i(a_i) \notin \mathfrak{p}$, but $R \setminus \mathfrak{p}$ are all units, so we can force $\varphi(a) = 1$ for some φ and a. Now, living in a local ring thus forces by φ to show that

$$M \cong R \oplus \ker \varphi,$$

but $\ker \varphi$ is trivial because any kernel would have to show up in the kernel of μ, which is trivial by hypothesis.

We don't discuss the other direction. ■

Remark 6.92. We can see that M will be generated by the elements a_i in the summation

$$\mu\left(\sum_{i=1}^n \varphi_i \otimes a_i\right) = 1.$$

Thus, M should be finitely generated.

This discussion gives us the following definition.

Definition 6.93 (Picard group)**.** Fix a Noetherian domain R. Then $\operatorname{Pic} R$ is the group of isomorphism classes of invertible R-modules.

Remark 6.94. The Picard group loosely corresponds to line bundles.

To be explicit, the group operation of $\operatorname{Pic} R$ is by

$$[X] \cdot [Y] \coloneqq [X \otimes_R Y],$$

our identity element is $[R]$, and the inverses are $[X]^{-1} \coloneqq [X^*]$.

6.5.4 The Class Group

To close out class, we discuss the connection to fractional ideals.

Lemma 6.95. Fix a Noetherian domain R. Then M is invertible if and only if M is isomorphic to some nonzero fractional ideal.

Proof. The idea is to embed M into $K(R)$ to extract our fractional ideal. Well, the embedding $R \to K(R)$ gives us an embedding

$$M \to K(R) \otimes_R M.$$

But now, $K(R) \otimes_R M \cong K(R)$ because $K(R) \otimes_R M$ is an invertible module over $K(R)$, which must be isomorphic to $K(R)$ because $K(R)$ only has the localization at the prime (0) (which does nothing).

As such, we have placed M as an R-submodule of $K(R)$ and hence is isomorphic to a nonzero fractional ideal. ■

As such, we can give an alternate characterization of the Picard group.

Lemma 6.96. Fix a Noetherian domain R. If I and J are fractional ideals, then

$$IJ \cong I \otimes_R J \qquad \text{and} \qquad I^{-1}J \cong \operatorname{Hom}(I.J).$$

Proof. The isomorphism $I \otimes_R J \cong IJ$ is by $a \otimes b \mapsto ab$. That $I^{-1}J \cong \operatorname{Hom}_R(I, J)$ follows from carefully considering the localizations. ■

Thus, modding out by principal ideals from the fractional ideals gives us the Picard group back again.

6.6 April 7

We continue.

6.6.1 Fractional Ideals

We continue discussing fractional ideals. Last time we showed the following results.

Lemma 6.97. Fix a Noetherian domain R. Then M is invertible if and only if M is isomorphic to some nonzero fractional ideal.

We were also in the middle of the following proof, which we will finish today.

Lemma 6.98. Fix a Noetherian domain R. If I and J are nonzero fractional ideals, then

$$IJ \cong I \otimes_R J \qquad \text{and} \qquad I^{-1}J \cong \operatorname{Hom}(I.J).$$

Proof. The map

$$I \otimes_R J \to IJ$$

is by $a \otimes b \mapsto ab$. This is of course surjective, so we just need injectivity. It suffices to show injectivity upon localizing by any prime $\mathfrak{p}$. But now we are looking at the map

$$I_\mathfrak{p} \otimes_{R_\mathfrak{p}} J_\mathfrak{p} \to (IJ)_\mathfrak{p},$$

which is injective because $I_\mathfrak{p}$ and $J_\mathfrak{p}$ are both free $R_\mathfrak{p}$-modules (by definition), so we get the injection here automatically because $R_\mathfrak{p}$ is an integral domain.

The map

$$I^{-1}J \to \operatorname{Hom}_R(I, J)$$

is by sending t to $\mu_t : x \mapsto tx$. This map is injective because $\mu_{t_1} = \mu_{t_2}$ implies they are equal on $a \in I$ (say), so $t_1 = t_2$ because R is an integral domain. In fact, we can even say that μ_t is injective for each nonzero t.

It remains to show surjectivity. Well, pick up some R-module homomorphism $\varphi : I \to J$. Now, for some $f \in I \setminus \{0\}$, suppose $\varphi(f) = g$ so that we may consider

$$\mu_{g/f}(f) = g,$$

and we can check that $\mu_{g/f} = \varphi$ everywhere by some computation. ■

Here is another helpful result.

Lemma 6.99. Fix a Noetherian domain R. Then $I \subseteq K(R)$ is an invertible fractional ideal if and only if $I^{-1}I = R$.

Proof. On one hand, we see that I being invertible implies that $I^{-1}I \cong \operatorname{Hom}_R(I, I) \cong R$. On the other hand, suppose $I^{-1}I = R$. Localizing gives us

$$I_\mathfrak{p} I_\mathfrak{p}^{-1} = R_\mathfrak{p}.$$

But then $vI_\mathfrak{p} \not\subseteq \mathfrak{p}R_\mathfrak{p}$ for some $v \in I^{-1}$, so we can conclude $vI_\mathfrak{p} = R_\mathfrak{p}$, so I is indeed locally free. ■

As such, we are able to build the following group.

Definition 6.100 (Cartier divisors)**.** Fix a Noetherian domain R. Then a *Cartier divisor* is an invertible fractional ideal.

From the above results, the Cartier divisors are an abelian group with respect to multiplication, which we all $C(R)$.

Now, we note that we have a homomorphism

$$C(R) \to \operatorname{Pic} R$$

by $I \mapsto [I]$. Notably, Lemma 6.97 tells us that this homomorphism is surjective, and its kernel consists of ideals I such that $[I] = [R]$, which means $I \cong R$ (as R-modules), which means I is principal, generated by some element of $K(R)$. Thus, we have the exact sequence

$$K(R)^\times \to C(R) \to \operatorname{Pic} R \to 0.$$

We would like to make this have 0s on the end, so we note that $a \in K(R)^\times$ will have $(a) = R$ if and only if $a \in R^\times$, so we get to write

$$0 \to R^\times \to K(R)^\times \to C(R) \to \operatorname{Pic} R \to 0.$$

As such, we have a way to measure $\operatorname{Pic} R$ by objects only internal to $K(R)$.

To make this behave a little better, we pick up the following lemma.

Lemma 6.101. The group $C(R)$ is generated by invertible ideals $I \subseteq R$.

Proof. The point is to multiply an arbitrary invertible ideal from $K(R)$ to R. Indeed, any invertible fractional ideal $I \in C(R)$ will at least live in $K(R)$. Picking up any nonzero $a \in I \times R$, we note that

$$I = \left(a^{-1}\right) \cdot (aI),$$

and $aI \subseteq R$ by construction of a. So we are indeed able to generate $C(R)$ as an R-module by these invertible ideals. ■

Let's see some examples.

Example 6.102. Fix a principal ideal domain R. Then every ideal is principal and hence isomorphic to R, so $\operatorname{Pic} R = 0$. Namely, $C(R)$ only consists of principal ideals.

Exercise 6.103. We discuss $\operatorname{Pic} \mathbb{Z}[\sqrt{-5}]$.

Proof. Fix the Noetherian domain $R = \mathbb{Z}[\sqrt{-5}]$. This is normal because it is the integral closure of $\mathbb{Z}$ in $\mathbb{Q}(\sqrt{-5})$, as we showed on the homework. This is dimension 1 because R is integral over $\mathbb{Z}$, and $\dim \mathbb{Z} = 1$. However, R is not a principal ideal domain because it is not factorial, as

$$\left(1+\sqrt{-5}\right)\left(1-\sqrt{-5}\right) = 2 \cdot 3$$

shows. In particular, the ideal $\mathfrak{p} := \left(2, 1+\sqrt{-5}\right)$ is not principal. In fact, $\mathbb{Z}/\mathfrak{p} = \mathbb{Z}/2\mathbb{Z}$ is a field,[4] so $\mathfrak{p}$ is maximal.

We will take on faith that $\mathfrak{p}$ is not principal because just look at it. To show that $\mathfrak{p}$ is invertible, we note that localizing at any prime which is not $\mathfrak{p}$ will automatically trivialize, so we have left to study

$$\mathfrak{p}R_\mathfrak{p} \subseteq R_\mathfrak{p}.$$

But in $R_\mathfrak{p}$, we see that

$$2 = \frac{1}{3} \cdot \left(1-\sqrt{-5}\right)\left(1+\sqrt{-5}\right),$$

so

$$\mathfrak{p}R_\mathfrak{p} = \left(1+\sqrt{-5}\right),$$

which is indeed principal.

Thus, we have a nontrivial element of $\operatorname{Pic} \mathbb{Z}[\sqrt{-5}]$. We can also compute

$$\mathfrak{p}^2 = \left(2, 1+\sqrt{-5}\right)^2 = \left(4, 2+2\sqrt{-5}, -4+2\sqrt{-5}\right) = \left(4, 2+2\sqrt{-5}, -6\right) = \left(2, 2+2\sqrt{-5}, -6\right) = (2),$$

so this is indeed principal. So $\mathfrak{p}$ is of order 2 in $\operatorname{Pic} \mathbb{Z}[\sqrt{-5}]$. In fact, this is an isomorphism, which one can see by taking Math 254A. ■

Example 6.104. Fix $R := k[x,y]/\left(y^2 - x^3\right) \cong k\left[t^2, t^3\right]$ so that $k[t]$ is the normalization of R. Now, any ideal of $k[t]$ is principal, so $\operatorname{Pic} k[t] = 0$. However, for any invertible ideal I of $k[t]$, then $I \cap k\left[t^2, t^3\right]$ will remain invertible by tracking through the definition. For example, if we take $1 + at$ as a varies over k, we have a map

$$k \to \operatorname{Pic} R$$

by $a \mapsto (1 + at)$, which turns out to be an isomorphism. For more, see exercises 11.15 and 11.16.

Remark 6.105. It is not technically necessary for R to be a domain in the above results, but the proofs are more annoying. Namely, instead of using the fraction field $K(R)$, one should use the total quotient $K(R)$.

6.6.2 Divisors

We now talk about divisors a little more generally. We pick up the following definition.

Definition 6.106 (Pure codimension)**.** Fix a Noetherian domain R. Then $I \subseteq R$ has *pure codimension* 1 if and only if every prime associated to I has codimension 1.

[4] Track through the map $\mathbb{Z} \to \mathbb{Z}[\sqrt{-5}]/\mathfrak{p}$, and we can note that it is surjective and has kernel (2).

Theorem 6.107. Fix a Noetherian domain R such that $R_{\mathfrak{m}}$ is factorial for each maximal ideal $\mathfrak{m}$. Then the following are true.

(a) An ideal $I \subseteq R$ is invertible if and only I has pure codimension 1.

(b) An invertible fractional ideal I can be written uniquely as

$$I = \mathfrak{p}_1^{m_1} \cdots \mathfrak{p}_n^{m_n},$$

for distinct prime ideals $\mathfrak{p}_1, \ldots, \mathfrak{p}_n$ of codimension 1.

We will prove this momentarily, but let's talk about some consequences.

Corollary 6.108. Fix a Noetherian domain R. Then $C(R)$ is a free abelian group generated by prime ideals $\mathfrak{p}$ of codimension 1.

Proof. This follows directly from part (b) of the theorem. ■

Here is the case that number theorists care about.

Definition 6.109 (Dedekind)**.** A *Dedekind domain* is a Noetherian normal domain of dimension 1.

Notably, in a Dedekind domain, all primes of codimension 1 are maximal, which are all now invertible by (a) of the theorem. In particular, $R_{\mathfrak{m}}$ is indeed factorial for all maximal ideals $\mathfrak{m}$ because we showed last class that a Noetherian domain being normal is equivalent to all the primes $\mathfrak{p}$ associated to a principal ideal has $\mathfrak{p}R_{\mathfrak{p}} \subseteq R_{\mathfrak{p}}$ principal, which makes $R_{\mathfrak{p}}$ a discrete valuation ring and in particular factorial.

We now prove our theorem.

Proof of Theorem 6.107. We go one at a time.

(a) Fix I an invertible fractional ideal. Then $R_{\mathfrak{m}}$ is factorial, so we showed a while ago that this implies $\mathfrak{m}R_{\mathfrak{m}}$ (which is a codimension-1 prime) must be principal, so we are done.

We now show the other direction. Well, if $\mathfrak{p}$ is a prime of codimension 1, then place $\mathfrak{p}$ in some maximal ideal $\mathfrak{m}$, and we see that $\mathfrak{p}_{\mathfrak{m}}$ is principal and hence codimension 1 in the factorial ring $R_{\mathfrak{m}}$. This finishes this direction.

(b) Fix an invertible fractional ideal I. Then we know that any prime $\mathfrak{p}$ associated to I has codimension 1, by part (a). To start, we show that I is a finite product of primes. Well, otherwise we could find an ideal I of R maximal with respect to not being a product of primes, and place I in a maximal ideal $\mathfrak{m}$. Of course, $I \subsetneq \mathfrak{m}$ because $\mathfrak{m}$ is its own factorization, so we look at

$$\mathfrak{m}^{-1} I \subsetneq R.$$

Notably, $\mathfrak{m}^{-1} I \supsetneq I$ would imply that $\mathfrak{m}^{-1} I$ would have a factorization into primes, giving I a factorization into primes.

So we have left to show $I \subsetneq \mathfrak{m}^{-1} I$ require using that R is normal. In particular, $\mathfrak{m}^{-1} I = I$ would imply, by the Cayley–Hamilton theorem, we have that every element $x \in \mathfrak{m}^{-1}$ is integral over R and hence is in R, so $\mathfrak{m}^{-1} = R$, which does not make sense.

Lastly, we show uniqueness. Well, if

$$\prod_{k=1}^{m} \mathfrak{p}_k = \prod_{\ell=1}^{n} \mathfrak{q}_\ell,$$

we pick up some $\mathfrak{q}_n$, and by the product, we can say that some $\mathfrak{p}_k$ contains $\mathfrak{q}_1$. But $\mathfrak{p}_k$ has codimension 1, so $\mathfrak{p}_k = \mathfrak{q}_1$, so we can cancel from both sides and then induct downwards. ■

With the above in mind, we see that we are justified in only caring about the primes of codimension 1. This gives us the following definition.

Definition 6.110 (Divisor)**.** Fix a Noetherian domain R. Then the group of *divisors* $\operatorname{Div} R$ is the free abelian group generated by all primes of codimension 1 (as letters).

Notably, there is a good homomorphism

$$\varphi : C(R) \to \operatorname{Div} R,$$

though they are not the same. To see this, take an invertible ideal $I \in C(R)$ and then set

$$\varphi(I) := \sum_{\mathfrak{p}} \ell(R_\mathfrak{p}/I_\mathfrak{p})[\mathfrak{p}].$$

Notably, the length $\ell(R_\mathfrak{p}/I_\mathfrak{p})$ is finite because $\dim R_\mathfrak{p}/I_\mathfrak{p} = 0$ (making $R_\mathfrak{p}/I_\mathfrak{p}$ Artinian) by the principal ideal theorem: we get $\dim R_\mathfrak{p} = 1$ and $\dim I_\mathfrak{p} = 1$, so we bound $\dim R_\mathfrak{p}/I_\mathfrak{p}$ down to 0. It requires some work to show that φ is a homomorphism. Namely, we have to show that

$$\ell(R_\mathfrak{p}/(IJ)_\mathfrak{p}) \stackrel{?}{=} \ell(R_\mathfrak{p}/I_\mathfrak{p}) + \ell(R_\mathfrak{p}/I_\mathfrak{p}).$$

We are able to force $I_\mathfrak{p}$ and $J_\mathfrak{p}$ to be principal by using our theory of modules of finite length, so by replacing R with $R_\mathfrak{p}$, we are showing

$$\ell(R/(IJ)) \stackrel{?}{=} \ell(R/I) + \ell(R/J),$$

where $I = (a)$ and $J = (b)$. But then we can build the filtration for $R/(IJ)$ by hand by zippering the filtrations for R/I and R/J together.

Remark 6.111. The homomorphism φ is in general not injective, but it will be injective when R is also normal. The main idea is that, if R is normal, then $R_\mathfrak{p}$ will be factorial and in particular a discrete valuation ring, so $\ell(R_\mathfrak{p}/I_\mathfrak{p})$ vanishing everywhere forces I to vanish.

THEME 7
HIGHER DIMENSIONS

To deal with a 14-dimensional space, visualize a 3-D space and say 'fourteen' to yourself very loudly. Everyone does it.

—Geoffrey Hinton

7.1 April 12

We continue.

7.1.1 The Hilbert Function

Today we are discussing the Hilbert–Samuel function and its relation to dimension. Here is the main result for today.

Definition 7.1 (Hilbert function)**.** Fix a local Noetherian ring R with unique maximal ideal $\mathfrak{m}$. Let $\kappa := R/\mathfrak{m}$ be the residue class field. Then the function

$$H_R(n) := \dim_\kappa \mathfrak{m}^n/\mathfrak{m}^{n+1}$$

is called the *Hilbert function* of R.

Theorem 7.2. Fix a local Noetherian ring R with unique maximal ideal $\mathfrak{m}$. Let $\kappa := R/\mathfrak{m}$ be the residue class field. Then the Hilbert function of R agrees with a polynomial $P_R(n)$ for sufficiently large n, and $\dim R = 1 + \deg P_R$.

As such, we have the following definition.

Definition 7.3 (Hilbert polynomial)**.** Fix a local Noetherian ring R. Then the polynomial P_R which agrees with the Hilbert function H_R is called the *Hilbert polynomial*.

Remark 7.4. If R is not local, then we could get different dimensions out of $H_R(n)$ by various localizations, but we want to talk about $\dim R$ "globally." As such, we need the ring to be local.

Example 7.5. Fix $R := k[x_1, \ldots, x_r]_{(x_1,\ldots,x_r)}$ which has maximal ideal $\mathfrak{m} := (x_1, \ldots, x_r)$. Then

$$H_R(n) = \dim_k \mathfrak{m}^n/\mathfrak{m}^{n+1}$$

Another way to view this computation is by noting $\operatorname{gr}_{\mathfrak{m}} R \cong k[x_1, \ldots, x_r]$. As such, we are counting the number of monomials of degree n in r variables, which is

$$P_R(n) := \binom{n+r-1}{r-1}$$

by a counting argument: from $n+r-1$ slots, choose $r-1$ dividers, which uniquely determines a tuple of nonnegative integers which sum to n. As such, we see that $\deg P_R(n) = r-1 = \dim R - 1$, which is what we wanted.

Example 7.6. If $\dim R = 0$, then R is Artinian, so the filtration

$$\mathfrak{m} \supseteq \mathfrak{m}^2 \supseteq \mathfrak{m}^3 \supseteq \cdots$$

must stabilize, so $\mathfrak{m}^{n+1} = \mathfrak{m}^n$ for sufficiently large n. As such, we see that $H_R(n) = 0$ for sufficiently large n, so $P_R \equiv 0$. As such, we set by convention $\deg P_R = \deg 0 = -1$ to agree with $\dim R = 0$.

7.1.2 The Hilbert–Samuel Function

To prove Theorem 7.2, we work in higher generality. First, we will replace R with a finitely generated module; second, we will replace $\mathfrak{m}$ by a more arbitrary ideal. To start, recall the following definitions.

Definition 7.7 (Krull dimension, modules)**.** Fix a finitely generated module M over a Noetherian ring R. Then we define the *dimension*

$$\dim M := \dim R/\operatorname{Ann} M.$$

Definition 7.8 (Finite colength)**.** Fix a finitely generated module M over a Noetherian ring R. Then an ideal $\mathfrak{q} \subseteq R$ is of *finite colength* if and only if $\ell(M/\mathfrak{q}M) < \infty$.

For example, if M is a faithful module (i.e., with trivial annihilator), then there exists d such that

$$\mathfrak{m}^d \subseteq \mathfrak{q} \subseteq \mathfrak{m},$$

where $\mathfrak{q}$ can be generated by $\dim M$ total elements, by the Principal ideal theorem. More generally, if we first mod out R by $\operatorname{Ann} M$, we can say that

$$\mathfrak{m}^d \subseteq \mathfrak{q} + \operatorname{Ann} M \subseteq \mathfrak{m}.$$

As such, we take the following definition.

Definition 7.9 (Hibert–Samuel function)**.** Fix a local Noetherian ring R with finitely generated R-module M and some prime of finite colength $\mathfrak{q}$. Then we define the *Hilbert–Samuel function* by

$$H_{\mathfrak{q},M}(n) := \ell\left(\mathfrak{q}^n M/\mathfrak{q}^{n+1}\right).$$

We start by checking that this is well-defined.

Lemma 7.10. The value $\ell\left(\mathfrak{q}^n M/\mathfrak{q}^{n+1} M\right)$ is finite.

Proof. Without loss of generality, we know immediately that M is faithful (by first modding out by $\operatorname{Ann} M$). We start by noting that $M/\mathfrak{q}M$ has finite length by hypothesis on $\mathfrak{q}$. Now, $R/\mathfrak{q}$ embeds into $\operatorname{End}_R(M/\mathfrak{q}M)$, the latter of which is finite length because $M/\mathfrak{q}M$ is of finite length, so we conclude that $R/\mathfrak{q}$ is of finite length and in particular Artinian. It follows that $\mathfrak{q}^nM/\mathfrak{q}^{n+1}M$, which is finitely generated over $R/\mathfrak{q}$, must also be Artinian and in particular of finite length because everything involved is Noetherian. ■

The point is that, provided that our module is faithful, we see that we get to replace $\mathfrak{m}$ with any ideal containing some power of $\mathfrak{m}$.

Remark 7.11. We can replace R with $\operatorname{gr}_{\mathfrak{q}} R$ and M with $\operatorname{gr}_{\mathfrak{q}} M$.

7.1.3 Finite Differences

We now have a short digression into finite differences.

Definition 7.12 (Discrete derivative)**.** Given a function $f : \mathbb{N} \to \mathbb{C}$, we define the *discrete derivative*

$$\delta(f) := f(n+1) - f(n).$$

We have the following result.

Lemma 7.13. Suppose that we have some $f : \mathbb{N} \to \mathbb{C}$ such that $\delta(f)$ is a polynomial of degree d, for sufficiently large n. Then f is a polynomial of degree $d+1$, for sufficiently large n.

Proof. By shifting, we may assume that $\delta(f)$ is a polynomial of degree d. Now, note that the functions

$$\binom{n}{k}$$

form a basis of the set of polynomials $\mathbb{N} \to \mathbb{C}$. In fact,

$$\delta\left(\binom{n}{k}\right) = \binom{n+1}{k} - \binom{n}{k} = \binom{n}{k-1},$$

so δ is very well-behaved here. As such, writing

$$\delta(f)(n) = \sum_{k=0}^{d} a_k \binom{n}{k},$$

we can use our evaluation of δ on the binomials to read back the coefficients of f. ■

7.1.4 The Hilbert–Samuel Polynomial

And so ends our intermission. Here is a proposition.

Proposition 7.14. Fix a finitely generated module M over a local Noetherian ring R. Given an ideal $\mathfrak{q} = (x_1, \ldots, x_r)$ of finite colength on M, we have the following.

(a) The function $H_{\mathfrak{q},M}(n)$ agrees with a polynomial $P_{\mathfrak{q},M}$ for sufficiently large n.

(b) $\deg P_{\mathfrak{q},M} \le r$.

Proof. We induct on r. The point is that we can apply an inductive hypothesis to M/x_1M so that $\mathfrak{q}' := (x_2, \ldots, x_r)$ has finite colength on M/x_1M. As such, we have the following exact sequence.

$$0 \to \ker x_1 \to M \xrightarrow{x_1} M(1) \to (\operatorname{coker} x_1)(1) \to 0.$$

Notably, we are using $M(1)$ (which is the twist of M by $M(1)_n := M_{n+1}$) by reducing to the graded case where $\operatorname{gr}_\mathfrak{q} M \mapsto M$ and $\operatorname{gr}_\mathfrak{q} R \mapsto R$. Taking the length everywhere in the nth component, we find that

$$H_{\mathfrak{q},\ker x_1}(n) - H_{\mathfrak{q},M}(n) + H_{\mathfrak{q},M(1)}(n) - H_{\mathfrak{q},\operatorname{coker} x_1(1)}(n) = 0.$$

Applying the shifting, we see that

$$\delta(H_{\mathfrak{q},M})(n) = H_{\mathfrak{q},M}(n+1) - H_{\mathfrak{q},M}(n) = H_{\mathfrak{q},\operatorname{coker} x_1}(n+1) - H_{\mathfrak{q},\ker x_1}(n).$$

Now, both $\operatorname{coker} x_1 = M/x_1M$ and $H_{\mathfrak{q},\ker x_1}$ will have degree at most $r-1$ by the inductive hypothesis, so we are done by Lemma 7.13. ■

To prove Theorem 7.2, we will need to be a little more careful in the above argument. We start by keeping track of the degree in short exact sequences.

Lemma 7.15. Fix a local Noetherian ring R. Given a short exact sequence of finitely generated modules

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

Then

$$P_{\mathfrak{q},B}(n) = P_{\mathfrak{q},A}(n) + P_{\mathfrak{q},C}(n) - F,$$

where F is some polynomial of degree strictly less than $\deg P_{\mathfrak{q},A}(n)$. In fact, the coefficients of F are all positive.

Remark 7.16. The main idea here is to generalize the fact that we get an exact equality when we are looking at just lengths.

Proof. We construct an auxiliary function

$$L_{\mathfrak{q},M}(n) := \ell\left(M/\mathfrak{q}^n M\right) = \sum_{i=0}^{n-1} H_{\mathfrak{q},M}(i)$$

to more easily keep track of the length in our filtration. In particular, $\delta(L_{\mathfrak{q},M}) = H_{\mathfrak{q},M}$, so $\deg L_{\mathfrak{q},M} = 1 + \deg H_{\mathfrak{q},M}$, assuming things are nonzero. Now, we would like to quotient our short exact sequence by $\mathfrak{q}^n B$, but we cannot do that because that doesn't preserve exactness. So we instead write

$$0 \to (A \cap \mathfrak{q}^n B)/\mathfrak{q}^n A \to A/\mathfrak{q}^n A \to B/\mathfrak{q}^n B \to C/\mathfrak{q}^n C \to 0.$$

As such, we see that

$$L_{\mathfrak{q},B}(n) = L_{\mathfrak{q},A}(n) + L_{\mathfrak{q},C}(n) - \ell\left(\frac{A \cap \mathfrak{q}^n M}{\mathfrak{q}^n A}\right).$$

We would like to understand the object $\frac{A\cap\mathfrak{q}^n M}{\mathfrak{q}^n A}$, for which we use the Artin–Rees lemma. Recall the statement.

Theorem 7.17. Fix R a Noetherian ring and $I \subseteq R$ an ideal with M a finitely generated R-module granted a stable I-filtration $\mathcal{J}$ denoted by

$$M = M_0 \supseteq M_1 \supseteq M_2 \supseteq \cdots.$$

Then given a submodule $M' \subseteq M$, the induced filtration by $M'_k := M_k \cap M'$ is also a stable I-filtration.

In particular, we see that the $\mathfrak{q}$-filtration on B induces a $\mathfrak{q}$-stable filtration on A. In other words, there is an m so that $n \geq m$ will have

$$A \cap \mathfrak{q}^n B = \mathfrak{q}^{n-m}\left(A \cap \mathfrak{q}^n B\right) = \mathfrak{q}^{n-m} A,$$

so the length

$$\ell\left(\frac{A \cap \mathfrak{q}^n M}{\mathfrak{q}^n A}\right) \leq L_{\mathfrak{q},A}(n) - L_{\mathfrak{q},A}(n-m),$$

which agrees with a polynomial of smaller degree, so we are done because F is a polynomial for free as it is the difference of polynomials. ■

And here is our theorem.

Theorem 7.18. Fix a local Noetherian ring R with unique maximal ideal $\mathfrak{m}$. Further, take a finitely generated module M and an ideal $\mathfrak{q}$ of finite colength on M. Then

$$\dim M = 1 + \deg P_{\mathfrak{q},M}.$$

Proof. The proof, like the original Star Wars, comes in three parts.

1. We show that $\deg P_{\mathfrak{q},M}$ does not depend on $\mathfrak{q}$. Being finite colength means that we can write

   $$\mathfrak{m}^d \subseteq \mathfrak{q} + \operatorname{Ann} M \subseteq \mathfrak{m}$$

   for each d. This implies that

   $$H\mathfrak{m}, M(n) \leq H_{\mathfrak{q},M}(n) \leq H\mathfrak{m}, M(dn),$$

   but the Hilbert polynomials on the left and right have the same degree.

2. We show $1 + \deg P_{\mathfrak{q},M} \leq \dim M$. By modding out by $\operatorname{Ann} M$ everywhere, we may assume that M is faithful, meaning $\dim M = \dim R$. For brevity, set $\dim M := r$ so that we can choose $\mathfrak{q}$ so that

   $$\mathfrak{m}^d \subseteq \mathfrak{q} \subseteq \mathfrak{m}$$

   to have r generators, by the Principal ideal theorem. So we are done by Proposition 7.14.

3. We show $1 + \deg P_{\mathfrak{q},M} \geq \dim M$. Again, modding out by $\operatorname{Ann} M$ everywhere lets us assume that M is faithful, giving $\dim M = \dim R$.

   Now, choose $\mathfrak{p}$ to be a prime associated to M so that $\dim M = \dim R/\mathfrak{p}$. In practice, this means that $\mathfrak{p}$ is minimal over (0) to minimize $\dim R/\mathfrak{p}$. Now, if M has dimension zero, then we are done by Example 7.6. Otherwise, $\mathfrak{q} \supsetneq \mathfrak{p}$, so we may find $x \in \mathfrak{q} \notin \mathfrak{p}$.

   Further, note that x can be chosen to not be a zero-divisor, yielding

   $$0 \to M \xrightarrow{x} M \to M/xM \to 0.$$

   In particular, Lemma 7.15 tells us that

   $$P_{\mathfrak{q},M} = P_{\mathfrak{q},M} + P_{\mathfrak{q},M/xM} - F.$$

   We now appeal to the following lemma to give $\deg P_{\mathfrak{q},M/xM} < \deg P_{\mathfrak{q},M} \leq \dim M$ exactly.

Lemma 7.19. If M is a finitely generated R-module with $x \in \mathfrak{m}$, then

$$\dim M/xM \geq \dim M - 1.$$

Thus, we get $\deg P_{\mathfrak{q},M/xM} = \dim M - 1$, so we are done by an induction on M, from this last statement.

The above steps finish the proof. ■

Corollary 7.20. Fix a local Noetherian ring R and a finitely generated module M. Then $\dim M = \dim \widehat{M}$. In particular, $\dim R = \dim \widehat{R}$.

Proof. This follows from the fact that $P_R = P_{\widehat{R}}$ because $H_R = H_{\widehat{R}}$ because

$$\operatorname{gr}_{\mathfrak{m}} R = \operatorname{gr}_{\widehat{\mathfrak{m}}} \widehat{R},$$

so we are done. ■

7.1.5 An Example

We close class with an example.

Exercise 7.21 (Eisenbud 12.2)**.** Consider the ideal $I \subseteq k[x,y,z,w]$ generated by the 2×2 minors of

$$\begin{bmatrix} x & y & z \\ y & z & w \end{bmatrix}.$$

In particular, $I := (xz - y^2, yw - z^2, xw - yz)$. We work out the Hilbert polynomial $P_{R,\mathfrak{q}}$ for $R = k[x,y,z,w]_{\mathfrak{m}}/I_{\mathfrak{m}}$, where $\mathfrak{m} = (x,y,z,w)$ and $\mathfrak{q} = (x,w)$.

Proof. We start by checking that $\mathfrak{q}$ is in fact of finite colength on R. Indeed, we are computing $\ell(R/\mathfrak{q})$, in which case (after taking the completion), we find

$$\ell(R/\mathfrak{q}) = \ell\left(\widehat{k[y,z]}/\left(y^2, z^2, yz\right)\right)$$

by sending z and w to 0. Because we can make three monomials, we see that this length is $3 < \infty$.

So we do indeed have a legitimate Hilbert function $H_{\mathfrak{q},R}$. The trick is to inject

$$R \to \widehat{k[s,t]}$$

by $x \mapsto s^3$ and $y \mapsto s^2 t$ and $z \mapsto st^2$ and $w \mapsto t^3$. We can check that this is an embedding. It follows that the image is all polynomials of degree divisible by 3, which for sufficiently large n agrees with a polynomial of degree 2 because we can compute directly as $3m + 1$ different monomials of prescribed degree. So our dimension comes out to be $\boxed{2}$. ■

7.2 April 14

Welcome back to class.

7.2.1 Overview

We take the following definition.

Definition 7.22 (Affine ring)**.** A ring R is *affine* if and only if it is finitely generated over a field as

$$k[x_1, \ldots, x_n]/I.$$

In particular, if I is prime, then R is a domain.

Today we are working towards the following theorem.

Theorem 7.23. Fix an affine domain R over the field k. Then $\dim R$ is equal to the transcendence degree of $K(R)$ over k.

Recall that the transcendence degree is defined as follows.

Definition 7.24. Fix an extension of fields K/k. Then one can choose a maximal set $\mathcal{B}$ of algebraically independent elements of K over k. The *transcendence degree of K over k* is $\#\mathcal{B}$.

It requires checking that the transcendence degree is well-defined and that

$$k[\mathcal{B}] \subseteq K$$

is an algebraic extension; this last assertion is just by maximality.

We will also show the following result.

Theorem 7.25. Fix an affine domain R over a field k. Then a maximal chain of prime ideals

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

in R has $m = \dim R$.

Intuitively, this is what we expect from vector spaces: any maximal basis has the same size.

Remark 7.26. There is an example in the homework that this does not true for general rings.

7.2.2 Proofs

In particular, we will use Noether normalization to prove Theorem 7.23 and Theorem 7.25. Before stating this, we prove the following result.

Lemma 7.27. Fix a polynomial ring $T := k[x_1, \ldots, x_r]$ and nonconstant polynomial $f \in T$. Then there are $x_1', \ldots, x_{r-1}'$ such that T is finite over $S := k[x_1', \ldots, x_{r-1}', f]$. If k is infinite, then we can choose the x_i' by taking $a_1, \ldots, a_{r-1}$ and setting $x_i' := x_i - a_i x_r$.

Proof. Supposing from the case that k is infinite, we see that the x_i are automatically in $k[x_1', \ldots, x_{r-1}', x_r]$, so it suffices to show that x_r is the root of some monic finite polynomial in $k[x_1', \ldots, x_r', f]$. For this, we can just stare at the system of equations

$$f(x_1, \ldots, x_r) = f(x_1' + a_1 x_r, \ldots, x_{r-1} + a_{r-1} x_r, x_r).$$

By inducting downwards, it suffices to set f_d to be the terms of maximal homogeneous degree and work with f_d. In particular, we find

$$f_d(x_1' + a_1 x_r, \ldots, x_{r-1}' + a_{r-1} x_r, x_r) = f_d(a_1, \ldots, a_{r-1}, 1) x_r^d + \sum_{i=0}^{d-1} c_i(x_1', \ldots, x_{r-1}') x_r^i.$$

This will be a fine monic polynomial for f, provided we can make $f_d(a_1, \ldots, a_{r-1}, 1)$ nonzero, but because k is infinite (!), we can find some a_i to work.

Now take k to be finite. The point is to set e very large (explicitly, larger than the degree of x_i in any monomial of f) and set

$$x_i' := x_i - x_r^{e^i}.$$

Some estimates combined with the previous trick is enough to give us our monic polynomial. ■

And here is our result.

Theorem 7.28 (Noether normalization)**.** Fix an affine ring R of dimension d. Given a chain

$$I_1 \subseteq I_2 \subseteq \cdots \subseteq I_m \subseteq R$$

with $d_j := \dim I_j$ such that $\{d_j\}_{j=0}^m$ is strictly decreasing. Then there is a subring $S \subseteq R$ such that

(a) $S \cong k[x_1, \ldots, x_d]$,

(b) R is finite over S, and

(c) any ideal I_j has $S \cap I_j = (x_{d_j+1}, \ldots, x_d)$.

In essence the given filtration on R becomes the polynomial filtration for S, which is quite amazing.

Proof. Because R is an affine ring, we can write $R = T/I$, where R is some polynomial ring. In particular, pulling back to T gives a filtration

$$I \subseteq I_1 \subseteq I_2 \subseteq \cdots \subseteq I_m \subseteq T$$

and run the theorem though. Thus, it suffices to take $R := k[y_1, \ldots, y_d]$ to be a polynomial ring.

Now, find any $x_d \in I_m$. By Lemma 7.27, we can find variables $x_1', \ldots, x_{d-1}'$ so that

$$k[x_1', \ldots, x_{d-1}', x_d] \subseteq I_m.$$

We can repeat this process. To be rigorous, suppose that we are in the middle of this process so that we have written down

$$k[x_1', \ldots, x_p', x_{p+1}, \ldots, x_d]$$

so that $(x_q, \ldots, x_d) \subseteq I_j$ for all $q > p$. To construct x_p, we have two cases.

- If $d_j = p$, then choose $x_p \in I_{j-1}$ and use Lemma 7.27 to move downwards.
- Otherwise, $d_j > p$, then choose x_p from I_j, doing the same thing. Notably, in this case, we know that such an x_p exists here by a dimension argument: we know that

$$\dim(x_{p+1}, \ldots, x_d) \leq \dim I_j,$$

  and we are getting strict inequality here because equality would make our extension integral, which is bad.

We can continue the above process downward until $j = 0$. Thus,

$$S = k[x_1, \ldots, x_d]$$

is finitely generated by d elements. Now, certainly

$$I_j \cap S$$

will contain $(x_{d_j+1}, \ldots, x_d)$ (by construction) and $\dim(I_j \cap S) = \dim I_j = d_j$, so we get our equality just fine. Namely, we cannot go any bigger, lest we violate the dimension. ∎

From here Theorem 7.23 follows quickly.

Proof of Theorem 7.23. By Theorem 7.28, we extract our promised S. Now,

$$K(S) \subseteq K(R)$$

is finite (because $S \subseteq R$ is finite) and hence algebraic, so the transcendence degree of $K(S)$ over k is equal to the desired transcendence degree. But now this transcendence degree is equal to the number of variables of S, which is $\dim R = \dim S$. This finishes. ∎

And here is the proof of the second part.

Proof of Theorem 7.25. Fix a maximal chain of disctint primes

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

in R. Extracting S as needed from Theorem 7.28, we see that we do get a maximal chain of primes

$$\mathfrak{q}_0 \subsetneq \mathfrak{q}_1 \subsetneq \cdots \subsetneq \mathfrak{p}_m$$

by intersection. In particular, we get $m \leq \dim S$. Because primes in S are pretty well-understood (namely, these are just generated by the free variables in S by construction of S), so $m < \dim S$ would imply that the bottom chain is not maximal; suppose we can insert some prime $\mathfrak{q}$ as

$$\mathfrak{q}_j \subsetneq \mathfrak{q} \subsetneq \mathfrak{q}_{j+1}$$

for some j. Thus, lifting (which we know to be at least comparable), we get the following image.

$$\begin{tikzcd}
\mathfrak{q}_j \arrow[r, phantom, "\subsetneq"] \arrow[d, dash] & \mathfrak{q} \arrow[r, phantom, "\subsetneq"] \arrow[d, dash] & \mathfrak{q}_{j+1} \arrow[d, dash] \\
\mathfrak{p}_j \arrow[r, phantom, "\subsetneq"] & \mathfrak{p} \arrow[r, phantom, "\subsetneq"] & \mathfrak{p}_{j+1}
\end{tikzcd}$$

Modding out by $\mathfrak{p}_j$, we may assume that $\mathfrak{p}_j = \mathfrak{q}_j = 0$. Now, we can certainly go up, as we discussed earlier in the class, so going down (preserving the inclusions!) is the only problem. As such, we have the following lemma.

Lemma 7.29. Fix a normal ring S and a finite S-algebra R. If we are given primes

$$\mathfrak{q} \subsetneq \mathfrak{q}_1$$

of S such that there exists a prime $\mathfrak{p}_1$ of R with $\mathfrak{q}_1 = \mathfrak{p}_1 \cap S$, then there exists a prime $\mathfrak{p}$ such that $\mathfrak{q} = \mathfrak{p} \cap S$.

Proof. Diagrammatically, we are constructing the highlighted prime below.

$$\begin{tikzcd}
\mathfrak{p} \arrow[r, phantom, "\subsetneq"] \arrow[d, dash] & \mathfrak{p}_1 \arrow[d, dash] \\
\mathfrak{q} \arrow[r, phantom, "\subsetneq"] & \mathfrak{q}_1
\end{tikzcd}$$

This is a little hard. We know that $K(S) \subseteq K(R)$ is a finite extension of fields, so we can find a normal closure L, and we set $G := \operatorname{Gal}(L/K(S))$. We then set T to be the integral closure of R in L, giving the following tower.

$$\begin{tikzcd}
 & & T \arrow[r, phantom, "\subseteq"] \arrow[d, dash] & L \arrow[d, dash] \\
\mathfrak{p} \arrow[r, phantom, "\subseteq"] \arrow[d, dash] & \mathfrak{p}_1 \arrow[d, dash] & R \arrow[r, phantom, "\subseteq"] \arrow[d, dash] & K(R) \arrow[d, dash] \\
\mathfrak{q} \arrow[r, phantom, "\subseteq"] & \mathfrak{q}_1 & S \arrow[r, phantom, "\subseteq"] & K(S)
\end{tikzcd}$$

Now, we lift construct lifts as follows.

$$\begin{tikzcd}
\mathfrak{p}'' \arrow[r, phantom, "?"] \arrow[d, dash] & \mathfrak{p}_1'' \arrow[d, dash] & T \arrow[r, phantom, "\subseteq"] \arrow[d, dash] & L \arrow[d, dash] \\
\mathfrak{p} \arrow[r, phantom, "\subseteq"] \arrow[d, dash] & \mathfrak{p}_1 \arrow[d, dash] & R \arrow[r, phantom, "\subseteq"] \arrow[d, dash] & K(R) \arrow[d, dash] \\
\mathfrak{q} \arrow[r, phantom, "\subseteq"] & \mathfrak{q}_1 & S \arrow[r, phantom, "\subseteq"] & K(S)
\end{tikzcd}$$

A priori, we cannot construct $\mathfrak{p}''$ to live inside $\mathfrak{p}_1''$, but it turns out that a Galois conjugate of $\mathfrak{p}''$ will be good enough: upon intersecting back down with R, all will be made well, for we can get inside $\mathfrak{p}_1$ while still being on top of $\mathfrak{q}$. ■

To complete the proof of the above lemma, we need to finish the proof of the result on conjugates of primes. This is as follows.

Proposition 7.30. Fix a normal domain S and a field L such that $K(S) \subseteq L$ is a finite normal extension with Galois group G. Letting T be the integral closure of S in L, then G acts transitively on the primes lying over some fixed prime $\mathfrak{q}$ of S.

Proof. Let $\mathfrak{p}_1, \ldots, \mathfrak{p}_n$ be a G-orbit of primes in T lying over $\mathfrak{q}$. Now, suppose for the sake of contradiction that we have a prime $\mathfrak{p}$ lying over $\mathfrak{q}$ distinct from all of these. Because primes lying over $\mathfrak{q}$ are incomparable, we find some $a \in T$ in $\mathfrak{p}$ but none of the $\mathfrak{p}_i$.

However, we see that

$$\prod_{g \in G} ga$$

lives in $\mathfrak{p} \cap S = \mathfrak{q}$ while not living in any of the $\mathfrak{p}_i$ (because we have a Galois orbit present here), which is a contradiction. Note that we used normality when showing $S = R^G$. ■

This completes the proof of Theorem 7.25. ■

7.2.3 Corollaries

Let's show some corollaries because we have a little time on our hands.

Corollary 7.31. Fix an affine domain R. Given an ideal $I \subseteq R$, we have

$$\dim I + \operatorname{codim} I = \dim R.$$

Proof. If I is not prime, then take I to be any minimal prime $\mathfrak{p}$ containing I. Then this is exactly Theorem 7.25, upon gluing chains ascending and descending from $\mathfrak{p}$. ■

Corollary 7.32. Fix an affine domain R. Then $\dim R = \operatorname{codim} \mathfrak{m}$ for any maximal ideal $\mathfrak{m} \subseteq R$.

Proof. Fix any maximal descending chain from $\mathfrak{m}$; then this comes from Theorem 7.25. ■

Remark 7.33. Geometrically, we are saying that we can determine the dimension of R (when R is the coordinate ring of an affine variety) locally at any point.

Corollary 7.34. Suppose that we have an inclusion $R \subseteq T$ of affine domains over k. Then

$$\dim T = \dim R + \dim K(R) \otimes_R T.$$

Proof. The point is to use Theorem 7.23, using the chain

$$k \subseteq K(R) \subseteq K(T).$$

In particular, by additivity of the transcendence degree, it suffices to show that the transcendence degree of $K(R) \subseteq K(T)$ is the dimension of $\dim K(R) \otimes_R T$, which is true by staring at it, I guess. ■

Remark 7.35. Geometrically, we are saying that the dimension of a generic fiber $K(R) \otimes_R T$ plus the dimension of the base of a family $\dim R$ is equal to the dimension of the original variety $\dim T$.

Corollary 7.36. Fix an affine domain R and a nonzero, non-unit $f \in R \setminus (\{0\} \cup R^\times)$. Then

$$\dim R/(f) = \dim R - 1.$$

Proof. Certainly $\dim R/(f) < \dim R$ because (f) lives in some maximal ideal $\mathfrak{m}$, so $\dim R/(f) \le \operatorname{codim} \mathfrak{m} < \dim R$. On the other hand, localizing R at any maximal ideal $\mathfrak{m}$ containing (f), we see that

$$\dim R_\mathfrak{m}/(f)R_\mathfrak{m} \ge \dim R_\mathfrak{m} - 1$$

as we showed earlier for general modules over a local ring, which completes the proof. ■

7.3 April 19

Welcome back.

7.3.1 The Nullstellensatz Two, Electric Boogaloo

Last time we showed Noether normalization. Today we go over some consequences. Recall the statement of Noether normalization.

Theorem 7.37 (Noether normalization)**.** Fix an affine ring R of dimension d. Given a chain

$$I_1 \subseteq I_2 \subseteq \cdots \subseteq I_m \subseteq R$$

with $d_j := \dim I_j$ such that $\{d_j\}_{j=0}^m$ is strictly decreasing. Then there is a subring $S \subseteq R$ such that

(a) $S \cong k[x_1, \ldots, x_d]$,

(b) R is finite over S, and

(c) any ideal I_j has $S \cap I_j = (x_{d_j+1}, \ldots, x_d)$.

As an example application, we show Hilbert's Nullstellensatz.

Theorem 7.38 (Nullstellensatz)**.** Fix R an (affine) k-algebra.

(a) Given a maximal ideal $\mathfrak{m} \subseteq R$, then $R/\mathfrak{m}$ is a finite extension of k. In particular, if k is algebraically closed, then $R/\mathfrak{m} \cong k$.

(b) The ring R is Jacobson: any prime ideal is the intersection of maximal ideals.

From here one can deduce the usual Nullstellensatz. Anyway, let's prove this.

Proof. We go one at a time.

(a) The dimension of $R/\mathfrak{m}$ is 0 because $R/\mathfrak{m}$ is a field, but $R/\mathfrak{m}$ is an integral extension of k (because R is) while being of finite length (and finitely generated as a k-algebra), so $R/\mathfrak{m}$ is a finite extension of k.

(b) As usual, pick up a prime $\mathfrak{p}$, and we need to show

$$\mathfrak{p} \stackrel{?}{=} \bigcap_{\mathfrak{m} \supseteq \mathfrak{p}} \mathfrak{m}.$$

Certainly we have $\subseteq$, so we show $\supseteq$. As such, for each $f \notin \mathfrak{p}$, we need to show that there exists a maximal ideal $\mathfrak{m}$ containing $\mathfrak{p}$ but not f.

Now, taking the quotient by $\mathfrak{p}$, we may assume that R is an integral domain and that $\mathfrak{p} = (0)$. In particular, we need to show that $f \neq 0$ is avoided by some maximal ideal. However, we showed last time that

$$\dim R/(f) = \dim R - 1.$$

Running through Noether normalization, we can choose $S \cong k[x_1, \ldots, x_d]$ so that $S \cap (f) = (x_1)$. So to get our maximal ideal, we choose

$$(x_1 - 1, x_2, x_3, \ldots, x_d) \subseteq S$$

and then lift to R to some maximal ideal $\mathfrak{n}$. Notably, $f \in \mathfrak{n}$ implies that $\mathfrak{n} \cap S$ contains x_1, which doesn't make sense by the above construction. This finishes. ■

7.3.2 The Geometric $AKLB$ Set-Up

Here is another application.

Proposition 7.39 ($AKLB$ for geometers)**.** Fix an affine domain R over a field k. Now, set L to be a finite extension of $K := K(R)$, and let T be the integral closure of R in L. Then T is a finitely generated R-module; in particular, T is an affine domain.

Proof. Here is the image.

$$\begin{array}{ccc} T & \subseteq & L \\ | & & | \\ R & \subseteq & K \end{array}$$

To begin, we use Noether normalization to force S to be a polynomial ring. Namely, T is still integral over S (because of the chain $S \subseteq R \subseteq T$), and it still suffices to show that T is finite over S.

As such, we may assume that R is a unique factorization domain and in particular is normal. As another reduction, by taking the normal closure of L, we would only make T bigger, so it suffices to take L/K to be a normal extension of fields.

We would like our extension to be Galois, but for this we must fight with the separability condition. In particular, L/K is an inseparable extension if an only if there is an irreducible polynomial $\pi \in K[x]$ with a multiple root α; here, this element α is called purely inseparable. This will in fact mean that $\alpha(\operatorname{char} K)^n \in K$ for some n.

Nonetheless, with L/K any normal extension, we can talk about its automorphism group G and then build the following tower.

$$\begin{array}{l} L \\ \big| \text{ purely insep} \\ L^G \\ \big| \text{ Galois} \\ G \end{array}$$

Namely, we want to not think very hard about L/L^G, but we must.

Example 7.40. The extension $k(t) \subseteq k\left(t^{1/p}\right)$, where $p := \operatorname{char} k > 0$, is a purely inseparable extension.

Anyway, this tower that we may assume that L/K is either Galois or purely inseparable. We do these cases separately.

- Take L/K to be purely inseparable. Here, $K = k(x_1, \ldots, x_d)$. Because L/K is finite and purely inseparable, we can find some q (which is a large power of p) so that L is contained in

$$k'\left(x_1^{1/q}, \ldots, x_d^{1/q}\right),$$

  where in k' we have to possibly add in some qth roots to make this legal. In particular, we take $L = K\left(\alpha_1^{1/q}, \ldots, \alpha_d^{1/q}\right)$ and then take out the qth roots of variables we need using the fact that $(x+y)^q = x^q + y^q$.

  As such, it suffices to show our result in the case where $L = k'\left(x_1^{1/q}, \ldots, x_d^{1/q}\right)$. But now we can exactly describe our integral closure as

$$T = k'\left[x_1^{1/q}, \ldots, x_d^{1/q}\right],$$

  which is finite over R because k'/k is finite, and each of the $x_i^{1/q}$ is the root of a monic polynomial $t^q - x_i = 0$ over R. This finishes.

- Now take L/K to be a Galois extension. We pick up the following lemma. We simply outsource the logic here to the following lemma.

Lemma 7.41. Fix a normal Noetherian domain R. Now, set L to be a finite, Galois extension of $K := K(R)$ where $G := \operatorname{Gal}(L/K)$, and let T be the integral closure of R in L. Then T is a finitely generated R-module.

Proof. Note $R \subseteq K = L^G$, and R is normal (i.e., is its own Galois closure in K), so it follows that $R^G = R$. Now, by clearing denominators, we may choose elements $b_1, \ldots, b_n$ to be a basis of L over K. Additionally, we enumerate the elements of G as

$$\{g_1, \ldots, g_n\},$$

where $n := \#\operatorname{Gal}(L/K) = [L : K]$. Now, the Galois action preserves integrality, so the matrix

$$M := \begin{bmatrix} g_1b_1 & \cdots & g_1b_n \\ \vdots & \ddots & \vdots \\ g_nb_1 & \cdots & g_nb_n \end{bmatrix}.$$

Now, set $d := \det M$. We make the following observations about d.

- Note that $d \neq 0$ because this would require a relation of the rows

$$\sum_{i=1}^n a_ig_ib_j = 0$$

  for all j, so in particular $\sum_i a_ig_i = 0$ (as a function $L \to K$!), which contradicts linear independence of automorphisms.[1]

- We do see that $d^2 \in R$ because, picking up any $g \in G$ to the matrix M will merely permute the rows of M, so $gd = \pm d$. In particular, d^2 is fixed by G and hence lives in K. Because d is a linear combination of integral elements (namely, elements that live in T), it is integral over R, so $d \in R$ by normality.

- Lastly, we note that $T \subseteq \frac{1}{d^2}R$. Well, pick up some $b \in T$ and write

$$b = \sum_{i=1}^n a_ib_i$$

[1] This linear independence is Artin's lemma. As a sketch of the proof, if there is a nontrivial relation, choose the smallest relation, and then rearrange by plugging things in to subtract off and get a smaller relation.

with $a_i \in K$ using the fact that the $\{b_i\}$ are a basis of L/K. However, pushing this "vector" through M, the ith component comes out to

$$\sum_{j=1}^{n} g_i(b_j) \cdot c_j = g_i\left(\sum_{j=1}^{n} c_j b_j\right) = g_i(b) \in T.$$

In particular, letting M^* denote the adjugate matrix of M, we see that pushing M^* through the above will show that all coefficients live in $\frac{1}{d}R \subseteq \frac{1}{d^2}R$ (because $M^*M = dI$). Thus, we get $c_i \in \frac{1}{d}R$, which is what we wanted.

The last claim shows that T is a submodule of a finitely generated R-module, which shows that T is finite over R, as needed. ■

The above lemma finishes the last case of the proof. ■

Here is an example application.

Exercise 7.42. Fix an algebraically closed field k of characteristic 0. Then consider the fraction field of $k[\![x]\!]$ as

$$k[\![x]\!] \subseteq k((x)).$$

However, $k((x))$ no longer needs to be algebraically closed, so let L be some finite extension. Then, setting T to be the integral closure of R in L, we get that T is finite over R by Proposition 7.39. In fact, we show $T \cong k[\![x^{1/n}]\!]$ for some n.

Proof. Note that T is normal, local, and finitely generated over the ring R. Letting $\mathfrak{m}$ be its maximal ideal, we can get $\mathfrak{m} = (\pi)$ for some element π by pushing a little. As such, T we see that T is a discrete valuation ring. Further, because T is finite over R, we get some n such that

$$\pi^n$$

can be written as lower terms. But this requires $\pi^n = ux$ for some unit u, and the unit u has an nth power by Hensel's lemma (here is where we use $\operatorname{char} k = 0$), so we get that we can replace π by $t^{1/n}$. This finishes. ■

Remark 7.43. This classifies all algebraic extensions of $k((x))$ as $k((x^{1/n}))$, so the algebraic closure of $k((x))$ is simply

$$\bigcup_{n \geq 1} k((x^{1/n})),$$

which is pretty nice.

Example 7.44. Fix some $f \in \mathbb{C}[x,y]$. Writing down $f \in \mathbb{C}[x][y]$ as a polynomial in y, we may write

$$f(x,y) = \sum_{i=1}^{n} p_n(x) y^n.$$

Taking the completion to $\mathbb{C}[\![x]\!][y]$ (i.e., looking locally at $x = 0$), we hope that f is still irreducible; otherwise, we can just take some irreducible factor. Now, we can directly solve for y in this system as some series

$$\sum_{i=-m}^{\infty} c_i x^{i/n}.$$

Now, if p_n is monic, then we can assert that y lives in the integral closure of R, so q is a bona fide power series.

7.3.3 Invariant Theory

Let's return to discussing invariant theory for the end of class; recall that, in an invariant theory, we are interested in studying the group invariants of some group action on an affine ring. We have the following result.

Theorem 7.45. Fix a finite group G and an affine ring T with a G-action. Then T^G is also an affine ring.

Proof. In some sense, we are "quotienting" by the G-action and hoping that we recover an affine ring. Very quickly, note that T is integral over T^G, which we get because G is finite. Namely, for $a \in T$, we simply use the polynomial

$$\prod_{g \in G} (x - ga),$$

which is monic and in $T^G[x]$ because multiplying by some $g \in G$ will merely permute the terms of the product.

We now note that, because T is an affine ring, we suppose that the elements $\{y_1, \ldots, y_m\}$ generate T. Now, we let S be the k-algebra generated by the elementary symmetric polynomials in the $g_i y_j$, of which there are still finitely many while maintaining $S \subseteq T^G$. Now, T is a finitely generated S-module because the generators of S are roots of the polynomials

$$\prod_{g \in G} (x - gy_j) \in S[x],$$

so T is finite over S, meaning that T^G is finite over S. It follows that T^G is an affine ring. ■

Our last topic is on elimination theory, which is what we will spend the next two lectures on. We will have a total of 13 homeworks.

7.4 April 26

We begin with some announcements.

- There will be no class on Thursday.
- There will be a review session next Tuesday.

7.4.1 Projective Varieties

Today we are speed-running elimination theory. There will be a lot of geometry. At a high level, commutative rings are supposed to be functions over affine varieties. Similarly, graded rings are supposed to be functions over a projective variety.

As in the case of affine rings, points and varieties are cut out by ideals of

$$k[x_0, \ldots, x_n].$$

Explicitly, this time our varieties are cut out by homogeneous polynomials, and our points are in bijection with maximal homogeneous ideals except for the irrelevant ideal $(x_0, \ldots, x_n)$. We will not prove this here, but we will state that these maximal homogeneous ideals take the form

$$\mathfrak{m}_a = (a_\ell x_k - a_k x_\ell),$$

where $a = (a_0 : \cdots : a_n)$ is some point in $\mathbb{P}^n(k)$; in particular, the thing that we would have to check is that $V(\mathfrak{m}_a)$ is the line spanned by $(a_0, \ldots, a_n)$ in $\mathbb{A}^{n+1}(k)$.

We pick up the following facts.

Proposition 2.204. Fix $R = R_0 \oplus R_1 \oplus \cdots$ a graded ring and M a graded module over R. Suppose that we have $m \in M$ and $\mathfrak{p} := \operatorname{Ann} m$ an associated prime ideal. Then $\mathfrak{p}$ is a graded ideal of R.

There is also a notion of Noether normalization for graded rings.

Proposition 7.46. Fix a graded (affine) ring R of dimension n. Then one can choose homogeneous and algebraically independent elements $x_1, \ldots, x_n \in R$ so that R is finite over $k[x_1, \ldots, x_n]$.

Proof. A similar proof to the Noether normalization theorem (Theorem 7.28) applies here. ■

Proposition 2.93. Fix affine algebraic sets X and Y. Then $A(X \times Y) \cong A(X) \otimes_k A(Y)$ canonically as k-algebras.

Proof. This is on the homework, though these notes do include a proof from earlier. ■

We would like to do something like Proposition 2.93 for projective varieties. Namely, Proposition 2.93 tells us how to turn the product of affine varieties into an affine variety, but this is a little subtler for projective varieties.

Well, let's take two projective spaces $\mathbb{P}^m(k)$ and $\mathbb{P}^n(k)$. Then, given two points $(x_0 : x_1 : \ldots : x_m)$ and $(y_0 : y_1 : \ldots : y_n)$, we want to glue them together in some meaningful way. In particular, we hope that

$$\mathbb{P}^m(k) \times \mathbb{P}^n(k)$$

is a projective variety in some larger space. To begin, we make a matrix

$$M := \begin{bmatrix} x_0y_0 & \cdots & x_0y_n \\ \vdots & \ddots & \vdots \\ x_my_0 & \cdots & x_my_n \end{bmatrix}.$$

This makes an $(m+1) \times (n+1)$ matrix, defined up to scalar: scaling either $(x_0 : \ldots, x_m)$ or $(y_0 : \ldots : y_n)$ by some $c \in k^\times$ merely multiplies either all rows or all columns (respectively) by the scalar c. Thus, "linearizing" M, we think about M as living in $\mathbb{P}^{(m+1)(n+1)-1}$.

This gives us a way to map $\mathbb{P}^m(k) \times \mathbb{P}^n(k)$ into a large projective space, but we still need to actually cut out our variety; observe that it is not even completely obvious that we can do this because the map

$$\mathbb{P}^m(k) \times \mathbb{P}^n(k) \to \mathbb{P}^{(m+1)(n+1)-1}(k)$$

is continuous (as an embedding), which need not send Zariski closed sets to Zariski closed sets. Regardless, we define

$$z_{ij} := x_iy_j.$$

Now, pick a pair of indices (i, j) and (i', j'), and we note that the matrix

$$\begin{bmatrix} x_iy_j & x_iy_{j'} \\ x_{i'}y_j & x_{i'}y_{j'} \end{bmatrix}$$

is also invariant up to scaling (for the same reason that M is), so in particular its determinant should vanish; as such, we should mod out $\mathbb{P}^{(m+1)(n+1)-1}(k)$ out by the polynomials

$$z_{i\ell}z_{kj} = z_{ij}z_{k\ell}.$$

We will not prove it here, but these relations are sufficient to cut out $\mathbb{P}^m(k) \times \mathbb{P}^n(k)$.

7.4.2 Elimination Theory Examples

We are now ready to formulate the main theorem of elimination theory.

Theorem 7.47. Fix an affine variety X over an algebraically closed field k and consider the natural projection map $\pi\colon X \times \mathbb{P}^n(k) \to X$ for some projective space $\mathbb{P}^n(k)$. Then, given a closed subset $Z \subseteq X \times \mathbb{P}^n(k)$, the image $\pi(Z)$ is also closed.

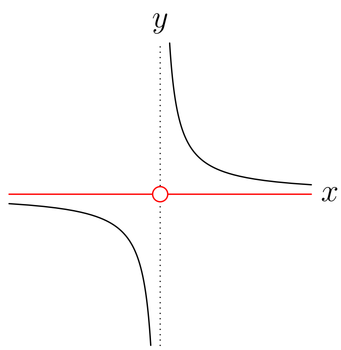
Note that there is a reason why we are using projective space for our second coordinate.

Exercise 7.48. Fix an algebraically closed field k. Let $\pi\colon \mathbb{A}^1(k)\times\mathbb{A}^1(k) \to \mathbb{A}^1(k)$ be the natural projection onto the first coordinate. We exhibit a closed subset $Z \subseteq \mathbb{A}^1(k) \times \mathbb{A}^1(k)$ such that $\pi(Z)$ is not closed.

Proof. By Proposition 2.93, we might as well think about $\mathbb{A}^1(k)\times\mathbb{A}^1(k)$ as $\mathbb{A}^2(k)$ because they have the same affine coordinate rings. As such, the point is that π is merely a continuous map and need not send closed sets to closed sets; to manifest this, we set

$$Z := \left\{(x,y) \in \mathbb{A}^2(k) : xy = 1\right\}.$$

Now, $\pi(Z) = \mathbb{A}^1(k) \setminus \{0\}$. Here is the image.



It is not terribly difficult to just compute $\pi\left(Z\right)$ directly.

- For $x \neq 0$, we see that $(x, 1/x) \in Z$, so $x \in \pi(Z)$.
- For $x = 0$, there is no $y \in k$ such that $xy = 1$, so $x \notin \pi(Z)$.

The above cases do verify that $\pi(Z) = \mathbb{A}^1(k) \setminus \{0\}$. It remains to see that $\pi(Z)$ is not actually Zariski closed. Well, for any $f \in k[x]$ vanishing on $\pi(Z)$, we see that f must have infinitely many roots from $k \setminus \{0\}$ (because k is algebraically closed), so $f = 0$. It follows that

$$V(I(\pi(Z))) = V((0)) = \mathbb{A}^1(k),$$

so $\pi(Z)$ is not equal to its own Zariski closure, implying that $\pi(Z)$ is not Zariski closed. ■

Let's explain why we are calling our theory "elimination theory." To begin, note that all points take the form

$$\big(\underbrace{(x_1, \ldots, x_m)}_{s}, (y_0 : \ldots : y_n)\big) \in X \times \mathbb{P}^n(k).$$

Now, we can define our Zariski closed subset $Z \subseteq X \times \mathbb{P}^n(k)$ via some equations

$$\begin{cases} f_1(s, y_0, \ldots, y_n) = 0, \\ \qquad \vdots \\ f_r(s, y_0, \ldots, y_n) = 0. \end{cases}$$

Now, $\pi(Z)$ consists of those $s \in X$ such that there exists some point $(y_0 : \ldots : y_n) \in \mathbb{P}^n(k)$ living in Z; in other words, we are searching for $s \in X$ such that there is a nonzero solution $(y_0, \ldots, y_n)$ to the above equations $f_1, \ldots, f_s$. So we are in some sense trying to "eliminate" these $y_\bullet$ from our parameters.

There was a relatively rich classical field dealing with these types of questions; let's see a few examples; we start with two variables and two linear equations.

Exercise 7.49. Work in the context of Theorem 7.47, and fix $Z \subseteq X \times \mathbb{P}^1(k)$ given by the equations

$$\begin{cases} f_0(s)y_0 + f_1(s)y_1 = 0, \\ g_0(s)y_0 + g_1(s)y_1 = 0. \end{cases} \tag{1}$$

We verify that $\pi(Z) \subseteq X$ is Zariski closed.

Proof. We need to find all $s \in X$ such that there is $(y_0 : y_1) \in \mathbb{P}^1(k)$ so that $(s, (y_0 : y_1))$ satisfies (1). Of course, the $(y_0 : y_1)$ really have no constraints except for being nonzero, so we are really asking for (1) to have a solution (s, y_0, y_1) where $(y_0, y_1) \neq (0, 0)$.

Imagining that s is fixed for a moment, we see that we are thus really asking for

$$\begin{bmatrix} f_0(s) \\ g_0(s) \end{bmatrix} \quad \text{and} \quad \begin{bmatrix} f_1(s) \\ g_1(s) \end{bmatrix}$$

to have a nontrivial relation (given by (y_0, y_1)), which is equivalent to the matrix

$$M := \begin{bmatrix} f_0(s) & f_1(s) \\ g_0(s) & g_1(s) \end{bmatrix}$$

being singular. Well, M is singular if and only if $\det M$ vanishes, so we see we are asking for all $s \in X$ such that

$$g_1(s)f_0(s) - f_1(s)g_0(s) = 0,$$

This does indeed cut out an algebraic set of X, so we are safe. ■

Going a little further, we can do arbitrary two variables and two equations in general.

Exercise 7.50 (Sylvester)**.** Work in the context of Theorem 7.47, and fix $Z \subseteq X \times \mathbb{P}^1(k)$ given by the equations

$$\begin{cases} f_0(s)y_0^d + f_1(s)y_0^{d-1}y_1 + \cdots + f_{d+1}(s)y_1^d = 0, \\ g_0(s)y_0^e + g_1(s)y_0^{e-1}y_1 + \cdots + g_{e+1}(s)y_1^e = 0. \end{cases} \tag{2}$$

We verify that $\pi(Z)$ is Zariski closed.

Proof. The point is to use the resultant. In the following discussion, we will fix some $s \in X$ and write f_i and g_j for $f_i(s)$ and $g_j(s)$, respectively. To construct the resultant, we build the following $e \times (e + d)$ matrix

$$\begin{bmatrix} f_0 & f_1 & \cdots & f_{d+1} & 0 & \cdots & 0 & 0 \\ 0 & f_0 & \cdots & f_d & f_{d+1} & \cdots & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \cdots & 0 & 0 & \cdots & f_{d+1} & 0 \\ 0 & 0 & \cdots & 0 & 0 & \cdots & f_d & f_{d+1} \end{bmatrix}$$

and attach the following $d \times (e + d)$ matrix

$$\begin{bmatrix} g_0 & g_1 & \cdots & g_{e+1} & 0 & \cdots & 0 & 0 \\ 0 & g_0 & \cdots & g_e & g_{e+1} & \cdots & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \cdots & 0 & 0 & \cdots & g_{e+1} & 0 \\ 0 & 0 & \cdots & 0 & 0 & \cdots & g_e & g_{e+1} \end{bmatrix}$$

below it to make a $(e+d)\times(e+d)$ matrix. For concreteness, our matrices will be written with $d=2$ and $e=3$ (though the argument will work in higher generality), which gives

$$M := \begin{bmatrix} f_0 & f_1 & f_2 & & \\ & f_0 & f_1 & f_2 & \\ & & f_0 & f_1 & f_2 \\ g_0 & g_1 & g_2 & g_3 & \\ & g_0 & g_1 & g_2 & g_3 \end{bmatrix}.$$

We claim that we have a solution to our equations for a given $s\in X$ if and only if the determinant of M vanishes.

In one direction, suppose that $s\in\pi(Z)$ so that we have a point $(y_0,y_1)\neq(0,0)$ such that $(s,(y_0,y_1))\in Z$. The main point is to consider the following matrix product

$$\begin{bmatrix} f_0 & f_1 & f_2 & & \\ & f_0 & f_1 & f_2 & \\ & & f_0 & f_1 & f_2 \\ g_0 & g_1 & g_2 & g_3 & \\ & g_0 & g_1 & g_2 & g_3 \end{bmatrix} \begin{bmatrix} y_0^4 \\ y_0^3y_1 \\ y_0^2y_1^2 \\ y_0y_1^3 \\ y_1^4 \end{bmatrix}.$$

Now, by multiplying our equations through, we see that the first e rows are all the first equation of (2) multiplied by some suitable $y_0^ay_1^b$, and the last d rows are the second equation of (2) again multiplied by some suitable $y_0^ay_1^b$. In particular, because our point (y_0,y_1) satisfies (2), we have found a nontrivial element in $\ker M$ (nontrivial because $y_0\neq0$ or $y_1\neq0$), so $\det M=0$ follows.

In the reverse direction, suppose $\det M=0$. Set V_n to be the k-vector space of homogeneous spaces of degree n in $k[y_0,y_1]$; by the usual monomial-counting arguments, we see $\dim V = n+1$, spanned by the monomials

$$y_0^n,\, y_0^{n-1}y_1,\, \ldots,\, y_0y_1^{n-1},\, y_1^n.$$

Note that multiplying by our first equation f gives us a map

$$\begin{aligned} \mu_f\colon V_{e-1} &\to V_{e+d-1} \\ \alpha &\mapsto \alpha f \end{aligned}$$

because f is homogeneous of degree d. Similarly, multiplying by our second equation gives us a map

$$\begin{aligned} \mu_g\colon V_{d-1} &\to V_{e+d-1} \\ \beta &\mapsto \beta g \end{aligned}$$

because g is homogeneous of degree e. In particular, we can glue these into a map $\mu_f\oplus\mu_g\colon V_{e-1}\oplus V_{d-1}\to V_{d+e-1}$, which we can see becomes a $(e+d)\times(e+d)$ matrix under our basis. In particular, we have

$$f\cdot y_0^ay_1^{e-1-a}=\sum_{k=0}^d f_ky_0^{a+d-k}y_1^{(e-1-a)+k} \qquad\text{and}\qquad g\cdot y_0^ay_1^{d-1-a}=\sum_{k=0}^e g_ky_0^{a+e-k}y_1^{(d-1-a)+k},$$

which means that $\mu_f\oplus\mu_g$ is the matrix (using $(d,e)=(2,e)$)

$$\begin{bmatrix} f_0 & & & g_0 & \\ f_1 & f_0 & & g_1 & g_0 \\ f_2 & f_1 & f_0 & g_2 & g_1 \\ & f_2 & f_1 & g_3 & g_2 \\ & & f_2 & & g_3 \end{bmatrix} = M^\intercal$$

on the basis $\{y_0^{e-1},y_0^{e-2}y_1,\ldots,y_0y_1^{e-2},y_1^{e-1}\}\cup\{y_0^{d-1},y_0^{d-2}y_1,\ldots,y_0y_1^{d-2},y_1^{d-1}\}$ of $V_{e-1}\oplus V_{d-1}$.

So because $\det M=0$, we see that $\det(\mu_f\oplus\mu_g)=0$, so $\mu_f\oplus\mu_g$ is singular as a linear transformation and therefore has nontrivial kernel. Thus, we can find a pair of polynomials $(\alpha,\beta)\in V_{e-1}\oplus V_{d-1}$ with $(\alpha,\beta)\neq(0,0)$ such that

$$\alpha(y_0,y_1)f(s,y_0,y_1)=\beta(y_0,y_1)g(s,y_0,y_1).$$

Without loss of generality, we will take $\beta \neq 0$ so that $\deg\beta = d-1$. Dividing out by y_1^{e+d-1} makes everything into a polynomial in $y := y_0/y_1$ as

$$\alpha(y,1)f(s,y,1) = \beta(y,1)g(s,y,1)$$

because all polynomials involved are homogeneous. Now, $f(s,y,1)$ will have d roots counted with multiplicity in k while $\beta(y,1)$ has $d-1$ roots counted with multiplicity in k (recall $\beta \neq 0$), so $f(s,y,1)$ is forced to share a root with $g(s,y,1)$. This root is our witness to $(s,(y:1)) \in X \times \mathbb{P}^1(k)$. ■

Remark 7.51. The above construction $\det M$ is called the resultant $\operatorname{res}(f,g)$; its main purpose is that $\operatorname{res}(f,g)$ vanishes if and only if f and g have a common root, which roughly follows from the argument given in the proof. For example, f has a double root if and only if it shares a root with f', which means we want to compute the discriminant $\operatorname{disc} f := \operatorname{res}(f,f')$.

7.4.3 Elimination Theory Proofs

There are two proofs of Theorem 7.47 in Eisenbud. The text of the chapter has an advanced proof which achieves more, but we do not have time for it. Instead, we will follow the proof presented in Exercise 14.1. Recall the statement.

Theorem 7.47. Fix an affine variety X over an algebraically closed field k and consider the natural projection map $\pi\colon X \times \mathbb{P}^n(k) \to X$ for some projective space $\mathbb{P}^n(k)$. Then, given a closed subset $Z \subseteq X \times \mathbb{P}^n(k)$, the image $\pi(Z)$ is also closed.

Proof of Theorem 7.47. We proceed directly. As suggested, we can define our subset $Z \subseteq X \times \mathbb{P}^n(k)$ as cut out by the equations

$$\begin{cases} f_1(s,y_0,\ldots,y_n) = 0, \\ \qquad\vdots \\ f_r(s,y_0,\ldots,y_n) = 0. \end{cases} \tag{3}$$

Here each of the equations f_i are homogeneous in the $y_\bullet$s. Now,

$$\pi(Z) = \{s \in X : (s,(y_0 : \ldots, y_n)) \in X \times \mathbb{P}^n(k)\},$$

so $\pi(Z)$ consists of the $s \in X$ for which there is a nonzero solution for the $y_\bullet$s in (3).

For now, imagine fixing some $s \in S$. If we look for all solutions $(y_0,\ldots,y_n) \in \mathbb{A}^{n+1}(k)$, we see that the equations in (3) cut out some ideal

$$I_s \subseteq k[y_0,\ldots,y_n].$$

Because I_s is generated by homogeneous polynomials (of positive degree by multiplying an equation f_i by $y_0\cdots y_n$ as necessary), the point $(0,\ldots,0)$ is certainly in $V(I_s)$, but we are hoping that $V(I_s)$ has some point outside $(0,\ldots,0)$. In particular, using the Nullstellensatz, we are hoping for

$$V(I_s) \neq \{(0,\ldots,0)\} \iff \operatorname{rad} I_s = I(V(I_s)) \neq I(V(\{(0,\ldots,0\})) = (y_0,\ldots,y_n)$$

by Theorem 3.88. Well, because we know that $V(I_s)$ at least contains $(0,\ldots,0)$, we get $I \subsetneq k[y_0,\ldots,y_s]$; as such, $\operatorname{rad} I_s = (y_0,\ldots,y_n)$ is equivalent to having $y_k^{e_k} \in I$ for some suitably large e_k for each e_k, which is equivalent to

$$(y_0,\ldots,y_n)^e \subseteq I$$

for some suitably large $e \in \mathbb{N}$.

We now let $s \in X$ vary again. Unraveling the above discussion, we see that

$$\pi(Z) = \left\{s \in S : I_s \not\supseteq (y_0,\ldots,y_n)^d \text{ for all } d \in \mathbb{N}\right\}.$$

For brevity, set $J := (y_0, \ldots, y_n)$ (note this is the irrelevant ideal of $k[y_0, \ldots, y_n]$) and define

$$X_e := \left\{s \in X : I_s \not\supseteq J^d\right\}$$

for $d \in \mathbb{N}$. It follows that

$$\pi(Z) = \bigcap_{d \geq 0} X_d,$$

so it now suffices to show that the X_d are Zariski closed (for sufficiently large d) and appeal to the topological fact that the intersection of closed sets is closed.

For concreteness, continue to let $s \in X$ vary somewhat, and let d_i be the degree of the $y_\bullet$ in equation f_i, and we will go ahead and suppose that $d > d_i$ for all i. To test $I_s \not\supseteq J^d$, we note that J^d is generated by the degree-d monomials in the $y_\bullet$. As such, we let

$$V_d \subseteq k[y_0, \ldots, y_n]$$

be the degree-d component as before, and we again recall that V_d has a basis given by the degree-d monomials in the $y_\bullet$, which are exactly the generators of J^d. Thus,

$$J^d \not\subseteq I_s \iff V_d \not\subseteq I_s.$$

Continuing to take cues from Exercise 7.50, we define the map

$$\begin{aligned} \mu_i \colon V_{d-d_i} &\to V_d \\ \alpha &\mapsto f\alpha \end{aligned}$$

which again is well-defined because f is homogeneous of degree d_i. Now, taking the direct sum of all the μ_i gives us a map

$$\begin{aligned} \mu \colon \bigoplus_{i=1}^r V_{d-d_i} &\to V_d, \\ (\alpha_i)_{i=1}^r &\mapsto \sum_{i=1}^r f_i\alpha_i. \end{aligned}$$

By the grading, we note that the image of μ is $I_s \cap J^d = (f_1, \ldots, f_r) \cap J^d$. So to make sure that I_s is avoiding V_d, we need to check that μ is not surjective.

Quickly, observe that, as in the case of Exercise 7.50, we can write out μ as some giant

$$\dim V_d \times \left(\sum_{i=1}^r \dim V_{d-d_i}\right)$$

matrix M in terms of the natural bases of V_{d-d_i} and V_d, though we will not do this explicitly; the point is that all the entries of this matrix are just the components of $f_i(s)$ and are therefore polynomials in s. We now claim that μ is not surjective if and only if all $(\dim V_d) \times (\dim V_d)$ minors of M vanish. This will finish because each of these minors vanishing cuts out a single polynomial equation in X and will thus show that X_d is an affine set.

- Well, in one direction, if μ is not surjective, then all its columns need to lie in some subspace of dimension strictly smaller than $\dim V_d$. As such, any $(\dim V_d) \times (\dim V_d)$ minor—which consists entirely of column vectors of M—must vanish because the column vectors are forced to have a linear dependence.

- Conversely, if μ is surjective, then its columns contain a spanning set and hence contain a basis for V_d, which means any $(\dim V_d) \times (\dim V_d)$ consisting exactly of these $\dim V_d$ column vectors must vanish.

The above equivalence shows that X_d can be cut out by polynomial equations (namely, the minors of M) and therefore is closed. This finishes the proof. ■

Remark 7.52. Annoyingly, this proof is non-constructive (in the equations to cut out the variety $\pi(Z)$) because we took an infinite intersection of these closed sets to show that our set was closed. The exercises we did above were more constructive but not generalizable. Such is life.

Roughly speaking, we are kind of saying that projective space is compact, in the sense that the image is closed, and compact sets are approximately the only ones which stay compact/closed through a continuous map.[2] More precisely,

Corollary 7.53. The image of a projective variety through a map $\varphi\colon Y\to X$ is closed.

Proof. We use Theorem 7.47. Place $Y\subseteq\mathbb{P}^m(k)$ and $X\subseteq\mathbb{P}^n(k)$. By embedding our spaces in a sufficiently large projective space, we may assume that $m=n$; namely, if $n\le m$, then extend φ by the embedding $\mathbb{P}^n(k)\hookrightarrow\mathbb{P}^m(k)$ by $(a_0:\ldots:a_n)\mapsto(a_0:\ldots:a_n:1:1:\ldots:a)$. Otherwise, if $m<n$, then we can just extend φ to do nothing with the extra coordinates granted by $\mathbb{P}^n(k)$, and X is still a closed subspace of $\mathbb{P}^n(k)$ under the embedding $\mathbb{P}^m(k)\hookrightarrow\mathbb{P}^n(k)$ while $\operatorname{im}\varphi$ remains unchanged.

Now, the point is to be able to consider the "graph"

$$Z\coloneqq\{(x,y)\in X\times\mathbb{P}^n(k):y\in Y,\,x=\varphi(y)\}.$$

Note that the direction of the coordinates is reversed so that we can project onto the first coordinate later on to get $\operatorname{im}\varphi$. As such, we proceed in steps.

1. Note that $X\times X\subseteq\mathbb{P}^n(k)\times\mathbb{P}^n(k)$ is closed: if X is cut out by some homogeneous polynomials $\{f_1,\ldots,f_r\}$, then $X\times X$ is cut out by the polynomials

$$\{f_1(x_0,\ldots,x_n),\ldots,f_r(x_0,\ldots,x_n)\}\cup\{f_1(y_0,\ldots,y_n),\ldots,f_r(y_0,\ldots,y_n)\}.$$

   Explicitly, $(a,b)\in X\times X$ if and only if $a\in X$ and $b\in X$ if and only if a satisfies the equations $\{f_1(x_0,\ldots,x_n),\ldots,f_r(x_0,\ldots,x_n)\}$ and b satisfies the equations $\{f_1(y_0,\ldots,y_n),\ldots,f_r(y_0,\ldots,y_n)\}$.

2. Further, we see that

$$\Delta_{\mathbb{P}^n(k)}\coloneqq\{(x,x):x\in\mathbb{P}^n(k)\}$$

   is also closed. Explicitly, we can be cut out as a projective variety from $\mathbb{P}^{2n}(k)$ by the homogeneous equations

$$x_iy_j-x_jy_i=0.$$

   Namely, certainly any element $(a,b)\in\Delta_{\mathbb{P}^n(k)}$ does indeed satisfy all the above equations because we can write $a=\lambda b$ for some $\lambda\in k^\times$, which causes all the above equations to vanish as needed.

   Conversely, if a pair of nonzero points $((a_0,\ldots,a_n),(b_0,\ldots,b_n))$ satisfies the given equations, then suppose without loss of generality that a_0 and b_0 are nonzero. Then the equations

$$a_ib_0-a_0b_i=0$$

   forces $b_i=(b_0/a_0)b_i$, so $\lambda\coloneqq b_0/a_0\in k^\times$ gives $(b_0,\ldots,b_n)=\lambda(a_0,\ldots,a_n)$, meaning our point does live in $\Delta_{\mathbb{P}^n(k)}$.

3. Next, we note that

$$\Delta_X\coloneqq(X\times X)\cap\Delta_{\mathbb{P}^n(k)}=\{(a,b):a,b\in X\text{ and }a=b\}=\{(a,a):a\in X\}$$

   is closed as the intersection of closed sets. It follows that Δ_X is also a closed set in $X\times X$.

[2] The Zariski topology is not Hausdorff, but this is fine.

4. Now, $(\mathrm{id}_X \times \varphi)\colon X \times \mathbb{P}^n(k) \to X \times X$ is a continuous map as the product of continuous maps, so
$$\begin{aligned}(\mathrm{id}_X \times \varphi)^{-1}(\Delta_X) &= \{(a,b) \in X \times \mathbb{P}^n(k) : a = \mathrm{id}_X\, x \text{ and } b = \varphi(x) \text{ for some } x \in X\} \\ &= \{(a,b) \in X \times \mathbb{P}^n(k) : b = \varphi(a)\} \\ &= Z\end{aligned}$$
is also closed, as the pre-image of a closed set through a continuous map.
5. Now, we may project Z down to the X coordinate to recover
$$\{x \in X : x = \varphi(y) \text{ for some } y \in Y\} = \operatorname{im} \varphi,$$
which by Theorem 7.47 is also Zariski closed in X.

The last step finishes the proof. ■

Let's see an example of the above.

Example 7.54. We embed $\mathbb{P}^1(k) \to \mathbb{P}^2(k)$ by
$$(s : t) \mapsto \left(s^3 : s^2t + st^2 : t^3\right).$$
This should have closed image in $\mathbb{P}^2(k)$, and indeed we can see that the image is cut out by the equation
$$y^3 - x^2z - xz^2 - 3xyz = 0,$$
which we can see by direct expansion.

Remark 7.55. The final exam might ask us to do something like the above computations.

7.4.4 Speed Run

The following speed-run will not show up on the final, but it is fun. So let's talk about dimension theory.

To continue our geometric story, we as usual fix some morphism of affine varieties $\varphi\colon X \to Y$. One might ask what we can see about the image. The image is allowed to be open (as in Exercise 7.48), but we can say more. We have the following definition.

Definition 7.56 (Locally closed)**.** An affine set X is *locally closed* if and only if it is the intersection a Zariski closed and a Zariski open set.

Definition 7.57 (Constructible)**.** An affine set X is *constructible* if and only if it is a finite union of locally closed sets.

And here is our theorem.

Theorem 7.58 (Chevalley)**.** Fix a ring homomorphism $\varphi\colon R \to S$ so that S is finite over R. Define
$$X(\varphi) := \left\{\varphi^{-1}\mathfrak{q} : \mathfrak{q} \in \operatorname{Spec} S\right\}$$
to be the image of φ. Then $X(\varphi)$ is constructible.

We can even be a little sharper as to how our fibers behave. To review, given a maximal point $\mathfrak{p} \in \operatorname{Spec} R$, we note that
$$K(R/\mathfrak{p}) \otimes_R S$$
is the ring of functions on the fiber $\varphi^{-1}\mathfrak{p}$. One has to be careful that the fiber might not be a variety meaning that $K(R/\mathfrak{p}) \otimes_R S$ need not be a domain. Regardless, we have the following.

Theorem 7.59. Fix a ring homomorphism $\varphi\colon R \to S$ so that S is finite over R. Then the map

$$\mathfrak{p} \in \operatorname{Spec} R \longmapsto \dim K(R/\mathfrak{p}) \otimes_R S$$

is semicontinuous. If in fact S is graded as an R-algebra by $R = S_0$, then the set of points of R with points of dimension greater than d is closed.

The above result can actually recover Theorem 7.47.

7.5 May 3

Today we will review.

7.5.1 Flat and Projective Modules

Recall the following equivalent conditions for an R-module M to be flat.

- $N \hookrightarrow N'$ remains an injection as $M \otimes_R N \hookrightarrow M \otimes_R N'$.
- $\operatorname{Tor}_1^R(M, -)$ vanishes.
- $\operatorname{Tor}_1^R(M, R/I)$ vanishes for any finitely generated ideal I.

Here are some equivalent conditions for an R-module M to be projective.

- $\operatorname{Hom}_R(M, -)$ is exact.
- There is some N for which $M \oplus N$ is free.

One way to see that a projective module is to flat is to note that $\operatorname{Tor}_1^R(M, -)$ vanishes easily because the (augmented) projective resolution for M is simply

$$\cdots \to 0 \to 0 \to M \to 0.$$

Other examples are flat modules tend to be localizations or tensor products of such things. For example, $\mathbb{Q}$ is a flat but not projective module. It does turn out that finitely presented flat modules are projective, which one can see because in this case both flat and projective are the same as being locally free.

7.5.2 Invertible Modules

Invertible modules are finitely generated modules which are locally isomorphic to $R_\mathfrak{p}$ (namely, upon localizing at a prime $\mathfrak{p}$). For example, take $R \coloneqq \mathbb{Z}[\sqrt{-5}]$. Then the invertible modules are the fractional ideals of $\mathbb{Q}(\sqrt{-5})$, which generate $C(R)$.

Notably, $\mathbb{Z}[\sqrt{-5}]$ is normal (it's the normal closure of $\mathbb{Z}$) and of dimension 1 (it's integral over the one-dimensional ring $\mathbb{Z}$), so R is a Dedekind domain. Thus, all nonzero ideals are invertible, and there is unique prime factorization of invertible ideals, so our invertible ideals in $C(R)$ are freely generated by our prime ideals.

However, $\mathbb{Z}[\sqrt{-5}]$ is not a principal ideal domain because it is not a unique factorization domain, as witnessed by

$$\left(1 + \sqrt{-5}\right)\left(1 - \sqrt{-5}\right) = 2 \cdot 3.$$

For example, this means that the Picard group $\operatorname{Pic} R$ is nontrivial.

As another example, take $R \coloneqq \mathbb{Z}[\sqrt{5}]$. This ring is not normal, so we might be able to find an ideal which is not invertible. For example, we can see that the kernel of the map

$$\mathbb{Z}[\sqrt{5}] \to \mathbb{Z}/2\mathbb{Z}$$

by taking $\sqrt{5} \mapsto 1$ is $I := (2, 1+\sqrt{5})$. As such, we conclude that I is a maximal ideal. To see that I is invertible, we proceed by the definitions: if we localize at an ideal $\mathfrak{p}$ away from I, then we will get $I_\mathfrak{p} = R_\mathfrak{p}$ set-theoretically because I will have an element outside $\mathfrak{p}$.

Lastly, with $\mathfrak{p} = I$, we need to show that I_I is not principal, for which we check instead that

$$\dim_{R_I/I_I} I_I/I_I^2 \neq 1.$$

Now, $R/I \cong \mathbb{F}_2$, so $R_I/I_I \cong \mathbb{F}_2$ still. Well, we compute

$$I^2 = \left(4, 2+2\sqrt{5}, 6+2\sqrt{5}\right) = \left(4, 2+2\sqrt{5}\right).$$

Then I/I^2 will have the elements 2 and $1+\sqrt{5}$ remaining linearly independent, so we are done.

Remark 7.60. Back in $\mathbb{Z}[\sqrt{-5}]$, the ideal $\mathfrak{p} := (2, 1+\sqrt{-5})$ is still invertible. The difference is that $\mathfrak{p}_\mathfrak{p}$ is now still principal, generated by $1+\sqrt{-5}$ because the other generator has

$$(1+\sqrt{-5}) \cdot \frac{1-\sqrt{-5}}{3} = 2.$$

7.5.3 Grassmannian

Let's do an example of a projective variety: Grassmannians $\mathrm{Gr}(p, n)$.

Definition 7.61 (Grassmannian)**.** Set k be an algebraically closed field. The space $\mathrm{Gr}(p, n)$ consists of the p-dimensional subspaces of k^n.

Example 7.62. Recall

$$\mathbb{P}^{n-1} = \mathrm{Gr}(1, n),$$

meaning that $\mathbb{P}^{n-1}$ is made up of the 1-dimensional subspaces of k^n.

We would like to show that Grassmannians are projective varieties.

Exercise 7.63. Set $X := \mathrm{Gr}(2, 4)$. We show X is projective and compute $\dim X$.

Proof. We are looking at planes in k^4. For concreteness, give k^4 the standard basis $\{e_1, e_2, e_3, e_4\}$. As such, we can enumerate planes $V \subseteq k^4$ by their basis

$$\begin{bmatrix} a_1 \\ a_2 \\ a_3 \\ a_4 \end{bmatrix} \qquad \text{and} \qquad \begin{bmatrix} b_1 \\ b_2 \\ b_3 \\ b_4 \end{bmatrix}.$$

We glue these together into matrices

$$M := \begin{bmatrix} a_1 & b_1 \\ a_2 & b_2 \\ a_3 & b_3 \\ a_4 & b_4 \end{bmatrix}.$$

Of course, for this to make a plane, we need the matrix to have full rank, which means that there is no nontrivial relation among the columns; this cuts out a Zariski open set from k^8. Let $M_0(k)$ be the set of all such matrices.

Of course, it is possible for two matrices $M, M' \in M_0(k)$ to generate the same plane, which will happen whenever there is a way to make the columns of M' as a linear combination from the columns of M. Equivalently, we are asking for a matrix $A \in \mathrm{GL}_2(k)$ such that

$$M' = MA.$$

In general, there is a $\mathrm{GL}_2(k)$-action on $M_0(k)$, so our planes can be nicely parameterized as elements of $X = M_0(k)/\mathrm{GL}_2(k)$.

To make X projective, we set

$$p_{ij} = \deg \begin{bmatrix} a_i & b_i \\ a_j & b_j \end{bmatrix}$$

using the coordinates for M above. Of course, scaling M merely changes the p_{ij} but does not change the plane (and the condition that our matrices have full rank means that at least one of the p_{ij} is nonzero), so we can be assured a well-defined map

$$X \to \mathbb{P}^5(k)$$

by mapping to our coordinates $(p_{12} : p_{13} : p_{14} : p_{23} : p_{24} : p_{34})$. We now turn to computing the dimension of X.

For example, suppose $p_{12} \neq 0$. After doing some shifting via our $\mathrm{GL}_2(k)$-action, we may assume that we have a matrix of the form

$$\begin{bmatrix} 1 & 0 \\ 0 & 1 \\ x_1 & y_1 \\ x_2 & y_2 \end{bmatrix}.$$

In particular, localizing our space X at $p_{12} = 1$, we will simply get $\mathbb{A}^2(k)$ for the bottom four coordinates.

Running the above argument through for all coordinates p_{ij}, we have covered X with six copies of $\mathbb{A}^4(k)$, so X is a four-dimensional projective variety.

Remark 7.64. In general, $\dim \mathrm{Gr}(p, n) = p(n - p)$.

We now turn to writing down equations for X. We start by noting that

$$p_{12}p_{34} - p_{13}p_{24} + p_{14}p_{23} = 0 \tag{$*$}$$

essentially by directly expanding the definition of the p_{ij}. A vaguely smarter way is to optimize our computation by using our affine charts of $\mathbb{A}^4(k)$.

It remains to see that $(*)$ is our only equation. Well, we construct our matrix backwards by hand. Without loss of generality, take $p_{12} = 1$ (after some scaling and rearranging), and we just use the matrix

$$\begin{bmatrix} 1 & 0 \\ 0 & 1 \\ -p_{23} & p_{13} \\ -p_{24} & p_{14} \end{bmatrix}.$$

So indeed, $(*)$ is sharp enough to cut out X. ■

Remark 7.65. In general, the Grassmannians are all quadratic varieties.

7.5.4 The Associated Graded Ring

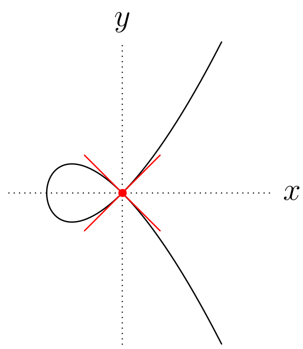
Recall the associated graded ring

$$\mathrm{gr}_I R := \bigoplus_{n \geq 0} I^n / I^{n+1}.$$

Geometrically, we might imagine R is an affine domain and I a maximal ideal; then $\mathrm{gr}_I R$ is the ring of functions on the tangent cone.

Exercise 7.66. We work out the tangent cone for $y^2 = x^2(x+1)$ at $(0,0)$.

Proof. Here is our image.



We expect the tangent cone to be the union of the two lines $y = x$ and $y = -x$.

On the algebraic side, we are setting

$$R := \frac{k[x,y]}{(y^2 - x^2(x+1))} \qquad \text{and} \qquad \mathfrak{m} = (x,y),$$

and we want to study $\operatorname{gr}_{\mathfrak{m}} R$. To begin, we note that R is not normal because $t := y/x$ satisfies the monic polynomial

$$t^2 - (x+1) = 0.$$

As such, our normalization will have to include t; concretely, our normalization map takes

$$x \mapsto t^2 - 1 \qquad \text{and} \qquad y \mapsto t\left(t^2-1\right),$$

which will turn out to embed $R \hookrightarrow k[t]$, with $R \cong k\left[t^2-1, t^3-t\right]$. In particular,

$$\mathfrak{m} = \left(t^2-1, t^3-t\right)$$

under this embedding, so t^2-1 and t^3-t will generate $\mathfrak{m}/\mathfrak{m}^2$. However, multiplying these two generators together will kill them in $\mathfrak{m}^2/\mathfrak{m}^3$, so we see

$$\operatorname{gr}_{\mathfrak{m}} R \cong k[z,w]/(zw)$$

after a little reparameterization. The $z = 0$ and $w = 0$ correspond to $t = 1$ and $t = -1$, which are our tangent cone lines $y = \pm x$. ■

7.5.5 Open Maps

As a last remark to close out class, we do a little more algebraic geometry.

Theorem 7.67. Suppose $\varphi\colon X \to Y$ is a map of affine varieties, and suppose accordingly that $A(Y)$ is normal and that $A(X)$ is integral over $A(Y)$ by the map

$$\varphi^*\colon A(Y) \to A(X).$$

In this case φ is an open map.

Proof. Let $U \subseteq X$ be Zariski open so that $U = X \setminus V(f)$ for some element $f \in A(X)$. We need to show that

$$Y \setminus \varphi(U) = Y \setminus Z(f)$$

is closed in Y. Translating this into algebra, we are asking which maximal ideals $\mathfrak{m} \subseteq A(Y)$ to contain f so that this localization goes through correctly.

We leave the rest of the proof as an exercise; the main idea is that f satisfies a monic polynomial in elements of $\operatorname{im} \varphi^*$, so we should show that $Y \setminus \varphi(U)$ is given by the ideal generated by the coefficients of this monic polynomial. Then we use the geometric $AKLB$ set-up. ■

Remark 7.68. The final is expected to emphasize dimension theory (but not exclusively dimension theory). It will be about 8 problems.

List of Definitions