250B: Commutative Algebra
Or, Eisenbud With Details

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 $r_1, \dots, r_n \in R$ such that $I = (r_1, \dots, r_n)$.

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.

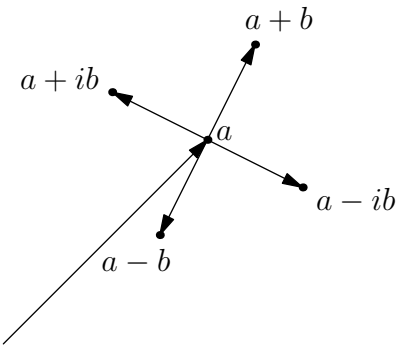
Lemma 1.34. The ring $\mathbb{Z}[i]$ is Euclidean, where our norm is $\mathrm{N}(a + bi) := a^2 + b^2$. In other words, given $\alpha, \beta \in \mathbb{Z}[i]$, we need to show that there exists $q \in \mathbb{Z}[i]$ such that

$$a = bq + r$$

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 $|\beta| \leq |\alpha|$, 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

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

  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

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

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

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

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 $R[x_1, \dots, x_n]$, 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 $k[x_1, \dots, x_n]$ 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 $k[x_1, \dots, x_n]^G$?

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

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 $R^G = k[x_1, \dots, x_n]^G$ 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 $\deg \varphi(f) \leq \deg f$.

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

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

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.

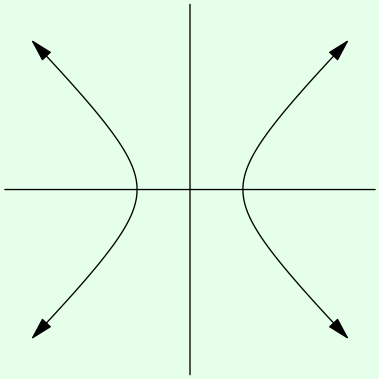
Definition 1.62 (Algebraic)**.** A subset $X \subseteq \mathbb{A}^n(k)$ is (affine) *algebraic* if and only if it is the set of solutions to some system of polynomials equations $f_1, \ldots, f_n \in k[x_1, \ldots, x_d]$.

[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 $I \subseteq k[x_1, \dots, x_n]$, 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 $(x^2 + 1)$ 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 $S \subseteq k[x_1, \dots, x_n]$ 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 $k[x_1, \dots, x_n]$, 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 $Z(S_1), \dots, Z(S_n)$, 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 $k[x_1, \dots, x_n]$ 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 $k[x_1, \dots, x_n]$ 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 $k[x_1, \dots, x_n]$. 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 $1 \le i \le N$ 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 $1 \in \operatorname{rad}(f_1, \dots, f_r)$. Then it follows $1 = 1^n \in (f_1, \dots, f_r)$ for some positive integer n, so there exists $p_1, \dots, p_r \in k[x_1, \dots, x_n]$ 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 $a = (a_1, \dots, a_n) \in \mathbb{A}^n(k)$ makes a closed set corresponding to the ideal

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

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

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

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

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 $a = (a_1, \dots, a_n) \in X$ are in bijection with maximal ideals $\mathfrak{m}_a \subseteq A(X)$ by

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

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

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

Proof. By the Nullstellensatz,

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

so $1 \in I$ follows. ■

Now, we have already shown that $I(\{a\}) = (x_1 - a_1, \dots, x_n - a_n)$. 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 $I(\{a\})/I(X) = (x_1 - a_1, \dots, x_n - a_n)/I(X)$.

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

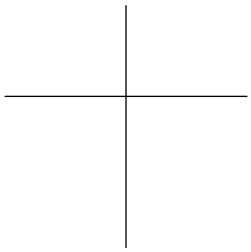
$$(a_0 : a_1 : \ldots : a_n) \in \mathbb{P}^n(k)$$

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 $k[x_0, \ldots, x_n]$.

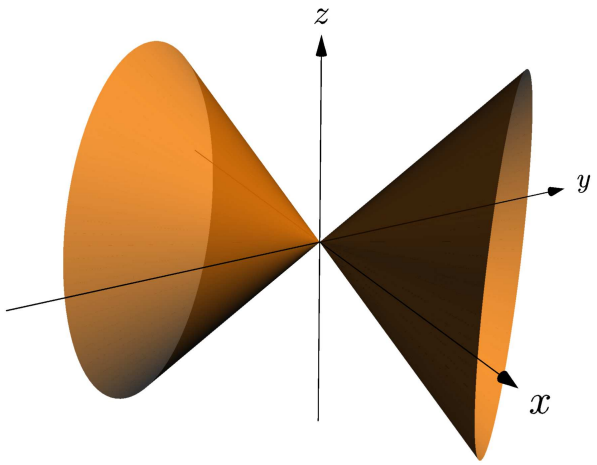
Here is an example.

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 $R_i R_j \subseteq R_{i+j}$ 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 $R_i M_j \subseteq M_{i+j}$ for any $i \in \mathbb{N}$ and $j \in \mathbb{Z}$.

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

Proposition 1.103. 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

$$I := R_1 \oplus R_2 \oplus \cdots$$

is finitely generated over R, so fix $I := (r_1, \dots, r_N)$. We claim that

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

For $\supseteq$, there is nothing to say. For $\subseteq$, pick up some $f \in R$, and we show that $f \in R_0[r_1, \dots, r_N]$. 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 $f \in R_0 \subseteq R_0[r_1, \dots, r_N]$ and are done immediately. So take $d > 0$. Then $f \in I = (r_1, \dots, r_N)$, so we may write

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

for some $g_1, \dots, g_N \in R$. 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, $g_i \in R_0[r_1, \dots, r_N]$, and $f \in R_0[r_1, \dots, r_N]$ by the decomposition of f in I. This finishes the proof. ∎

1.2.8 The Hilbert Function

For this subsection, let $R := k[x_0, \dots, x_n]$ (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

$$M'_d := \bigoplus_{e \geq d} M_e \subseteq M$$

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

$$H_M(d) := \dim_k M_d.$$

Exercise 1.105. Let $M = R = k[x_0, \dots, x_n]$; 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 $k[x_0, \dots, x_n]$. Thus, we are counting tuples $(a_0, \dots, a_n)$ 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 $(a_0, \dots, a_n)$, 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 1.106. Let M be a finitely generated graded module over the ring $R := k[x_0, \dots, x_n]$, 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 1.107 (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 $k[x_0, \dots, x_n]$ implies that $M/x_n M$ will be finitely generated over $k[x_0, \dots, x_{n-1}]$ 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 $M/x_r M$ is in fact a graded module by

$$\frac{M}{x_n M} \cong \frac{\bigoplus_{d \in \mathbb{Z}} M_d}{\bigoplus_{d \in \mathbb{Z}} x_n M_d} = \frac{\bigoplus_{d \in \mathbb{Z}} M_d}{\bigoplus_{d \in \mathbb{Z}} x_n M_{d-1}} \cong \bigoplus_{d \in \mathbb{Z}} \frac{M_d}{x_n M_{d-1}},$$

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 $M \xrightarrow{x_n}$, 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

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

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 $M(-1) \xrightarrow{x_n} M$ multiplication by x_n, and we get to write

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

We take a moment to recognize $K(-1) \subseteq M(-1)$ is finitely generated over $k[x_0, \dots, x_n]$ 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 $k[x_0, \dots, x_{n-1}]$.

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 1.108 (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 1.106 justifies the following definition.

Definition 1.109 (Hilbert polynomial)**.** Let M be a finitely generated graded module over the ring $R := k[x_0, \dots, x_n]$, where R is graded by degree. The polynomial promised by Theorem 1.106 is called the *Hilbert polynomial* of M.

Remark 1.110. 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 1.111. 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 $finik[x, y, z]$ 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 $\left(x^2 + y^2 + z^2\right)$, 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

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

Note the first map is well-defined because $\left(x^2+y^2+z^2\right) R_{d-2} \subseteq R_2 R_{d-2} \subseteq R_d$. In fact, we claim that $\left(x^2+y^2+z^2\right) R_{d-2} = I \cap R_d$, for any $f \in I \cap R_d$ has $f(x,y,z)/\left(x^2+y^2+z^2\right)$ 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 1.105 is $\binom{n+2}{2} - \binom{n}{2} = \frac{n^2+3n+2}{2} - \frac{n^2-n}{2} = 2n+1$. ■

Remark 1.112. Continuing with the previous remark, we see the degree of the Hilbert polynomial of M above is 1, so the associated projective variety $Z\left(x^2+y^2+z^2\right)$ 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 1.113 (Eisenbud 1.19)**.** Define $M := k[x,y,z]/\left(xz - y^2, yx - z^2, xw - yz\right)$ as an $R := k[x,y,z]$-module. We compute the Hilbert function for M.

Proof. We outline. For brevity, we set $I := \left(xz - y^2, yx - z^2, xw - yz\right)$. 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

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

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 $U = R\backslash\{0\}$ 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.

$$\begin{array}{ccc} R & \xrightarrow{\varphi} & R\left[U^{-1}\right] \\ & \searrow^{\psi} & \downarrow{\scriptstyle \gamma} \\ & & S \end{array}$$

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

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

Now we claim that

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

as an $R\left[U^{-1}\right]$-ideal. Certainly $(x_1/1, \dots, x_n/1) \subseteq I$. 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

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

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 $\mathrm{Hom}_R(M,N)$ to be the abelian group of R-module homomorphisms $M \to N$.

In fact, we can endow $\mathrm{Hom}_R(M,N)$ 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 $\mathrm{End}_R(M) := \mathrm{Hom}_R(M,M)$.

Note that $\mathrm{End}_R(M)$ 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 $\mathrm{Hom}_R(R,M) \cong M$ 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 $\mathrm{Hom}_R(M_1,N_1) \to \mathrm{Hom}_R(M_2,N_2)$ by $\varphi \mapsto \beta \circ \varphi \circ \alpha$. In fact, this is an R-module homomorphism.

3. We have that
$$\mathrm{Hom}_R\left(\bigoplus_{\alpha\in I} M_\alpha, N\right) \cong \prod_{\alpha\in I} \mathrm{Hom}_R(M_\alpha, N)$$
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
$$0 \to \mathrm{Hom}_R(M,A) \to \mathrm{Hom}_R(M,B) \to \mathrm{Hom}_R(M,C).$$
Similarly,
$$0 \to \mathrm{Hom}_R(C,M) \to \mathrm{Hom}_R(B,M) \to \mathrm{Hom}_R(A,M)$$
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 $\mathrm{Hom}_R(M,C)$ might not be extendable to a map $\mathrm{Hom}_R(M,B)$. 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 $\mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}/2\mathbb{Z}, -)$ 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 $\mathrm{Hom}_R(R,M) \cong M$ is functorial as follows: given $\varphi : M \to N$, the following diagram commutes.

$$\begin{array}{ccc} \mathrm{Hom}_R(R,M) & \xrightarrow{\varphi} & \mathrm{Hom}_R(R,M) \\ \cong\downarrow & & \downarrow\cong \\ M & \xrightarrow{\varphi} & N \end{array}$$

Here the map $\varphi : \mathrm{Hom}_R(R,M) \to \mathrm{Hom}_R(R,N)$ is by $f \mapsto \varphi \circ f$. To see that this diagram commutes, note that some $f \in \mathrm{Hom}_R(R,M)$ 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

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

and

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

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

$$(a_1 m_1 + a_2 m_2) \otimes (b_1 n_1 + b_2 n_2) = a_1 b_1 (m_1 \otimes n_1) + a_1 b_2 (m_1 \otimes n_2) + a_2 b_1 (m_2 \otimes n_1) + a_2 b_2 (m_2 \otimes n_2).$$

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.
$$\begin{array}{ccc} M & \xrightarrow{\varphi} & N \\ \cong\downarrow & & \downarrow\cong \\ R \otimes_R M & \xrightarrow[\varphi]{} & R \otimes_R N \end{array}$$
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
$$\mathbb{Z} \xrightarrow{\times a} \mathbb{Z} \to \mathbb{Z}/a\mathbb{Z} \to 0$$
by $\mathbb{Z}/b\mathbb{Z}$ gives the right-exact sequence
$$\mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Z}/b\mathbb{Z} \xrightarrow{\times a} \mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Z}/b\mathbb{Z} \to \mathbb{Z}/a\mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Z}/b\mathbb{Z} \to 0.$$
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
$$\mathbb{Z}/b\mathbb{Z} \xrightarrow{\times a} \mathbb{Z}/b\mathbb{Z} \to \mathbb{Z}/a\mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Z}/b\mathbb{Z} \to 0.$$
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

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

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

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

However, the map $\xrightarrow{\times 2}$ 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

$$V \cong \bigoplus_{\alpha \in I} kv_\alpha \qquad \text{and} \qquad W \cong \bigoplus_{\beta \in J} kw_\beta,$$

so the above facts let us write

$$V \otimes_k W \cong \bigoplus_{\alpha \in I, \beta \in J} (kv_\alpha \otimes_k kw_\beta).$$

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 $M \otimes_R - : \mathrm{Mod}_R \to \mathrm{Mod}_R$ 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

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

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

$$\begin{array}{ccccccc}
\mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Z}/n\mathbb{Z} & \xrightarrow{\times n} & \mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Z}/n\mathbb{Z} & \longrightarrow & \mathbb{Z}/n\mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Z}/n\mathbb{Z} & \longrightarrow & 0 \\
\downarrow & & \downarrow & & \downarrow & & \\
\mathbb{Z}/n\mathbb{Z} & \xrightarrow{f} & \mathbb{Z}/n\mathbb{Z} & \longrightarrow & \mathbb{Z}/n\mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Z}/n\mathbb{Z} & \longrightarrow & 0
\end{array}$$

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 $m \mapsto 1 \otimes m$.

$$\begin{array}{ccc}
A & \longrightarrow & B \\
\downarrow & & \downarrow \\
R \otimes_R A & \longrightarrow & R \otimes_R B
\end{array}$$

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.

$$\begin{array}{ccc}
R^n \otimes_R A & \longrightarrow & R^n \otimes_R B \\
\downarrow & & \downarrow \\
(R \otimes_R A)^n & \longrightarrow & (R \otimes_R B)^n
\end{array}$$

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-bilinaerity, 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.

$$\begin{array}{ccc} R\left[U^{-1}\right] \otimes_R A & \longrightarrow & R\left[U^{-1}\right] \otimes_R B \\ \downarrow & & \downarrow \\ A\left[U^{-1}\right] & \longrightarrow & B\left[U^{-1}\right] \end{array}$$

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

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

where in $\overset{*}{\cong}$ 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.)

$$\begin{array}{ccccccccc} 0 & \longrightarrow & A\left[U^{-1}\right] & \longrightarrow & B\left[U^{-1}\right] & \longrightarrow & C\left[U^{-1}\right] & \longrightarrow & 0 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 0 & \longrightarrow & R\left[U^{-1}\right] \otimes_R A & \longrightarrow & R\left[U^{-1}\right] \otimes_R B & \longrightarrow & R\left[U^{-1}\right] \otimes_R C & \longrightarrow & 0 \end{array}$$

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 $M_1, \dots, M_n \subseteq M$ 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

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

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 $\frac{1}{u}[x]_{M_i} \mapsto \left[\frac{x}{u}\right]_{M_i[U^{-1}]}$. 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 $\mathrm{Res}^S_R(f) : \mathrm{Res}^R_S M \to \mathrm{Res}^R_S N$. In other words, we define

$$\mathrm{Res}^S_R(f)(m) := f(m).$$

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

$$\mathrm{Res}^S_R(f)(rm) f(\psi(r)m) = \psi(r)f(m) = r \cdot \mathrm{Res}^S_R(f)(m).$$

Now, to show functoriality, we note that $\mathrm{Res}^S_R(\mathrm{id}_M)(m) = m$ 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 $\mathrm{Res}^S_R(g \circ f)(a) = (g \circ f)(a) = \left(\mathrm{Res}^S_R(g) \circ \mathrm{Res}^S_R(g)\right)(a)$. ∎

In the other direction, if M is an R-module, we can create an S-module the "induced" module $\mathrm{Ind}^S_R M := S \otimes_R M$, 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)

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

Proof. We construct forwards and backwards maps manually.

- Fix $f \in \mathrm{Hom}_R(M, \mathrm{Res}^S_R N)$. Then we define $\widetilde{f} \in \mathrm{Hom}_S(S \otimes_R M, N)$ 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 $m \in M$,

    $$\widetilde{f}(r_1 s_1 + r_2 s_2, m) = (r_1 s_1 + r_2 s_2) f(m) = r_1 \widetilde{f}(s_1, m) + r_2 \widetilde{f}(s_2, m).$$

    Given $s \in S$ and $r_1, r_2 \in R$ and $m \in M$,

    $$\widetilde{f}(s, r_1 m_1 + r_2 m_2) = sf(r_1 m_1 + r_2 m_2) = r_1 \widetilde{f}(s, m_1) + r_2 \widetilde{f}(s, m_2).$$

    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 $f, g \in \mathrm{Hom}_R(M, \mathrm{Res}^S_R N)$ 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 $f \in \mathrm{Hom}_R(M, \mathrm{Res}^S_R N)$ 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 $g \in \mathrm{Hom}_S(S \otimes_R M, N)$. 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 $\mathrm{Hom}_S(S \otimes_R M, N)$ to $\mathrm{Hom}_R(M, \mathrm{Res}^S_R N)$.

Note that it merely remains to check the surjectivity of $f \mapsto \widetilde{f}$, so it suffices to show that, for any $g \in \mathrm{Hom}_S(S \otimes_R M, N)$, 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
$$S \otimes_R \mathrm{Hom}_R(M, N) \qquad \text{and} \qquad \mathrm{Hom}_S(S \otimes_R M, S \otimes_R N),$$
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
$$\alpha : S \otimes_R \mathrm{Hom}_R(M, N) \to \mathrm{Hom}_S(S \otimes_R M, S \otimes_R N).$$

Proof. The main idea is to use Proposition 2.59. To begin with, note that there is a function
$$\gamma : \mathrm{Hom}_R(M, N) \to \mathrm{Hom}_S(S \otimes_R M, S \otimes_R N)$$
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
$$\gamma : \mathrm{Hom}_R(M, N) \to \mathrm{Res}^S_R \mathrm{Hom}_S(S \otimes_R M, S \otimes_R N)$$

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 $f_1, f_2 \in \mathrm{Hom}_R(M,N)$ with $s \otimes m \in S \otimes_R M$, and we see

$$\gamma(r_1 f_1 + r_2 f_2)(s \otimes m) = s \otimes (r_1 f_1 + r_2 f_2)(m) = r_1(s \otimes f_1(m)) + r_2(s \otimes f_2(m)) = \big(r_1\gamma(f_1) + r_2\gamma(f_2)\big)(s \otimes m).$$

Now, because γ is an R-module map, Proposition 2.59 promises a canonical map

$$\widetilde{\gamma} : S \otimes_R \mathrm{Hom}_R(M,N) \to \mathrm{Hom}(S \otimes_R M, S \otimes_R N).$$

In fact, we can compute $\widetilde{\gamma}$ by tracking Proposition 2.59 and γ through. Given $s \otimes f \in S \otimes_R \mathrm{Hom}_R(M,N)$ 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.

$$\begin{array}{ccc} S \otimes_R \mathrm{Hom}_R(M',N) & \xrightarrow{\alpha} & \mathrm{Hom}_S(S \otimes_R M', S \otimes_R N) \\ \downarrow{\scriptstyle \varphi} & & \downarrow{\scriptstyle \varphi} \\ S \otimes_R \mathrm{Hom}_R(M,N) & \xrightarrow[\alpha]{} & \mathrm{Hom}_S(S \otimes_R M, S \otimes_R N) \end{array}$$

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 $S \otimes_R \mathrm{Hom}_R(R^n, N) \cong \mathrm{Hom}_S(S \otimes_R R^n, S \otimes_R N)$, and tracking the isomorphism through will reveal that it is α. Pick up some $s \otimes f \in S \otimes_R \mathrm{Hom}_R(R^n, N)$ which we will track through.

- Note that $S \otimes_R \mathrm{Hom}_R(R^n, N) \cong S \otimes_R \mathrm{Hom}_R(R, N)^n \cong S \otimes_R N^n$ 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 $(S \otimes_R N)^n \cong \mathrm{Hom}_S(S^n, S \otimes_R N)$ by sending $(s \otimes f(e_k))_{k=1}^n$ to the morphism
$$(s_k)_{k=1}^n \mapsto \sum_{k=1}^n s s_k \otimes f(e_k).$$
- Note that $\mathrm{Hom}_S(S^n, S \otimes_R N) \cong \mathrm{Hom}_S((S \otimes_R R)^n, S \otimes_R N)$ by sending the morphism $(s_k)_{k=1}^n \mapsto \sum_k s s_k \otimes f(e_k)$ to the morphism defined by $(s_k \otimes 1)_{k=1}^n \mapsto \sum_k s s_k \otimes f(e_k)$.
  In particular, the morphism in the codomain is
$$(s_k \otimes r_k)_{k=1}^n \mapsto \sum_{k=1}^n s s_k \otimes f(r_k e_k).$$

- Note that $\mathrm{Hom}_S((S \otimes_R R)^n, S \otimes_R N) \cong \mathrm{Hom}_S(S \otimes R^n, S \otimes_R N)$ by sending $(s_k \otimes r_k)_{k=1}^n \mapsto \sum_k s s_k \otimes r_k f(e_k)$ to

$$s_0 \otimes (r_k)_{k=1}^n \mapsto \sum_{k=1}^n s s_0 \otimes f(r_k e_k) = s s_0 \otimes f\left((r_k)_{k=1}^n\right).$$

So indeed, we have tracked our isomorphism, and we can see from the last point that $s \otimes f$ has gone to $s_0 \otimes m \mapsto s s_0 \otimes f(m)$, 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.

$$\begin{array}{ccccccccc} 0 & \longrightarrow & K & \longrightarrow & R^m & \longrightarrow & R/I & \longrightarrow & 0 \\ & & \downarrow & & \downarrow & & \| & & \\ 0 & \longrightarrow & I & \longrightarrow & R & \longrightarrow & R/I & \longrightarrow & 0 \end{array}$$

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 $\mathrm{coker}(K \to I) \cong \mathrm{coker}\,(R^m \to R)$, which is finitely generated because R will surject onto it. But then the short exact sequence

$$0 \to \mathrm{im}(K \to I) \to I \to \mathrm{coker}(K \to I) \to 0$$

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.

$$\begin{array}{ccccccc}
0 & \longrightarrow & S \otimes_R \operatorname{Hom}_R(M, N) & \longrightarrow & S \otimes_R \operatorname{Hom}_R(R^n, N) & \longrightarrow & S \otimes_R \operatorname{Hom}_R(R^m, N) \\
 & & \downarrow{\scriptstyle \alpha} & & \downarrow{\scriptstyle \alpha} & & \downarrow{\scriptstyle \alpha} \\
0 & \longrightarrow & \operatorname{Hom}_S(S \otimes_R M, S \otimes_R N) & \longrightarrow & \operatorname{Hom}_S(S \otimes_R R^n, S \otimes_R N) & \longrightarrow & \operatorname{Hom}_S(S \otimes_R R^m, S \otimes_R N)
\end{array}$$

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 $r_1 x_1 + r_2 x_2 \in \operatorname{Ann} m$, 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 $x_1, \dots, x_n$, 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

$$um = \sum_{k=1}^{n} u a_k x_k = \sum_{k=1}^{n} a_k \cdot 0 = 0.$$

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

$$0 \to A \to B \xrightarrow{\pi} C \to 0. \tag{$*$}$$

This sequence splits if and only if $\operatorname{Hom}_R(C, B) \xrightarrow{\pi\circ -} \operatorname{Hom}_R(C, C)$ is surjective if and only if, for each maximal $\mathfrak{p}$, the map $\operatorname{Hom}_R(C, B)_{\mathfrak{p}} \xrightarrow{\pi\circ -} \operatorname{Hom}_R(C, C)_{\mathfrak{p}}$ is surjective by Corollary 2.86. Tracking Remark 2.69 through shows this is equivalent to

$$\operatorname{Hom}_{R_{\mathfrak{p}}}(C_{\mathfrak{p}}, B_{\mathfrak{p}}) \xrightarrow{\pi_{\mathfrak{p}}\circ -} \operatorname{Hom}_{R_{\mathfrak{p}}}(C_{\mathfrak{p}}, C_{\mathfrak{p}})$$

being surjective, which is equivalent to $(*)$ splitting locally for each maximal $\mathfrak{p}$.

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 $f \in k[x_1, \dots, x_m]$ has a unique representation as

$$f(x_1, \dots, x_m) = \sum_{d_1, \dots, d_m = 0}^{\infty} a_{d_1, \dots, d_m} \left(x_1^{d_1} \cdots x_m^{d_m} \right),$$

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 $k[x_1, \dots, x_m]$; similarly, the terms $y_1^{e_1} \cdots y_n^{e_n}$ form a k-basis of $k[y_1, \dots, y_n]$.

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 $k[x_1, \dots, x_m] \otimes_k k[y_1, \dots, y_n]$.

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 $k[x_1, \dots, x_m] \otimes_k k[y_1, \dots, y_m]$ 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

$$\sum_{\substack{d_1, \dots, d_m \in \mathbb{N} \\ e_1, \dots, e_n \in \mathbb{N}}} a_{d_1, \dots, d_m, e_1, \dots, e_n} \left(\prod_{i=1}^{m} (x_i \otimes 1)^{d_i} \right) \left(\prod_{j=1}^{n} (1 \otimes y_j)^{e_j} \right) = 0,$$

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

$$\sum_{\substack{d_1, \dots, d_m \in \mathbb{N} \\ e_1, \dots, e_n \in \mathbb{N}}} a_{d_1, \dots, d_m, e_1, \dots, e_n} \left(x_1^{d_1} \cdots x_m^{d_m} \otimes y_1^{e_1} \cdots y_n^{e_n} \right) = 0.$$

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 $I \subseteq k[x_1, \dots, x_m]$ and $Y = Z(J)$ for an ideal $J \subseteq k[y_1, \dots, y_m]$.

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 $k[x_1, \dots, x_m, y_1, \dots, y_n] = A\left(\mathbb{A}^m(k) \times \mathbb{A}^n(k)\right)$ 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

$$\frac{k[x_1, \dots, x_m, y_1, \dots, y_n]}{I + J} \cong \frac{k[x_1, \dots, x_m]}{I} \otimes_k \frac{k[y_1, \dots, y_n]}{J},$$

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

$$\psi : \frac{k[x_1, \dots, x_m]}{I} \times \frac{k[y_1, \dots, y_n]}{J} \to \frac{k[x_1, \dots, x_m, y_1, \dots, y_n]}{I + J}$$

  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

$$(f - f')g, f'(g - g') \in I + J \subseteq k[x_1, \dots, x_m, y_1, \dots, y_n],$$

    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

$$\overline{\psi} : \frac{k[x_1, \dots, x_m]}{I} \otimes_k \frac{k[y_1, \dots, y_n]}{J} \to \frac{k[x_1, \dots, x_m, y_1, \dots, y_n]}{I + J}$$

  by $f \otimes g \mapsto fg$.

- We cheat by appealing to Exercise 2.91, which provides a canonical k-algebra isomorphism

$$k[x_1, \dots, x_m, y_1, \dots, y_n] \cong k[x_1, \dots, x_m] \otimes_k k[y_1, \dots, y_n]$$

  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

$$\varphi : k[x_1, \dots, x_m, y_1, \dots, y_n] \to \frac{k[x_1, \dots, x_m]}{I} \otimes_k \frac{k[y_1, \dots, y_n]}{J}.$$

  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

$$\overline{\varphi} : \frac{k[x_1, \dots, x_m, y_1, \dots, y_n]}{I + J} \to \frac{k[x_1, \dots, x_m]}{I} \otimes_k \frac{k[y_1, \dots, y_n]}{J}.$$

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.

$$\begin{array}{ccccccc} I \otimes_R M & \longrightarrow & R \otimes_R M & \longrightarrow & (R/I) \otimes_R M & \longrightarrow & 0 \\ \downarrow & & \downarrow & & \vdots\downarrow & & \\ IM & \longrightarrow & M & \longrightarrow & M/IM & \longrightarrow & 0 \end{array}$$

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

$$[r]_I \otimes m \leftarrow\!\shortmid r \otimes m \mapsto rm \mapsto [rm]_{IM}.$$

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.

$$\begin{array}{ccc} (R/I) \otimes_R M & \xrightarrow{\varphi} & (R/I) \otimes_R N \\ \cong\downarrow & & \downarrow\cong \\ M/IM & \xrightarrow{\varphi} & N/IN \end{array}$$

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 $\overset{*}{\cong}$. ∎

Corollary 2.102. 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. ∎

2.3.2 Artinian Rings

We have the following definition, dual to the ascending chain condition for Noetherian modules.

Definition 2.103 (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 2.104. 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 2.105. 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 2.106. More generally, any finite-dimensional k-algebra is an Artinian ring.

Example 2.107. 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 2.108. 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 2.109 (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 2.110 (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 2.111 (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 2.112. 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 2.113. 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 2.114. 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.

  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. ∎

[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 $B_{k+1} + A$.

Remark 2.115 (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 2.116. 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 2.114; we will use it as a technical lemma in the proof.

Lemma 2.117. 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 2.114, fix a composition series

$$B =: B_0 \supsetneq B_1 \supsetneq \cdots \supsetneq B_{n-1} \supsetneq B_0 := (0),$$

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 $A_k := A \cap B_k$. 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 2.118 (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 2.119. 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 $k \leq n$.

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 2.117 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 $k - 1 \geq n - 1$, so $k \neq n$ follows. ■

It follows from Lemma 2.119 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 2.120. 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 2.112.

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 2.119 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 2.119, 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 2.119, 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 2.121. 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 $k \in \{1, \dots, n\}$, then $\operatorname{Supp} M = \{\mathfrak{p}_1, \dots, \mathfrak{p}_n\}$.

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 $k \in \{2, \dots, n\}$. So the inductive hypothesis promises

$$\operatorname{Supp} M_1 = \{\mathfrak{p}_2, \dots, \mathfrak{p}_n\}.$$

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

$$\operatorname{Supp} M = \{\mathfrak{p}_1, \mathfrak{p}_2, \dots, \mathfrak{p}_n\},$$

which is what we wanted. ■

And here is a nice result which we get from this.

Theorem 2.122. 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 2.123. 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 2.123. 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 2.108. 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 2.124. 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 2.123. For the other direction, we note that we can show all primes are maximal without tears.

Lemma 2.125. 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 2.126 (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 2.127. 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.

$$\begin{array}{ccccccccc}
0 & \longrightarrow & \dfrac{\mathfrak{m}_1 \cap \cdots \cap \mathfrak{m}_n}{\mathfrak{m}_1 \cap \cdots \cap \mathfrak{m}_n \cap \mathfrak{m}_{n+1}} & \longrightarrow & \dfrac{R}{\mathfrak{m}_1 \cap \cdots \cap \mathfrak{m}_n \cap \mathfrak{m}_{n+1}} & \longrightarrow & \dfrac{R}{\mathfrak{m}_1 \cap \cdots \cap \mathfrak{m}_n} & \longrightarrow & 0 \\
 & & & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & R/\mathfrak{m}_{n+1} & \longrightarrow & \displaystyle\bigoplus_{k=1}^{n+1} R/\mathfrak{m}_k & \longrightarrow & \displaystyle\bigoplus_{k=1}^{n} R/\mathfrak{m}_k & \longrightarrow & 0
\end{array}$$

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 2.128. 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 2.129 (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 2.123. The main idea is to try to make Lemma 2.127 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 2.130 (Serganova)**.** Here is alternate motivation for the below claim: the payoff to Lemma 2.127 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 2.131. 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 2.127, 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 2.116, 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 2.132 (Miles)**.** Here is an alternate finish after Lemma 2.131. 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 2.130 to write

$$\frac{J^k}{J^{k+1}} = \frac{\left(J^k\right)}{J\left(J^k\right)} \cong J^k \otimes_R \frac{R}{J} \cong J^k \otimes_R \bigoplus_{\mathfrak{m}} R/\mathfrak{m} \cong \bigoplus_{\mathfrak{m}} \left(J^k \otimes_R R/\mathfrak{m}\right).$$

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.

[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.

Proposition 2.133. 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 2.134. Fix $I \subseteq k[x_1, \dots, x_n]$. Then the following are equivalent.

(a) The ring $R := k[x_1, \dots, x_n]/I$ 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 $R := k[x_1, \dots, x_n]/I$ is Artinian. Then R has finitely many maximal ideals by Lemma 2.127, 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 $R = k[x_1, \dots, x_n]/I$ 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 $f, g \in k[x_1, \dots, x_n]$ 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.
- 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 2.135. 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 2.136. 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]

[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.

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 2.137. 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 2.135, 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. ■

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 2.138 (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 2.139. 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 2.140. Let n be a nonzero integer. Fix $M := \mathbb{Z}/n\mathbb{Z}$ as a $\mathbb{Z}$-module. Then $\operatorname{Ass} M = \{(p) : \text{prime } p \mid n\}$.

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 2.141. 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 2.142 (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 2.143. 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 2.141 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 2.144. 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 2.145. Fix R a Noetherian ring and M a nonzero R-module. Then $\operatorname{Ass} M$ is nonempty.

Proof. As in Proposition 2.144, 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 2.146 (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 2.147. 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 2.148. 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 2.144 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 2.144 that $\mathfrak{p}$ is indeed prime, so it is an associated prime containing $\operatorname{Ann} m$. ∎

Here are some corollaries.

Corollary 2.149. 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 2.148. ∎

Corollary 2.150. 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 2.149, $\ker \varphi \subseteq M$ 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 2.151. 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
$$\operatorname{Ann} \iota(a) = \{r \in R : r\iota(a) = 0\} = \{r \in R : \iota(ra) = 0\} \overset{*}{=} \{r \in R : ra = 0\} = \operatorname{Ann} a,$$
where in $\overset{*}{=}$ 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 2.152 (Nir)**.** Alternatively, any associated prime $\mathfrak{p} \in \operatorname{Ass} A$ induces an R-embedding $R/\mathfrak{p} \hookrightarrow A$ (by Lemma 2.141). Post-composing with ι gives an R-embedding $R/\mathfrak{p} \hookrightarrow B$, so Lemma 2.141 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 2.141); 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 2.141.

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
$$Rb \cap \operatorname{im} \iota \overset{?}{=} \{0\}.$$
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 2.153. 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 2.151. In particular, $\operatorname{Ass} A \cup \operatorname{Ass} C \subseteq \operatorname{Ass} B$, but Lemma 2.151 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 2.154. 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 2.153, 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 2.140 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 2.155. 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 2.141) 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 $0 \leq k < \ell$. 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 2.141), 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 2.156. Fix M a finitely generated module over a Noetherian ring R. Then $\operatorname{Ass} M$ is finite.

Proof. By Lemma 2.155, 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 2.151. But $\operatorname{Ass} M_{k+1}/M_k = \operatorname{Ass} R/\mathfrak{p}_k = \{\mathfrak{p}_k\}$ by Example 2.143. 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 2.157 (Nir)**.** The above theorem is "effective" in the sense that, if we could compute the filtration Lemma 2.155, we would have an effective upper bound on $\operatorname{Ass} M$. However, making the filtration required using the non-effective Proposition 2.144.

Let's also discuss some other ways we can access associated primes; just like support, associated primes commute with localization.

Proposition 2.158. 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 2.141 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 2.141 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 2.141.

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 2.159. 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 2.148, 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 2.160 (Serganova)**.** One could also proceed more directly, without using Proposition 2.148, by choosing $\mathfrak{p}$ to be maximal among annihilators containing $\operatorname{Ann} m$ as in the proof of Proposition 2.148.

Corollary 2.161. 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 2.159. 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

$$\{\mathfrak{p}_1, \dots, \mathfrak{p}_n\}$$

as the primes of $\operatorname{Ass} M$ maximal among the other primes of $\operatorname{Ass} M$; this labeling is finite because of Theorem 2.156. 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. Well, $J \not\subseteq \mathfrak{p}_k$ grants us some $y_k \in J \setminus \mathfrak{p}_k$, from which we set

$$x_k := y_k \prod_{\substack{1 \leq k \leq n \\ k \neq \ell}} x_{k,\ell}.$$

None of the factors here live in $\mathfrak{p}_k$, so $x_k \notin \mathfrak{p}_k$. However, x_k contains a factor in J and in $\mathfrak{p}_\ell$ for each $\ell \neq k$, so x_k lives in each of those ideals. To finish, we note

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

will live in J because each $x_k \in J$, but for each $\mathfrak{p}_k$, $x_k \notin \mathfrak{p}_k$ while $x_\ell \in \mathfrak{p}_\ell$ for each $\ell \neq k$, so $x \notin \mathfrak{p}_k$. Thus, $x \in J$ but not in any of the primes $\mathfrak{p}_k$, finishing. ∎

Lastly, we provide another way to generated associated primes, to close out our discussion.

Proposition 2.162. 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 2.145 tells us that

$$\operatorname{Ass}_{R_\mathfrak{p}} M_\mathfrak{p} \neq \varnothing.$$

However, Proposition 2.158 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 2.163. 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 2.164 ($\mathfrak{p}$-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 2.165. For a prime $p \in \mathbb{Z}$, the ideals $\left(p^k\right)$ are p-primary in $\mathbb{Z}$ by Exercise 2.140.

Example 2.166. Any prime ideal $\mathfrak{p}$ is $\mathfrak{p}$-primary in R because $\operatorname{Ass}(R/\mathfrak{p}) = \{\mathfrak{p}\}$ by Example 2.143.

Let's prove one nice lemma to finish off today.

Lemma 2.167. Fix M a module over a Noetherian ring R. Fix $N_1, \dots, N_m$ 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 2.151 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 2.145 because R is Noetherian and $N_1 \cap N_2 \subseteq N_1 \subsetneq M$. ∎

And we close by stating the theorem.

Theorem 2.168 (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

$$\mathfrak{p}_1 \supseteq \mathfrak{p}_2 \supseteq \cdots.$$

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 2.169 (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 2.170. 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 2.171. 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 2.162 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 2.156. ■

2.5.2 Primary Decomposition for Geometers

We note that Proposition 2.171 has the following corollary.

Corollary 2.172. 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 2.135, 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 2.171. ■

We close with a geometric interpretation of Corollary 2.172. We have the following definition.

Definition 2.173 (Irreducible)**.** Fix $X \subseteq \mathbb{A}^n(k)$ an affine algebraic set. Then X is *irreducible* if and only if $I(X) \subseteq k[x_1, \dots, x_n]$ 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 2.172 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

$$X = Z(I(X)) = Z\left(\bigcap_{\mathfrak{p} \in \mathcal{P}} \mathfrak{p}\right) = \bigcup_{\mathfrak{p} \in \mathcal{P}} Z(\mathfrak{p}).$$

[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 $I \cap J$.

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 2.174. 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. ■

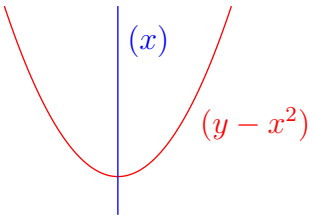
And now let's see a physical example.

Exercise 2.175. 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. ■

2.5.3 Primary Grab-Bag

In Corollary 2.172, 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 2.176 ($\mathfrak{p}$-primary)**.** Fix M a finitely generated module over R a Noetherian ring. Then a submodule $N \subseteq M$ is $\mathfrak{p}$-*primary* if and only if $\operatorname{Ass} M/N = \{\mathfrak{p}\}$.

Definition 2.177 ($\mathfrak{p}$-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 2.178. 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 2.162) 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 2.159 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 2.135, 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 2.179. 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

$$I := (x_1, \dots, x_m).$$

Additionally, because $I \subseteq \operatorname{rad} J$, we are promised positive integers $a_1, \dots, a_m$ 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 2.180 (Nir)**.** The Noetherian condition is necessary. Consider $R := k[x_1, x_2, x_3, \dots]$ with $I = (x_1, x_2, x_3, \dots)$ and $J = \left(x_1, x_2^2, x_3^3, \dots\right)$. 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 2.181. 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 2.182. 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 2.183 (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 2.184 (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 2.185. 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 2.186. 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 2.187 (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 2.188. 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 2.141, 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 $[m_{\mathfrak{q}}]_N := \iota_{\mathfrak{q}}([1]_{\mathfrak{q}})$. 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 2.189. 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 2.190 (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 $\operatorname{Ass} M/N \subseteq \{\mathfrak{p}_1, \dots, \mathfrak{p}_n\}$.

(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 2.151 and Corollary 2.153, we see

$$\operatorname{Ass} M/N \subseteq \operatorname{Ass}\left(\bigoplus_{i=1}^{n} M/N_i\right) = \bigcup_{i=1}^{n} \operatorname{Ass} M/N_i = \{\mathfrak{p}_1, \dots, \mathfrak{p}_n\},$$

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 2.151 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 2.151 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 2.167, 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 2.191 (Nir)**.** With Theorem 2.190, 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 $\operatorname{Ass} M/N = \{\mathfrak{p}_1, \dots, \mathfrak{p}_n\}$ by Theorem 2.190 part (b). In particular,

$$\#\operatorname{Ass} M/N \leq n.$$

In fact, it is not too hard to be convinced that this is achievable, essentially using the argument from Theorem 2.190 part (c): start with any primary decomposition and remove any removable terms until $\operatorname{Ass} M/N = \{\mathfrak{p}_1, \dots, \mathfrak{p}_n\}$ as in Theorem 2.190 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 2.192 (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 2.158 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 2.193. 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 2.182.

Remark 2.194 (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 2.195. 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 2.182. 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 2.191, 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 $n \leq \#\operatorname{Ass} R/(r)$.

  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 2.183 in the existence of the primary decomposition, so we would like to leverage this power to talk more directly about factorizations.

Proposition 2.196. 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 2.196. We begin with the forward direction. The main technical lemma is as follows.

Lemma 2.197. 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

$$x \in \left(\bigcap_{k=1}^{n} I_k \right) \setminus \mathfrak{p},$$

which finishes. ∎

Remark 2.198 (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 2.195, we get

$$\bigcap_{k=1}^{n} (p_k^{\alpha_k}) = (r) \subseteq \mathfrak{p}.$$

In particular, by Lemma 2.197, 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 2.196. 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 2.170 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 2.199 (Nir)**.** As an example of the condition in Proposition 2.196 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 2.200. 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

$$\left\{1, x, y, y^2, y^3, \ldots\right\}$$

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 2.195 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.

[8] Namely, $\varphi(f) = 0$ if and only if all monomials in f are divisible by x if and only if $f \in (x)$.

- We check that (y^n) is (x,y)-primary. For this, we search for possible associated primes of $R/(y^n)$. Suppose we have $m \in R/(y^n)$ with $\mathfrak{p} = \operatorname{Ann} m \in \operatorname{Ass} R/(y^n)$. 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 $R/(y^n)$: 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 2.190, we see $\operatorname{Ass} R = \{(x,y), (x)\}$, and Remark 2.191 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.

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 2.201. 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 unique factorization 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

$$\operatorname{cont}(rf) = (ra_0, \dots, ra_n) = r(a_0, \dots, a_n) = r \operatorname{cont}(f).$$

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

  $$f(x) = \sum_{k=0}^{\infty} a_k x^k \qquad \text{and} \qquad g(x) = \sum_{\ell=0}^{\infty} b_\ell x^\ell,$$

  where all but finitely many of the a_k and b_ℓ vanish. Then

  $$(fg)(x) = \sum_{n=0}^{\infty} \left(\sum_{k+\ell=n} a_k b_\ell \right) x^n.$$

  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 $a_k b_\ell \in \operatorname{cont}(f)\operatorname{cont}(g)$. 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 2.135,

  $$\operatorname{rad}\operatorname{cont}(fg) = \bigcap_{\operatorname{cont}(fg) \subseteq \mathfrak{p}} \mathfrak{p}.$$

  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 $f = g_0 h_0$ 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 $k[x_1, \dots, x_n]$ 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 $k[x_1, \dots, x_{n-1}][x_n]$ has unique factorization from $k[x_1, \dots, x_{n-1}]$, 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

$$C_{ij} := (-1)^{i+j} \det A_{i,j},$$

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

$$A' := \begin{bmatrix} a_{11} & \cdots & a_{1,i-1} & a_{1k} & a_{1,i+1} & \cdots & a_{1n} \\ \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots \\ a_{n1} & \cdots & a_{n,i-1} & a_{nk} & a_{n,i+1} & \cdots & a_{nn} \end{bmatrix}.$$

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 $\mu(p_A(x)) = 0 \in \mathrm{End}_R(R^n)$. 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

$$\begin{aligned}
\mu(p_A(x)) &= \mu\left(\det \begin{bmatrix} x-a_{11} & -a_{12} & \cdots & -a_{1n} \\ -a_{21} & x-a_{22} & \cdots & -a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ -a_{n1} & -a_{n2} & \cdots & x-a_{nn} \end{bmatrix}\right) \\
&= \det \begin{bmatrix} \mu(x-a_{11}) & \mu(-a_{12}) & \cdots & \mu(-a_{1n}) \\ \mu(-a_{21}) & \mu(x-a_{22}) & \cdots & \mu(-a_{2n}) \\ \vdots & \vdots & \ddots & \vdots \\ \mu(-a_{n1}) & \mu(-a_{n2}) & \cdots & \mu(x-a_{nn}) \end{bmatrix} \\
&= \underbrace{\det \begin{bmatrix} \varphi-\mu(a_{11}) & -\mu(a_{12}) & \cdots & -\mu(a_{1n}) \\ -\mu(a_{21}) & \varphi-\mu(a_{22}) & \cdots & -\mu(a_{2n}) \\ \vdots & \vdots & \ddots & \vdots \\ -\mu(a_{n1}) & -\mu(a_{n2}) & \cdots & \varphi-\mu(a_{nn}) \end{bmatrix}}_{\varphi\mu(I)-\mu(A)}.
\end{aligned}$$

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, $\varphi\mu(I) - \mu(A) \in \mathrm{End}_R\left(R^n\right)^{n\times n}$.

To show that $\det(\varphi\mu(I) - \mu(A)) = 0$, we note that $\varphi\mu(I) - \mu(A)$ will vanish on the vector $(\pi_1, \ldots, \pi_n) \in \mathrm{Mor}_{\mathrm{Set}}(R^n, R^n)^n$, 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 $\varphi \in \mathrm{End}_R(M)$. Then there exists some monic polynomial

$$p_\varphi(x) = x^n + p_1 x^{n-1} + \cdots + p_n$$

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

$$p_A(x) = \sum_{k=0}^n r_k x^k.$$

Then, for any m_j, we see that $\varphi m_j = Am_j$

$$p_A(\varphi)(m_j) = \sum_{k=0}^{n} r_k \varphi^k m_j = \sum_{k=0}^{n} r_k A^k m_j = p_A(A)m_j = 0,$$

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 $\{m_1', \dots, m_n'\}$. 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 $n \geq m$. 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 $[r]_{\mathfrak{m}} \neq [0]_{\mathfrak{m}} \in R/\mathfrak{m}$, 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 $\mathrm{id} \in \operatorname{End}_R(M)$, the fact that $IM = M$ (!) gives us a polynomial

$$p_{\mathrm{id}}(x) := x^n + p_1 x^{n-1} + \cdots + p_n \in R[x],$$

such that $p_{\mathrm{id}}(\mathrm{id}) = 0$ and $p_k \in I^k$ for each p_k. But plugging in $x = \mathrm{id}$, we see

$$0 = p_{\mathrm{id}}(\mathrm{id}) = \mathrm{id}^n + p_1 \mathrm{id}^{n-1} + \cdots + p_n \mathrm{id}^0 = \big(1 - (-p_1 - \cdots - p_n)\big)\mathrm{id}.$$

In particular, we set $r := -p_1 - \cdots - p_n \in I$ so that $(1-r)m = (1-r)\,\mathrm{id}\,m = 0$ 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

$$m - (r_1 m_1 + \cdots + r_n m_n) = xm_0 \in IM,$$

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

$$\ker \pi \to M \xrightarrow{\pi} R/\mathfrak{m} \to 0.$$

To finish, we note that tensoring is right-exact and therefore preserves surjections. Thus, there is an induced surjection

$$N \otimes_R \ker \pi \to N \otimes_R M \xrightarrow{\pi} N \otimes_R (R/\mathfrak{m}) \to 0.$$

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 2.102 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 2.102 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
$$m = \sum_{k=0}^{\infty} a_k s^k$$
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 $s^k \in \left\{1, s, s^2, \ldots, s^{n-1}\right\}$, 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
$$\left\{1, s, s^2, \ldots, s^{n-1}\right\}$$

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 $\left\{s^0, \dots, s^d\right\}$ is R-linearly independent (formally, add in the terms $0s^k$ for $d \le k < n$ to reduce to the set $\left\{s^0, \dots, s^n\right\}$, 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 $\left\{1, s, \dots, s^{n-1}\right\}$ 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 $(r_0, \dots, r_{n-1}) \mapsto r_0 s^0 + \cdots + r_{n-1} s^{n-1}$. 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 S-algebra R 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

$$\mu_s(r_1 s_1 + r_2 s_2) = s r_1 s_1 + s r_2 s_2 = r_1 s s_1 + s_2 s s_2 = r_1 \mu_s(s_1) + r_2 \mu_s(s_2).$$

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 $c_1, \dots, c_n$. Similarly, because B is finite over A, we get generators $b_1, \dots, b_m$. 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 $b_1, \dots, b_m$, 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 $S = R[s_1, \dots, s_n]$ where the elements $s_1, \dots, s_n$ are all integral over R. The key is to consider the chain

  $$R \subseteq R[s_1] \subseteq R[s_1, s_2] \subseteq \cdots \subseteq R[s_1, \dots, s_n].$$

  We show that $R[s_1, \dots, s_k]$ is finite over R by induction on k; when $k = 0$, there is nothing to say. For the inductive step, suppose that some $R[s_1, \dots, s_k]$ is finite over R by the elements $\{x_1, \dots, x_m\}$, and we show $R[s_1, \dots, s_{k+1}]$ is finite over R.

  Well, s_{k+1} is the root of some monic polynomial which we name $p \in R[x]$. But $p \in R[s_0, \dots, s_k]$ as well, so s_{k+1} is integral over $R[s_0, \dots, s_k]$. Thus, byProposition 3.44, $R[s_1, \dots, s_k][s_{k+1}]$ will still be finitely generated as an $R[s_1, \dots, s_k]$-module.

  It follows that $R[s_1, \dots, s_{k+1}]$ 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 $S = Rs_0R + \cdots + s_nR$ for some elements $s_0, \dots, s_n \in S$. 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 out of our algebra.

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 $v := uu_0u_1\cdots u_{n-1}$ and multiply through by $v = u^n$ to get
$$(vs)^n + \left(v \cdot \frac{r_{n-1}}{u_{n-1}}\right)(vs)^{n-1} + \cdots + \left(v^{n-1} \cdot \frac{r_1}{u_1}\right)(sv) + v^n \cdot \frac{r_0}{u_0} = 0.$$
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, 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.

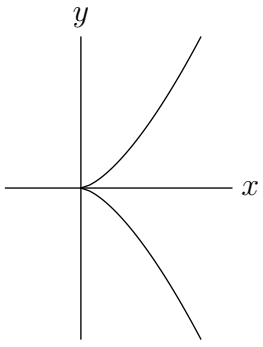
Remark 3.67. Of course, not all normal rings are unique factorization domains. For example, $\mathbb{Z}\left[\sqrt{-5}\right]$ is normal but not a unique factorization domain (by Warning 1.28). The fact that $\mathbb{Z}[\sqrt{-5}]$ is normal in $\mathbb{Q}(\sqrt{-5})$ is a problem on the homework.

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

$$f(x,y) := \sum_{k,\ell \in \mathbb{N}} a_{k,\ell} x^k y^\ell \equiv \sum_{k=0}^{\infty} b_k x^k + y \sum_{k=0}^{\infty} c_k x^k \pmod{y^2 - x^3},$$

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 $k[t]$.

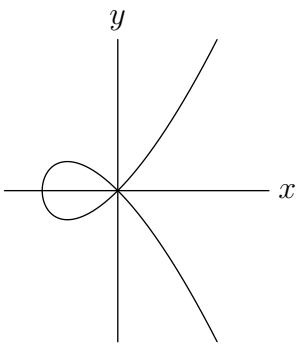
So to finish, we note that $\varphi(y/x) = t$, so because $\varphi : K(R) \to k(t)$ is injective, we see that we can just callously pull t back to y/x. In particular, our integral closure is

$$\varphi^{-1}(k[t]) = \boxed{R[y/x]},$$

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 $R[\alpha_1, \dots, \alpha_n, \beta_1, \dots, \beta_m] \subseteq S[\alpha_1, \dots, \alpha_n, \beta_1, \dots, \beta_m]$. 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, $R[\alpha_1, \dots, \alpha_n, \beta_1, \dots, \beta_m]$ 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 $R[\alpha_1, \dots, \alpha_n, \beta_1, \dots, \beta_m]$ 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 $f = g_0 h_0$ 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 S-algebra R. 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 $u_0 u_1 \cdots u_n$ 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.

3.3 February 17

Here we go.

3.3.1 The Nullstellensatz

Today we prove Hilbert's Nullstellensatz. Here is the statement.

Theorem 3.87 (Nullstellensatz)**.** Fix k an algebraically closed field.

(a) There are bijections between algebraic sets $X \subseteq \mathbb{A}^n(k)$ and radical ideals $J \subseteq k[x_1, \dots, x_n]$ by taking
$$X \mapsto I(X) := \{f \in k[x_1, \dots, x_n] : f(p) = 0 \text{ for all } p \in X\},$$
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 $k[x_1, \dots, x_n]/I(X)$, which are in bijection with maximal ideals of $k[x_1, \dots, x_n]$ 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
$$J \overset{?}{\supseteq} I(Z(J)).$$
We also remark that the last claim of (b) is merely ring theory.

Lemma 3.88. 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 3.89. Suppose that all maximal ideals of $k[x_1, \dots, x_n]$ take the form $(x_1 - a_1, \dots, x_n - a_n)$ for $(a_1, \dots, a_n) \in \mathbb{A}^n(k)$. Then (b) of Theorem 3.87 holds.

Proof. By the previous lemma, we only have to show the first sentence of (b). Our bijection will be by

$$(a_1, \dots, a_n) \in X \longmapsto (x_1 - a_1, \dots, x_n - a_n) \subseteq k[x_1, \dots, x_n].$$

We have the following checks to show (b).

- We check that $(x_1 - a_1, \dots, x_n - a_n)$ is maximal. To see this, we claim that $(x_1 - a_1, \dots, x_n - a_n)$ is the kernel of the surjective map
$$\varphi \in k[x_1, \dots, x_n] \to k$$
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 $f \in k[x_1, \dots, x_n]$, we can apply the division algorithm to f by each of the $x_i - a_i$ to write
$$f(x_1, \dots, x_n) = f(a_1, \dots, a_n) + \sum_{i=1}^{n} (x_i - a_i) q_i(x).$$
Formally, one should show this by induction on n, but we won't bother. The point is that $f \in \ker \varphi$ implies that $f(a_1, \dots, a_n) \in \ker \varphi$, so $f(a_1, \dots, a_n) = 0$, so $f \in (x_1 - a_1, \dots, x_n - a_n)$.

- We check that $(x_1 - a_1, \dots, x_n - a_n)$ contains $I(X)$. Indeed, if $f \in I(X)$, then f vanishes on $(a_1, \dots, a_n)$, so f lives in the kernel $\ker \varphi$ constructed above, so $f \in (x_1 - a_1, \dots, x_n - a_n)$.

- We show the map is injective. The key claim is that
$$Z((x_1 - a_1, \dots, x_n - a_n)) = \{(a_1, \dots, a_n)\}.$$
Indeed, if $(b_1, \dots, b_n)$ lives in this vanishing set, then $b_i - a_i = 0$ for each i, so $(a_1, \dots, a_n) = (b_1, \dots, b_n)$. Of course, each $x_i - a_i$ does vanish on $(a_1, \dots, a_n)$, so we are done.

  So to finish, we note that $(x_1 - a_1, \dots, x_n - a_n) = (x_1 - a_1', \dots, x_n - a_n')$ implies that their vanishing sets match, so $(a_1, \dots, a_n) = (a_1', \dots, a_n')$, 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
$$\mathfrak{m} = (x_1 - a_1, \dots, x_n - a_n)$$
by hypothesis. So we see that $\mathfrak{m} \supseteq I(X)$ implies that
$$X = Z(I(X)) \supseteq Z(\mathfrak{m}) = \{(a_1, \dots, a_n)\},$$
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 3.87 for uncountable fields. We prove Theorem 3.87 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 3.90. 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

$$S := \left\{ \frac{1}{x-a} : a \in k \right\}.$$

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. ∎

[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 $k[x] \cong k[T]$.

Corollary 3.91. 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 3.90 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 3.89 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 3.91, but k is algebraically closed, so this field must equal k. In particular, we are promised an isomorphism

$$\varphi : \frac{k[x_1, \ldots, x_n]}{\mathfrak{m}} \cong k.$$

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 3.92. 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 3.91. 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 3.88. 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 2.135 to write

$$J = \bigcap_{\mathfrak{p} \supseteq J} \mathfrak{p} \overset{*}{=} \bigcap_{\mathfrak{p} \supseteq J} \bigcap_{\mathfrak{m} \supseteq \mathfrak{p}} \mathfrak{m} = \bigcap_{\mathfrak{m} \supseteq J} \mathfrak{m},$$

where we have used Lemma 3.92 in $\overset{*}{=}$. 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 3.89. 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 3.89. 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 3.93 (Jacobson)**.** A ring R is *Jacobson* if and only if any prime ideal is the intersection of some maximal ideals.

Remark 3.94 (Nir)**.** We note that J is Jacobson if and only if, for each prime $\mathfrak{p}$,

$$\bigcap_{\mathfrak{m}\supseteq\mathfrak{p}} \mathfrak{m} = \mathfrak{p}. \tag{$*$}$$

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 3.88 says that (maximal) ideals $R/\mathfrak{p}$ are in bijection (maximal) ideals of R containing $\mathfrak{p}$ by π, so

$$\pi^{-1}\left(\bigcap_{\overline{\mathfrak{m}}\subseteq R/\mathfrak{p}} \overline{\mathfrak{m}}\right) = \bigcap_{\mathfrak{m}\supseteq\mathfrak{p}} \mathfrak{m} \quad \xRightarrow{\pi} \quad \bigcap_{\overline{\mathfrak{m}}\subseteq R/\mathfrak{p}} \overline{\mathfrak{m}} = \pi\left(\bigcap_{\mathfrak{m}\supseteq\mathfrak{p}} \mathfrak{m}\right).$$

Example 3.95. 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 3.96. 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 3.97. 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 $k[x_1, \dots, x_n]$ is Jacobson, akin to Lemma 3.92. In an attempt to generalize the argument given there, we have the following lemma.

Lemma 3.98. 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 3.99 (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 3.94. 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 3.98, we want to show that $\operatorname{rad} R/\mathfrak{p} = (0)$. Well, by Lemma 3.98, 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 3.100 (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 3.87 will follow from this, essentially using the same argument from before. We will be more explicit afterwards.

Proof of Theorem 3.100. 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 3.99. 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 3.99, 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 $b \in S'\backslash\{0\}$. By contraposition, we will actually suppose that we found $b \in S'\backslash\{0\}$ 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 3.99 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 3.96. 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
$$t^n + a_n^{-1}a_{n-1}t^{n-1} + \cdots + a_n^{-1}a_1 t + a_n^{-1}a_0 = 0,$$
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 $\left\{1, b, b^2, \ldots\right\} \subseteq K(S')$ must get a $K(R')$-relation eventually, which we label by
$$c_m b^m + \cdots + c_1 b + c_0 = 0,$$
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
$$R'\left[(c_0 a_n)^{-1}\right] \hookrightarrow S' \hookrightarrow S'\left[b^{-1}\right]$$
(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 $R'\left[(c_0 a_n)^{-1}\right]$ with unit leading coefficient, so b^{-1} is now integral over $R'\left[(c_0 a_n)^{-1}\right]$.

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

$$\pi : R[x_1, \dots, x_{r+1}] \twoheadrightarrow S.$$

Now, we set $S_0 := k[x_1, \dots, x_r]$ 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 3.87. All the logic is borrowed from the specific case, but we merely change the proof of the key lemmas Corollary 3.91 and Lemma 3.92 to use Theorem 3.100.

General proof of Theorem 3.87. We follow the argument from the special case. To start, note that k is Jacobson because it is (stupidly) a principal ideal domain, so $k \subseteq k[x_1, \dots, x_r]$ satisfies the hypotheses of Theorem 3.100. We have the following.

- We see that Corollary 3.91 holds for general algebraically closed fields k by part (b) of Theorem 3.100, which was what we needed for part (b) of Theorem 3.87.
- Additionally, we get Lemma 3.92 in the general case by part (a) of Theorem 3.100, which when combined with (b) of Theorem 3.87 is what we needed to prove part (a) of Theorem 3.87.

The above proves all of Theorem 3.87. ■

Remark 3.101. 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 3.102. 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 3.103. 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 3.102. 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 3.104. 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 2.190 tells us that $\operatorname{Ass} M = \{(x), (x,y)\}$. ■

Remark 3.105. 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 3.87,

$$I(Z) = \operatorname{rad}(a + d, ad - bc).$$

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

$$\frac{\mathbb{C}[a,b,c,d]}{(a+d, ad-bc)} \hookrightarrow \frac{\mathbb{C}[a,b,c]}{\left(a^2+bc\right)}.$$

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 $a^2 g$ term, so this factorization is trivial. ■

4.1.2 Filtration 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 $I_p I_q \subseteq I_{p+q}$.

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 $I_p I_q \subseteq I_{p+q}$ 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.

Anyways, let's see some examples.

Exercise 4.11. 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

$$\varphi\left(\sum_{p \geq 0} [f_p] \cdot \sum_{q \geq 0} [g_q]\right) = \varphi\left(\sum_{p+q=n} [f_p g_q]\right) = \sum_{p+q=n} \varphi_{p+q}([f_p g_q]) = \sum_{p+q=n} \varphi_p([f_p])\varphi_q([g_q]),$$

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

  $$f(x) = \sum_{d \geq n} a_d x^d$$

  has $a_n = 0$. In particular, we can write $f(x) = \sum_{d \geq n+1} a_d x^d$ 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 example because it is similar.

Example 4.12. 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 $a_0, a_1, a_2 \ldots \in \mathbb{Z}/p\mathbb{Z}$. In particular, 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 $\operatorname{gr}_{(p)} \mathbb{Z} \cong (\mathbb{Z}/p\mathbb{Z})[x]$.

4.1.4 Initial Forms

We have the following warning.

Warning 4.13. There is no natural ring homomorphism $R \to \operatorname{gr}_I R$.

However, there is a natural map of sets. Explicitly, for our filtration

$$R \supseteq I \supseteq I^2 \supseteq \cdots,$$

we want to find an element of the associated graded ring. In analogy to picking up the "initial" nonzero homogeneous part of a polynomial, we pick up $f \in R$ and define

$$\operatorname{in} f = f + I^{n+1},$$

where n is the largest possible such that $f \in I^n$. Of course, there is something of a problem when f lives in all of I^n, in which case we set $\operatorname{in} f := 0$.

Let's think about how this plays with our ring structure. Taking $f, g \in R$, if R is a domain, then we get that $\operatorname{in}(fg) = \operatorname{in}(f)\operatorname{in}(g)$. However, if f and g are zero-divisors, then we might be in trouble when $fg = 0$.

And now for some examples.

Example 4.14. Fix $X \subseteq \mathbb{A}^n(k)$ a Zariski closed set with $X = Z(J)$ such that $J \subseteq k[x_1, \ldots, x_n] =: R$ is an ideal. Taking $p \in X$ to correspond to a maximal ideal $\mathfrak{m} \subseteq A(X)$, we claim that

$$\operatorname{gr}_I R$$

is the ring corresponding to the "tangent cone to p at X."

As an example, consider the curve $y^2 = x^2(x+1)$, which splits at 0. At a point which is not $(0,0)$, we will have a line and therefore will expect to get a polynomial ring.

However, let's focus on what happens at $(0,0)$. Analytically, we find that

$$\frac{y^2}{x^2} = x + 1.$$

Very close to $(0,0)$, we get that

$$\left(\frac{dy}{dx}\right)^2 = 1$$

so that the slope is ± 1.

Let's try to think more algebraically. We have the following lemma.

Lemma 4.15. Work in the context of the above example. Then

$$\operatorname{gr}_I(R/J) = (\operatorname{gr}_I R)/\operatorname{in} J.$$

Proof. This is on the homework. ■

The point of this lemma is that $\operatorname{gr}_I R$ we know to be a polynomial ring. With $I = (x, y)$ as in the example we are working out, we find that $\operatorname{in}(x)^2 = \operatorname{in}(y)^2$ because our ideal J is $y^2 - x^2(x+1)$. Namely, our associated ring looks like functions generated by the lines $\operatorname{in} x = \operatorname{in} y$ and $\operatorname{in} x = -\operatorname{in} y$, which is what we expected.

In contrast, the cusp $y^2 = x^3 - x$ will give a double point, generated only at $\operatorname{in}(x)^2$. Here, we will be generated by $(\operatorname{in} y)^2$, which is what our cusp looks like intuitively.

4.1.5 Filtration of Modules

Consider the following construction.

Definition 4.16 (Hilbert function, rings)**.** Fix R a local Noetherian ring where I is the maximal ideal. Then we define

$$\dim_{R/I}(\operatorname{gr}_I R)_n = \dim_{R/I}\left(I^n/I^{n+1}\right) = H_R(n).$$

Note that this definition is well-formed because R/I is a field.

We would like to generalize this to modules. We have the following series of definitions.

Definition 4.17 (Filtration, modules)**.** Given an R-module M, a *filtration* is a descending chain

$$M = M_0 \supseteq M_1 \supseteq M_2 \supseteq \cdots.$$

This is an *I-filtration* if and only if $IM_n \subseteq M_{n+1}$.

There is no multiplicative condition on the filtration because M has no multiplication.

Definition 4.18 (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

$$\operatorname{gr}_{\mathcal{J}} M := M/M_1 \oplus M_1/M_2 \oplus \cdots.$$

We remark that $\operatorname{gr}_{\mathcal{J}} M$ is a graded $\operatorname{gr}_I R$-module, which is not too hard to check by hand.

Definition 4.19 (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 $IM_j = M_{j+1}$ for sufficiently large j.

It's a math class, so let's try to prove something today.

Proposition 4.20. Fix $I \subseteq R$ an ideal. Further, take M to be a finitely generated R-module, $\mathcal{J}$ to be a stable I-filtrations by finitely generated R-modules. Then $\operatorname{gr}_{\mathcal{J}} M$ is a finitely generated $\operatorname{gr}_I R$-module.

Proof. We definition-chase. Let our filtration be

$$M = M_0 \supseteq M_1 \supseteq M_2 \supseteq \cdots .$$

For sufficiently large n, we have that $I^k M_n = M_{n+k}$. Thus, it suffices to take generators for $M_0, M_1, \ldots, M_n$ to generate the entire associated graded module. ■

This lets us construct our Hilbert function for modules.

Definition 4.21 (Hilbert function, modules)**.** Fix R a local Noetherian ring where I is the maximal ideal with M a finitely generated R-module. Then we define

$$H_M(n) = \dim_{R/I} \left(I^n M / I^{n+1} M \right).$$

Note that this definition is well-formed because M is finitely generated.

4.1.6 The Artin–Rees Lemma

We are finally ready to provide our main result.

Theorem 4.22 (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 $N \subseteq M$, the induced filtration by $N_k := M_k \cap N$ is also a stable I-filtration.

Proof. To prove this, we need to introduce the blow-up ring.

Definition 4.23 (Blow-up ring)**.** Fix R a ring and $I \subseteq R$ an ideal. Then we define the *blow-up ring* $\mathrm{B}_I R$ by

$$\mathrm{B}_I R := R \oplus I \oplus I^2 \oplus \cdots .$$

Concretely, think about $\mathrm{B}_I R$ as getting its ring structure from $k[t]$ by something like $k[It]$. This also gives us our grading. In particular, is that $\mathrm{B}_I R / I \, \mathrm{B}_I R \cong \mathrm{gr}_I R$ after tracking everything through.

Example 4.24. 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 looks like $k[x, y][tx, ty]$. To look at points, we need to look at the "graded" spectrum of $\mathrm{B}_I R$. Here are some ways to do this.

- Look at $Z \subseteq \mathbb{A}^2(k) \times \mathbb{P}^1(k)$ to be points (p, ℓ) such that $p \in \ell$. We can project $Z \twoheadrightarrow \mathbb{A}^2(k)$ in the natural way. 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.
- Alternatively, focus on $k[x, y][tx, ty]$. Set $u = tx$ and $v = ty$ so that we are essentially looking at the ring

  $$\frac{k[x, y, u, w]}{(xw - yv)},$$

  which correspond to the 2×2 singular matrices. Taking the quotient by the "line action" of matrices

  $$\begin{bmatrix} 1 & 0 \\ 0 & \lambda \end{bmatrix}.$$

  Most of the time, this quotient process will give us 0, but rarely we will have an entire line after doing the quotient.

We remark that there is also a notion of the blow-up module.

Definition 4.25 (Blow-up ring)**.** Fix R a ring and $I \subseteq R$ an ideal. Further, fix $\mathcal{J}$ an I-filtration. Then we define the *blow-up module* $\mathrm{B}_I M$ by

$$\mathrm{B}_I M := M_0 \oplus M_1 \oplus M_2 \oplus \cdots,$$

which we can check to be a graded $\mathrm{B}_I R$-module.

In line with this, we have the following proposition.

Proposition 4.26. 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 $\mathrm{B}_{\mathcal{J}} M$ is finitely generated as a $\mathrm{B}_I R$-module if and only if $\mathcal{J}$ is I-stable.

Proof. We omit this proof. It is largely definition-chasing. ■

We are now ready to attack the proof of the Artin–Rees lemma. Let $\mathcal{J}'$ be the induced filtration for N. From the definition, we see that $\mathrm{B}_{\mathcal{J}'} N \subseteq \mathrm{B}_{\mathcal{J}} M$ is a $\mathrm{B}_I R$-submodule. Now, $\mathrm{B}_{\mathcal{J}'} N$ is a submodule of the finitely generated module $\mathrm{B}_{\mathcal{J}} M$ under the Noetherian ring $\mathrm{B}_I R$, so we are done. ■

Here is a nice application.

Theorem 4.27 (Krull intersection)**.** Fix R a Noetherian ring with an ideal I and finitely generated module M. Then

$$N := \bigcap_{s \geq 0} I^s M$$

satisfies that there is some $x \in I$ such that $(1-r)N = 0$.

Proof. By construction, we see that $IN = N$, which in particular holds because the standard I-filtration of M is stable. Then we showed as a lemma to Nakayama's lemma back in Lemma 3.34 that there is an element $r \in I$ with $(1-r)N = 0$. ■

Corollary 4.28. Fix R a Noetherian ring with a proper ideal I. Further, if R is local or a domain, then

$$\bigcap_{s \geq 0} I^s = 0.$$

Proof. Set

$$J := \bigcap_{s \geq 0} I^s.$$

By the proof of the theorem, we get $IJ = J$, which finishes by Nakayama's lemma. When R is a domain, then the theorem gives us some $r \in I$ such that $(1-r)J = 0$, but R being a domain will force $J = 0$ from this. ■

Remark 4.29. The condition that R is Noetherian is necessary.

We close with an exercise.

Exercise 4.30. Fix R a local Noetherian ring. If $\operatorname{gr}_I R$ is a domain, then R is a domain.

Proof. The main idea is that $\operatorname{in} f = 0$ implies $f = 0$, essentially by the corollary above. ■

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.

Theorem 4.31 (Krull intersection)**.** Fix R a Noetherian ring with an ideal I and finitely generated module M. Then

$$N := \bigcap_{s \geq 0} I^s M$$

satisfies that there is some $x \in I$ such that $(1-r)N = 0$.

The Noetherian condition is necessary here; consider the following example.

Exercise 4.32. Let R be the germ 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

$$\bigcap_{s>0} (x)^s$$

is nonzero.

Proof. The point is that

$$I := \bigcap_{s>0} (x)^s$$

is the set of germs represented by a function with all derivatives vanishing. However, it is a counterexample from real analysis that e^{-1/x^2} also has all derivatives vanish but is a nonzero function. ■

4.2.2 Flat Modules

Today we are talking about flatness and Tor. Let's start with flatness; we recall the definition.

Definition 4.33 (Flat)**.** Fix R a ring. Then an R-module M is *flat* if and only if the functor $M \otimes_R -$ is exact.

Remark 4.34. 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 also had the following examples.

Example 4.35. We showed long ago that R and therefore free modules R^n are flat.

For our next example, we pick up the following definition.

Definition 4.36 (Projective)**.** An R-module P is *projective* if and only if one of the following four equivalent conditions are satisfied.

(a) The functor $\mathrm{Hom}_R(P, -)$ is exact.

(b) There exists an R-module K such that $P \oplus K$ is a free R-module.

(c) If we have a surjection $M \twoheadrightarrow M'$ and a map $P \to M'$, there is a map $P \to M$ making the following diagram commute.

$$\begin{array}{ccc} & & P \\ & \swarrow & \downarrow \\ M & \twoheadrightarrow & M'' \end{array}$$

(d) Any short exact sequence

$$0 \to A \to B \to Q \to 0$$

splits.

It is not obvious that these definitions are equivalent, but they are. For example, (a) and (c) are equivalent by writing out what the commutative diagram is asking for in terms of Hom sets. Further, (c) implies (d) by lifting from the following diagram.

$$\begin{array}{ccccccccc} & & & & & & P & & \\ & & & & & \swarrow & \| & & \\ 0 & \longrightarrow & A & \longrightarrow & B & \twoheadrightarrow & P & \longrightarrow & 0 \end{array}$$

To show that (d) implies (b), we make the short exact sequence

$$0 \to \ker \pi \to \bigoplus_{m \in M} Rm \xrightarrow{\pi} M \to 0,$$

where π is defined in the natural way. Lastly, (b) implies (a) because it gives

$$\mathrm{Hom}_R(M \oplus K, -) \cong \mathrm{Hom}_R(M, -) \oplus \mathrm{Hom}_R(K, -).$$

This more or less completes the equivalences.

Example 4.37. Projective modules are flat, which we can see from the fact that $P \oplus K$ is free and then using the fact that free modules are flat already.

Example 4.38. For any multiplicative set $U \subseteq R$, the module $R\left[U^{-1}\right]$ is flat. We showed this a long time ago. As a small aside, we note that $R\left[U^{-1}\right] \otimes -$ is a priori only exact for $R\left[U^{-1}\right]$-modules, but this restricts to R-modules just fine (even when $R \to R\left[U^{-1}\right]$ is not injective).

And let's see a non-example.

Non-Example 4.39. The $\mathbb{Z}$-module $\mathbb{Z}/n\mathbb{Z}$ is not exact. For example, we take

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

apply $- \otimes \mathbb{Z}/n\mathbb{Z}$ to get

$$0 \to \mathbb{Z}/n\mathbb{Z} \xrightarrow{\times n} \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z} \to 0,$$

but this is no longer exact at $\mathbb{Z}/n\mathbb{Z}$ term because $\xrightarrow{\times n}$ is the zero map.

4.2.3 Flatness via Algebraic Geometry

In algebraic geometry, we are interested in families of affine varieties, which consists of a base B for a family and a map $\varphi : X \to B$. As usual, the algebraic story will reverse, so the family in the algebraic world becomes a function

$$\varphi^{-1} : A(B) \to A(X).$$

In particular, this 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 $\varphi : R \to S$. As such, we have the following definition.

Definition 4.40 (Flat)**.** An R-algebra S is *flat* if and only if S is flat as an R-module.

To access flatness, we talk about fibers. In the algebraic world, the fiber of a "point" $\mathfrak{m}$ should be the ring of functions in S on the point $\mathfrak{m}$, which means we want to look at

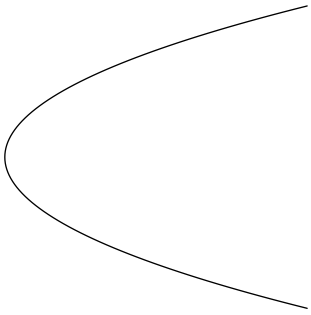
$$S/\mathfrak{m}S.$$

Flatness, roughly speaking, means that $S/\mathfrak{m}S$ varies continuously as the point $\mathfrak{m}$ moves.

Let's see some examples. We will take our base to be $B := \mathbb{A}^1(k)$ the affine line over an algebraically closed field k, which gives that $R := k[x]$.

Exercise 4.41. We consider the flatness of $S := R[x]/\left(x^2 - t\right)$ geometrically and algebraically.

Proof. This looks like the following.



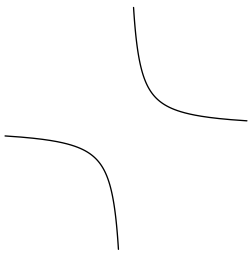
The fiber at $t = a$ as $a \in k$ varies is

$$\frac{k[x]}{(x^2 - a)} \cong \begin{cases} k^2 & a \neq 0, \\ k[x]/\left(x^2\right) & a = 0. \end{cases}$$

Visually, we can see that $a \neq 0$ has two points above it, and at $x = 0$, we are vertical. Because the dimension is constant as the point moves, we suspect S to be a flat R-algebra. And indeed, viewing $x^2 - t$ as a monic polynomial with coefficients in $R[t]$, we see that S is a free module over $R[t]$ of rank 2, so S is flat. ■

Exercise 4.42. We consider the flatness of $S := R[x]/\left(xt - 1\right)$ geometrically and algebraically.

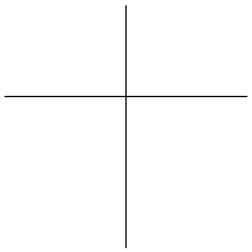
Proof. This looks like the following.



Visually, we can see that the fiber over any $t = a$ as $a \in k$ is one point, except when $a = 0$, where the fiber is empty. So we expect S to be flat, and indeed it is: $S = R\left[t^{-1}\right]$ is a localization and therefore flat. ■

Exercise 4.43. We consider the non-flatness of $S := R[x]/(tx - t)$ geometrically and algebraically.

Proof. This looks like the following.



The problem here is that the fiber is jumping at $t = 0$, so we expect S to not be flat as an R-module. For this, we have the following result.

Lemma 4.44. 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 point is to look at the short exact sequence

$$0 \to (a) \to R \to R/(a) \to 0.$$

Upon tensoring with M, we see that $(a) \otimes_R M \hookrightarrow R \otimes_R M$, so $(a)M \hookrightarrow M$. In particular, multiplication by a is injective on M, so $am = 0 = a \cdot 0$ implies $m = 0$. ■

From the above lemma, we note that $t(x - 1) = 0$ in S while t is not a zero-divisor, so S is not flat. ■

4.2.4 Homological Algebra

We will want to talk about Tor for our discussion, so we will want to talk about homological algebra.

Quote 4.45. The difference between homology and cohomology is that homology indexes like H_i, and cohomology indexes like H^i.

We will want to talk about chains in homological algebra, so we will start with complexes.

Definition 4.46 (Complex)**.** Fix $C := \oplus_{i \geq 0} C_i$ a $\mathbb{N}$-graded R-module. Then C is a *chain* if and only if it is equipped with a (graded) morphism $\partial \in \mathrm{End}_R(C)$ such that $\partial^2 = 0$. If $\deg \partial = -1$, this is homology, and if $\deg \partial = +1$, this is cohomology.

In the homology case, we can view this like

$$\cdots \xrightarrow{\partial} C_2 \xrightarrow{\partial} C_1 \xrightarrow{\partial} C_0 \xrightarrow{\partial} 0.$$

If we wanted, we could index the arrows as $\partial_i : C_i \to C_{i-1}$, but it makes things a little harder to keep track of.

Definition 4.47 (Homology)**.** Given a chain (C, ∂), we define the *homology groups* as

$$H_i(C) := \ker \partial_i / \operatorname{im} \partial_{i+1}$$

Note this is well-defined because $\partial^2 = 0$.

As usual in algebra, we will want morphisms between our objects.

Definition 4.48 (Chain morphism)**.** Fix chain complexes (C, ∂) and (C', ∂'), we define a morphism φ as a degree-0 morphism $\varphi : C \to C'$ preserving ∂ as in the following diagram.

$$\begin{array}{ccc} C_i & \xrightarrow{\partial} & C_{i-1} \\ {\scriptstyle\varphi}\downarrow & & \downarrow{\scriptstyle\varphi} \\ C_i' & \xrightarrow[\partial']{} & C_{i-1}' \end{array}$$

We can check that φ maps kernels of ∂ to kernels of ∂' and images of ∂ to images of ∂', so we get an induced map $H(\varphi) : H_i(C) \to H_i(C')$.

And because abstraction is all the rage, there is also a notion of morphisms being the same.

Definition 4.49 (Homotopically equivalent)**.** Two chain morphisms $\varphi, \psi : (C, \partial) \to (C', \partial')$ are *homotopically equivalent* if and only if there exists an R-module homomorphism $h : C \to C$ of degree 1 (i.e., $h : C_i \to C'_{i+1}$) such that $\varphi - \psi = h\partial + \partial' h$.

The image is as follows. As a warning, this diagram does not commute.

$$\begin{array}{ccccccccc} \cdots & \longrightarrow & C_2 & \longrightarrow & C_1 & \longrightarrow & C_0 & \longrightarrow & 0 \\ & & \downarrow & \swarrow^{h} & \downarrow & \swarrow^{h} & \downarrow & & \\ \cdots & \longrightarrow & C_2' & \longrightarrow & C_1' & \longrightarrow & C_0' & \longrightarrow & 0 \end{array}$$

The main point of this definition is the following.

Proposition 4.50. Suppose $\varphi, \psi : (C, \partial) \to (C', \partial')$ are homotopically equivalent. Then $H(\varphi) = H(\psi)$.

Proof. It suffices (by taking $\gamma := \varphi - \psi$) to show that if γ is homotopically equivalent to 0, then $H(\gamma)$ vanishes. Now, suppose we have any $c \in \ker \partial$, and we want to show that $\gamma(c) \in \operatorname{im} \partial'$. Well, we compute

$$\gamma(c) = (h\partial + \partial' h)(c) = \partial'(h) \in \operatorname{im} \partial',$$

so we are done. ∎

To close out class, we discuss the long exact sequence.

Theorem 4.51. Fix

$$0 \to C' \xrightarrow{\alpha} C \xrightarrow{\beta} C'' \to 0$$

a short exact sequence of complexes. Then there is a long exact sequence of homology

$$\cdots \to H_i(C') \xrightarrow{H(\alpha)} H_i(C) \xrightarrow{H(\beta)} H_i(C'') \xrightarrow{\delta} H_{i-1}(C') \to \cdots.$$

Proof. We will be very brief. The main point is the construction of δ. Fix some element $c \in \ker \partial_i''$ from $H_i(C'')$. Then we can pull it back to $\beta^{-1}(c)$ in $H_i(c)$, then push it forwards through ∂' to live in $H_{i-1}(C)$, which we can then lastly check lives in the image of α, so we finish by pulling backwards along α to get back to $H_{i-1}(C')$. ∎