250B: Commutative Algebra

Nir Elber

Spring 2022

Contents

Theme 1: Localization

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.

Integral domain

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 $b = 0$.

Units

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.

Field

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

Reduced

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

Local

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.

Ideal

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 $S \subseteq R$.

Finitely generated

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 $I = (r_1, \dots, r_n)$.

Principal

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.

Maximal

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.

Prime

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.

Principal ideal

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 smallest 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.

Irreducible, prime

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 prie ideal: $ab \in (r)$ implies $a \in (r)$ or $b \in (r)$.

This gives rise to the following important definition.

Unique factorization domain

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 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.

Ascending chain condition

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

Example 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 of 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 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. 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 $k + \ell \geq 1$. 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 $p_m \mid q_n$. But (p_m) and (q_n) are both maximal ideals, so $(p_m) \subseteq (q_n)$ 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. ∎

1.1.5 Digression on Gaussian Integers

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

Gaussian integers

Definition 1.29 (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.

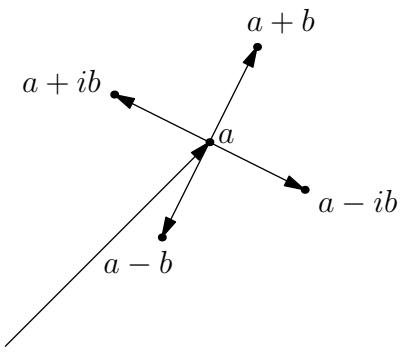
Lemma 1.30. The ring $\mathbb{Z}[i]$ is Euclidean, where our norm is $\mathrm{N}(a+bi) := a^2 + b^2$. In other words, given $\alpha, \beta \in \mathbb{Z}[i]$, we need to show that there exists $q \in \mathbb{Z}[i]$ such that

$$a = bq + r$$

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 1.31 (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 1.32. 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.

Noetherian ring

Definition 1.33 (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 1.34. 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.

- Suppos 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

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

contadicting 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. ■

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

Proposition 1.35. 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 quotienting is an algeebraic operation. In contrast, merely being a subring is less algebraic, so it is not so surpsising that $R_1 \subseteq R_2$ with R_2 Noetherian does not imply that R_1 is Noetherian.

Example 1.36. The ring $k[x_1, x_2, \ldots]$ is not Noetherian because we have th infinite ascending chain

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

Howver, $k[x_1, x_2, \ldots] \subseteq k(x_1, x_2, \ldots)$, 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 1.37 (Hilbert basis)**.** If R is a Noetherian ring, then $R[x]$ is also a Noetherian ring.

Corollary 1.38. By induction, if R is Noetherian, then $R[x_1, x_2, \ldots, x_n]$ is Notherian for any finite n.

Warning 1.39. 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 1.37. 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 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 gauarnteed 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.

Module

Definition 1.40 (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 1.41. Any ideal $I \subseteq R$ is an R-module. In fact, ideals exactly correspond to the R-submodules of R.

Example 1.42. 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.

Noetherian module

Definition 1.43 (Noetherian module)**.** We say that an R-module M is *Noetherian* if and only if all R-submodules of M are finitely generated.

Remark 1.44. 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 1.34.

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 1.45. 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 1.35.[1] ■

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

Proposition 1.46. 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 1.45. Anyways, the point is that M is the quotient of a Noetherian ring and hence Noetherian by Proposition 1.45 (again). ■

Here is the analogous result for algebras.

Algebra

Definition 1.47 (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 1.48. 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 a $R[x_1, \dots, x_n]$, which is Noetherian by Corollary 1.38, so S is Noetherian as well. ■

[1] In fact, Proposition 1.35 is exactly this in the case where $B = R$.

1.1.8 Invariant Theory

In our 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 1.49 (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 1.50 (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 1.51. 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 1.52. 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.

Reynolds operator

Definition 1.53 (Reynolds operator)**.** Fix everything as above. Then, given $f \in R$, we define the *Reynolds operator* $\varphi : R \to R$ as

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

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

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

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

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

Certainly we have $\supseteq$ here. For $\subseteq$, we show that any $f \in R^G$ lives in $k[f_1, \dots, f_n]$ 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 $f \in k \subseteq k[f_1, \dots, f_n]$. 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 $g_i \in k[f_1, \dots, f_n]$, and hence $f \in k[f_1, \dots, f_n]$ 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 $\varphi(g_i) \in k[f_1, \dots, f_n]$, and hence $f \in k[f_1, \dots, f_n]$ by summation. This finishes. ∎

The main example here is as follows.

> **Exercise 1.54.** Let S_n act on $R := k[x_1, \dots, x_n]$ as follows: $\sigma \in S_n$ acts by $\sigma x_m := x_{\sigma m}$. Then we want to describe R^G, the *homogeneous polynonmials 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

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

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

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

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 1.55. 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.

Affine space

Definition 1.56 (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.

Algebraic

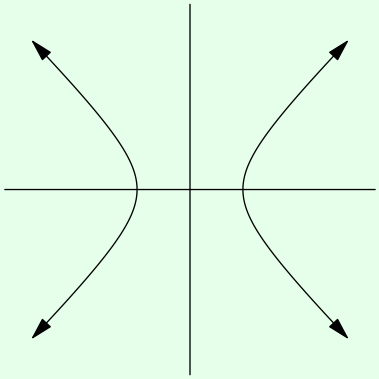
Definition 1.57 (Algebraic)**.** A subset $X \subseteq \mathbb{A}^n(k)$ is (affine) *algebraic* if and only if it is the set of solutions to some system of polynomials equations $f_1, \ldots, f_n \in k[x_1, \ldots, x_d]$.

[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 1.58. 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 1.59. The set $\varnothing \subseteq \mathbb{A}^1(\mathbb{R})$ is algebraic becasue 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 1.60. 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 1.61. 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.

$I(X)$

Definition 1.62 ($I(X)$)**.** 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.

Radical

Definition 1.63 (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.

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

Example 1.64. 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 $I \subsetneq \operatorname{rad} I$.

Here is an alternative characterization of being radical.

Lemma 1.65. 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 of the machinery we have in place, we can now state the idea of Hilbert's Nullstellensatz.

Theorem 1.66 (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.

$Z(I)$

Definition 1.67 ($Z(I)$)**.** 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 will may focus on the case where S is an ideal.

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

Theorem 1.68 (Nullstellensatz, II)**.** Fix k an algebraically closed field. Then for ideals $I \subseteq k[x_1, \ldots, x_n]$, we have

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

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

Remark 1.69. Yes, it is important that k is algebraically closed here. Essentially this comes from Example 1.59: 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 1.70. 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 1.71 (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.

Zariski topology, I

Definition 1.72 (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 1.73 (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. In fact, 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 $X(S)$ for given subsets $S \subseteq \mathcal{S}$ of $k[x_1, \dots, x_n]$, we note

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

  so the union is in fact an algebraic set.

- Finite unions of closed sets are closed: given algebraic sets $X(S_1), \dots, X(S_n)$, we note

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

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 $X(S_i)$ 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 1.74. 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 $1 \in \sum I$.

However, we can reduce this to a finite condition: $1 \in \sum_I$ 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.

Coordinate ring

Definition 1.75 (Coordinate ring)**.** Given an algebraic set $X \subseteq \mathbb{A}^n(k)$, we define the *coordinate ring* on X as

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

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 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 subsubsection.

Corollary 1.76. A system of polynomial equations

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

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

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

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 $p_1, \dots, p_n \in k[x_1, \dots, x_n]$ 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 $Z((f_1, \dots, f_r)) = \varnothing$, so

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

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 1.77. 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 1.78. 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 1.79. 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 alreadys 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 1.79 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 1.79 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 1.71. 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 $\mathfrak{m}_a$ 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.

  Thus, set $Z(I) = \{a\}$; note $a \in X$ because $I(X) \subseteq I$ (by Remark 1.71 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 only the 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 $A(Y)$ arre 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 1.80. 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.

Spectrum of a ring

Definition 1.81 (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.

Zariski topology, II

Definition 1.82 (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 1.83 (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 1.84. 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 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
$$(\operatorname{Spec} R \setminus X(I)) \cap (\operatorname{Spec} R \setminus X(J)) = \varnothing,$$
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
$$X\left(\sum_{I \in \mathcal{S}} I\right) = \bigcap_{I \in \mathcal{S}} X(I) = \varnothing.$$

[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 $I \subseteq \mathfrak{p}$.

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 varities, we need to define projective space first.

Projective space

Definition 1.85 (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

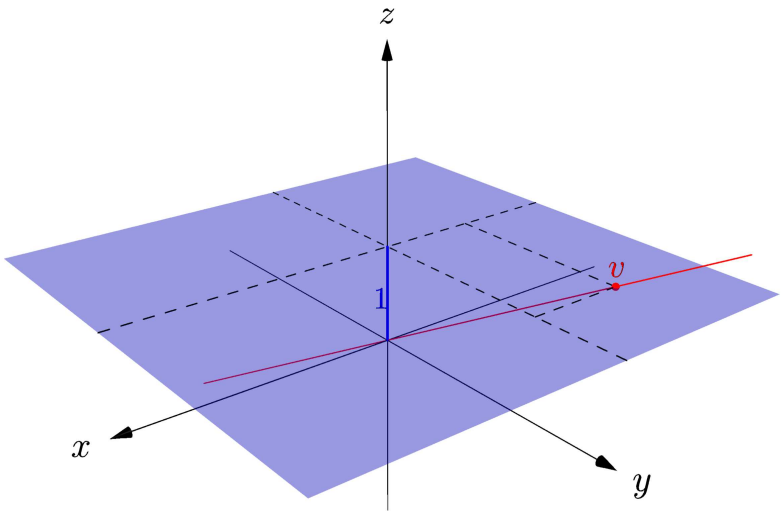
$$(a_0 : a_1 : \ldots : a_n) \in \mathbb{P}^n(k)$$

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,

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

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 the constant factors allowed to wiggle, we see that we really should only be looking at homogeneous equations. More concretely, if $f \in k[x_0, \dots, x_n]$, we want

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

to be unambiguous, so $f(a_0, \dots, a_n) = 0$ should be imply $f(ca_0, \dots, ca_n) = 0$ 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

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

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

Projective variety

Definition 1.86 (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 $k[x_0, \dots, x_n]$.

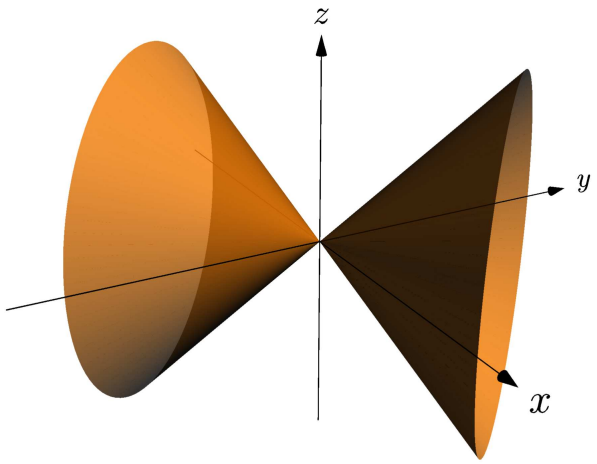
Here is an example.

Exercise 1.87. 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.

Graded ring

Definition 1.88 (Graded ring)**.** A ring R is *graded* by the abelian groups $R_0, R_1, \dots$ 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 1.89 (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 disjointness. 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 1.90. The ring $R = k[x_1, \dots, x_n]$ is "graded by degree" by setting R_d to be the space of all homogeneous n-variable polynomials of degree d (unioned with $\{0\}$).

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

Graded ideal

Definition 1.91 (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., $(x_0, x_1, \dots) \mapsto x_0 + x_1 + \cdots$).

Example 1.92. Given the graded ring $R = R_0 \oplus R_1 \oplus R_2 \oplus \cdots$, the ideal

$$I := R_1 \oplus R_2 \oplus R_3 \oplus \cdots$$

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

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

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.

Graded module

Definition 1.94 (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 1.95. 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 1.48. For the forwards direction, take $R = R_0 \oplus R_1 \oplus \cdots$ a Noetherian, graded ring. We note that quotienting R 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 $I := (r_1, \ldots, r_N)$. We claim that

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

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

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

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

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

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

1.2.8 The Hilbert Function

For this subsection, let $R := k[x_0, \ldots, x_n]$ (note the zero-indexing!) be a ring graded by degrree, 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.

Hilbert function

Definition 1.96 (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 1.97. 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 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 1.98. 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 $-\infty \leq -1$ for sufficiently large inputs.

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

Twist

Definition 1.99 (Twist)**.** Given a graded R-module M, we define the dth *twist* $M(d)$ of M to be the same underlying module but with grading given by

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

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

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

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

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

We do take a moment to remark $M/x_r M$ 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 $M \twoheadrightarrow M/x_n M$ 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 $x_n M_{d-1} \subseteq M_d$.

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 $x_r M_{d-1} \subseteq M_d$. So instead we have to write down

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

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

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

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

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

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

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

We can rewrite this as

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

so we see that the first finite difference of H_M agrees with $H_{M/x_n M}(d) - H_K(d-1)$, 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 1.100 (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 1.98 justifies the following definition.

Hilbert polynomial

Definition 1.101 (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 1.98 is called the *Hilbert polynomial* of M.

Remark 1.102. 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 1.103. Take $M := k[x, y, z]/\left(x^2 + y^2 + z^2\right)$ as a $R := k[x, y, z]$-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 $\dim M_0 = 1$.
- 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 $\dim M_1 = 3$.
- We see R_2 has basis $\left\{xy, yz, zx, x^2, y^2, z^2\right\}$, 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

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

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 1.97 is $\binom{n+2}{2} - \binom{n}{2} = \frac{n^2+3n+2}{2} - \frac{n^2-n}{2} = 2n + 1$. ∎

Remark 1.104. 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 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 1.105 (Eisenbud 1.19)**.** Define $M := k[x,y,z]/\left(xz-y^2, yx-z^2, xw-yz\right)$ as a $R := k[x,y,z]$-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.

1.3 January 25

Today we localize.

1.3.1 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 1.106. 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 possile 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 $I \subseteq k[x_1,\dots,x_n]$, 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."

1.3.2 Localization of Rings

Let's build towards the definition of localization.

Multiplicatively closed

Definition 1.107 (Multiplicatively closed)**.** Fix R a ring. Then a subset $U \subseteq R$ is *multiplicatively closed* 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 closd if and only if $1 \in U$ and for $x, y \in U$ to imply $xy \in U$.

Remark 1.108. 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.

Localization, rings

Definition 1.109 (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 1.110 (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 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 1.111. 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.

Multiplicative closure

Definition 1.112 (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.

Localization, again

Definition 1.113 (Localization, again)**.** Fix R a ring and $U \subseteq R$ an arbitrary subset. Then we define $R\left[U^{-1}\right] := R\left[\overline{U}^{-1}\right]$.

1.3.3 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.

Field of fractions

Definition 1.114 (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 1.115. We have that $K(\mathbb{Z}) = \mathbb{Q}$.

Example 1.116. 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.

Localization at a prime

Definition 1.117 (Localization at a prime)**.** Fix R a ring and $\mathfrak{p} \subseteq R$ a prime ideal. Then $R \setminus \mathfrak{p}$ is 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 1.118. When R is an integral domain, (0) is prime, and $R_{(0)} = K(R)$.

Example 1.119. 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 1.120. 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 tht $\mathfrak{p}R_{\mathfrak{p}}$ 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 1.121. 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.

Residue field

Definition 1.122 (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 1.123. We have that $\mathbb{Z}_{(p)}/p\mathbb{Z}_{(p)} \cong \mathbb{Z}/p\mathbb{Z}$. In particular, observe that the characteristic has changed.

Remark 1.124. 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 $\mathfrak{p}$. Hence 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 1.125. 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. ■

1.3.4 Localization of Modules

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

Localization, modules

Definition 1.126 (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 1.110 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 1.127. Fix an R-module M and $U \subseteq R$ a multiplicatively closd 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 1.128. If $0 \in U$, then all of R lives in the kernel of the canonical map $R \to R\left[U^{-1}\right]$.

Example 1.129. 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 $r = 0$.

1.3.5 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 $\varphi^{-1}(J) \subseteq R$.[4]

Remark 1.130. 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 1.131. 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 1.132. 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.

We now 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 $R\left[U^{-1}\right]$.

[4] 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 a $R\left[U^{-1}\right]$-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 1.133. 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 a $R\left[U^{-1}\right]$-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 1.132, 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 1.134. 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 1.133, 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 1.135. 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. ∎

1.3.6 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 1.136. 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.

Hom

Definition 1.137 (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.

End

Definition 1.138 (End)**.** Fix R a ring. Then we define the *endomorphisms* of an R-module 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 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 of 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 1.139. 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.

1.3.7 Tensor Product

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

Bilinear

Definition 1.140 (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.

Tensor product

Definition 1.141 (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 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 1.142. 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 $m \mapsto m \otimes 1$.
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.

Here are some example applications.

Exercise 1.143. 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 1.144. 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 1.145. 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 discusion of localization.

1.4 January 27

We localize more.

1.4.1 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 1.146. 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 injectivem ruining exactness at the front, and this is the only obstruction by right-exactness.

Example 1.147. 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

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

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.

Flat

Definition 1.148 (Flat)**.** Fix R a ring. Then an R-module M is *flat* if and only if the functor $M \otimes_R -$ is exact.

Remark 1.149. 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 1.150. 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 1.151. 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.

1.4.2 Localization via Tensoring

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

Proposition 1.152. 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 explcitly. 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

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

  which is what we wanted.

In the other direction, we note that we have a 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 $\frac{r_1 m}{u_1} = \frac{r_2 m}{u_2}$. 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

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

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 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 1.153. 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 1.154. 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. ∎

1.4.3 Localization via Flatness

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

Proposition 1.155. 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 1.153.)

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

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

$$\varphi(a) = \overline{\varphi}(a) = \overline{\varphi}\left(u \cdot \frac{a}{u}\right) = u \cdot \overline{\varphi}\left(\frac{a}{u}\right) = 0.$$

Because $\ker \varphi$ is trivial, we are forced to $a = 0$, so $\frac{a}{u} = 0$, so indeed $\ker \overline{\varphi}$ is trivial. ■

Corollary 1.156. Fix R a ring and $U \subseteq R$ a multiplicatively subset. Then $R\left[U^{-1}\right]$ is flat as an R-module.

Proof. The commutative diagram in the proof of Proposition 1.155 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 1.157. 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/isomorphc.

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 1.158. 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 of M.

Proof. The main point is that intersecitons 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 1.154 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 1.154, 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 $\frac{M}{M_i}\left[U^{-1}\right] \cong \frac{M\left[U^{-1}\right]}{M_i[U^{-1}]}$ by $\frac{1}{u}[x]_{M_i} \mapsto \left[\frac{x}{u}\right]_{M_i[U^{-1}]}$. Stitching these isomoprhisms 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 $\left(\left[\frac{x_k}{u}\right]_{M_i[U^{-1}]}\right)_{i=1}^n$.

Only now we do localize $(*)$. Upon localization, we get the left-exact sequence[5]

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

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

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

[5] 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 $0 \to A \to B \to \mathrm{im}(B \to C) \to 0$.

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 interseciotns.

Example 1.159. 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,

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

1.4.4 Tensor–Restriction Adjunction

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

Restriction

Definition 1.160 (Restriction)**.** Fix S an R-algebra, which means we are promised a ring homomorphism $\psi : R \to S$. Given an S-module M, we can give M an R-action by

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

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

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

Lemma 1.161. Fix S an R-algebra. Then the map $\operatorname{Res}_R^S : \operatorname{Mod}_S \to \operatorname{Mod}_R$ is a functor.

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

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

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

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

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

In the other direction, if N is an R-module, we can create an S-module the "induced" module $\mathrm{Ind}_R^S N := S \otimes_R N$, 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 1.162. 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)

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

Proof. We construt forwards and backwards maps manually.

- Fix $f \in \mathrm{Hom}_R(M, \mathrm{Res}_R^S N)$. 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 $f, g \in \mathrm{Hom}_R(M, \mathrm{Res}_R^S N)$ and $s \otimes m \in S \otimes_R M$ so that
$$\widetilde{f + g}(s \otimes m) = s(f + g)(m) = sf(m) + sg(m) = (\widetilde{f} + \widetilde{g})(s \otimes m).$$
  - Injective: we show $f \mapsto \widetilde{f}$ has trivial kernel. Indeed, suppose $f \in \mathrm{Hom}_R(M, \mathrm{Res}_R^S N)$ has $\widetilde{f} = 0$. Then, for any $m \in M$, we see
$$f(m) = 1_S f(m) = \widetilde{f}(1_S \otimes m) = 0.$$
- In the other direction, motivated by the above injectivity check, we notice that we have an R-module map $\iota : M \to S \otimes_R M$ by $m \mapsto 1_S \otimes m$. Indeed, for $r_1, r_2 \in R$ and $m_1, m_2 \in M$, we see
$$\iota(r_1 m_1 + r_2 m_2) = 1_S \otimes (r_1 m_1 + r_2 m_2) = r_1 \iota(m_1) + r_2 \iota(m_2).$$
Now, suppose that we have some $g \in \mathrm{Hom}_S(S \otimes_R M, N)$. 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 greanted the map $g \mapsto g \circ \iota$ from $\mathrm{Hom}_S(S \otimes_R M, N)$ to $\mathrm{Hom}_R(M, \mathrm{Res}_R^S N)$.

Note that it merely remains to check the surjectivity of $f \mapsto \widetilde{f}$, so it suffices to show that, for any $g \in \mathrm{Hom}_S(S \otimes_R M, N)$, 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 1.163. 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.

1.4.5 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 1.164. 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 1.162. 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 1.162 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 1.162 and γ through. Namely, 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 1.165 (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.

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

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 1.166. Work in the set-up of Lemma 1.164. If $M = R^n$ for some positive integer n, then α is an isomorphism.

Proof. We proceed by brute force. We will just show directly that $S \otimes_R \operatorname{Hom}_R(R^n, N) \cong \operatorname{Hom}_S(S \otimes_R R^n, S \otimes_R N)$, and tracking the isomorphism through will reveal that it is α. Pick up some $s \otimes f \in S \otimes_R \operatorname{Hom}_R(R^n, N)$ which we will track through.

- Note that $S \otimes_R \operatorname{Hom}_R(R^n, N) \cong S \otimes_R \operatorname{Hom}_R(R, N)^n \cong S \otimes_R N^n$ by sending $s \otimes f$ to $s \otimes (1_R \mapsto f(e_k))_{k=1}^n$ to $s \otimes (f(e_k))_{k=1}^n$.
  (Here, the $e_\bullet$ are the basis for R^n.)
- Note that $S \otimes_R N^n \cong (S \otimes N)^n$ by sending $s \otimes (f(e_k))_{k=1}^n$ to $(s \otimes f(e_k))_{k=1}^n$.
- Note that $(S \otimes_R N)^n \cong \operatorname{Hom}_S(S^n, S \otimes_R N)$ by sending $(s \otimes f(e_k))_{k=1}^n$ to the morphism
$$(s_k)_{k=1}^n \mapsto \sum_{k=1}^n ss_k \otimes f(e_k).$$
- Note that $\operatorname{Hom}_S(S^n, S \otimes_R N) \cong \operatorname{Hom}_S((S \otimes_R R)^n, S \otimes_R N)$ by sending the morphism $(s_k)_{k=1}^n \mapsto \sum_k ss_k \otimes f(e_k)$ to the morphism defined by $(s_k \otimes 1)_{k=1}^n \mapsto \sum_k ss_k \otimes f(e_k)$.
  In particular, the morphism in the codomain is
$$(s_k \otimes r_k)_{k=1}^n \mapsto \sum_{k=1}^n ss_k \otimes f(r_k e_k).$$
- Note that $\operatorname{Hom}_S((S \otimes_R R)^n, S \otimes_R N) \cong \operatorname{Hom}_S(S \otimes R^n, S \otimes_R N)$ by sending $(s_k \otimes r_k)_{k=1}^n \mapsto \sum_k ss_k \otimes r_k f(e_k)$ to
$$s_0 \otimes (r_k)_{k=1}^n \mapsto \sum_{k=1}^n ss_0 \otimes f(r_k e_k) = ss_0 \otimes f\left((r_k)_{k=1}^n\right).$$

So indeed, we have tracked our isomorphism, and we can see from the last point that $s \otimes f$ has gone to $s_0 \otimes m \mapsto ss_0 \otimes f(m)$, as needed by α. ∎

We would like to extend the above argument to work more generally, but this will require some hypotheses. One condition will be that S is flat over R; for the other condition we have the following definition.

Finitely presented

Definition 1.167 (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 1.168. The free R-module R^n is finitely presented due to the sequence $0 \to R^n \to R^n \to 0$.

Example 1.169. 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 1.46), so the R-submodule $\ker \varphi \subseteq R^n$ will be finitely generated over R. Thus, M is finitely presented.

Now, here is the culmination of base change.

Proposition 1.170. Work in the set-up of Lemma 1.164. Then if S is flat and M is finitely presented, then the α from Lemma 1.164 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 1.166.

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 1.165) 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 1.166, so the leftmost α is also an isomorphism. This finishes. ∎

Remark 1.171 (Nir)**.** I am really proud of the working out of the discussion in this subsection. There are a lot of moving parts.

1.4.6 Support of a Module

We have the following definition.

Support

Definition 1.172 (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.

Annihilator

Definition 1.173 (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 1.174. 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 characerization of $\operatorname{Supp} M$.

Proposition 1.175. 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 1.176. 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 1.175 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 1.177. 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 1.178. 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 1.175 that $\operatorname{Supp}(0) = \varnothing$ because no prime contains R.

To set up our last example, we have the following definition and then statement.

Simple

Definition 1.179 (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 1.180. 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 1.176 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 1.181. 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 $M = R/\mathfrak{m}$.

1.4.7 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 1.182. 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 1.183. 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 1.154, 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. ■

Additinally, we can learn something from the module itself by studying the support.

Proposition 1.184. Fix an R-module M. Then $M = 0$ if and only if $M_{\mathfrak{m}} = 0$ for all maximal ideals $\mathfrak{m} \subseteq R$. In particular,

Proof. We have already discussed the forwards direction in Example 1.178. In the other direction, supose 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 1.175, 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 1.185. 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 1.175, there is some m so that

$$\operatorname{Ann} m \subseteq \mathfrak{p}.$$

Placing $\mathfrak{p}$ inside of 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 1.186. Fix $\varphi : M \to N$ an R-module homomorphism and $\mathfrak{m} \subseteq R$ a maximal ideal. Then we are promised a localized map $\varphi_{\mathfrak{m}} : M_{\mathfrak{m}} \to N_{\mathfrak{p}}$. 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 1.157. 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 $\mathfrak{m}$.

Repeatig 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. ■

We continue our fact-collection.

Proposition 1.187. 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 1.175). 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 1.175 that $\mathfrak{p} \notin \operatorname{Supp}(M \otimes_R N)$. ∎

Remark 1.188. 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 here because I am under the impression that it is difficult.

Example 1.189. 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 1.175 that $\operatorname{Supp} \mathbb{Q} = \operatorname{Spec} R$. On the other hand, $\operatorname{Ann} \mathbb{Z}/2\mathbb{Z} = (2)$, so Proposition 1.176 gives $\operatorname{Supp} \mathbb{Z}/2\mathbb{Z} = \{(2)\}$. Thus,

$$\operatorname{Supp}(\mathbb{Q} \otimes_{\mathbb{Z}} \mathbb{Z}/2\mathbb{Z}) = \varnothing \subsetneq \{(2)\} = \operatorname{Supp} \mathbb{Q} \cap \operatorname{Supp} \mathbb{Z}/2\mathbb{Z}.$$

1.4.8 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 1.190. If we have two free k-algebras $k[x_1, \dots, x_n]$ and $k[y_1, \dots, y_m]$, then we claim that

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

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 1.145, 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 of 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 1.191. 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 1.192. 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 1.190, 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 isomorphsm. 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 tht $\overline{\psi} \circ \overline{\varphi}$ induces the identity on all of $A(X \times Y)$. This finishes. ■

Remark 1.193 (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 1.190 to show that $\overline{\varphi}$ is well-defined.

Remark 1.194. One can generalize this construction to fiber products.

Next class we will finish up localization by discussing modules of finite length.

1.5 February 1

Hopefully we finish localizing today.

1.5.1 A Little On Tensor Products

Let's start with some review exercises.

Proposition 1.195. 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

$$(R/I) \otimes_R M \cong M/IM.$$

canonically.

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

$$I \otimes_R M \cong \{rm : r \in I \text{ and } m \in M\} = IM.$$

So we are promised the right-exact sequence

$$IM \to M \to (R/I) \otimes_R M \to 0,$$

which gives the desired isomorphism. ∎

Remark 1.196 (Nir)**.** As usual, this isomorphism is functorial in M.

Corollary 1.197. 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 conclude

$$(R/I) \otimes_R (R/J) \cong \frac{R/J}{I(R/J)} \cong \frac{R/J}{(I+J)/J} \cong \frac{R}{I+J}.$$

This finishes. ∎

The above result could be used for fun and profit on the homework.

Remark 1.198. Professor Serganova does not care too much about noncommutative rings in this class.

We also have the following "change of constants" results.

Proposition 1.199. Fix S an R-algebra. Then, given S-modules A and B and C, we have

$$(A \otimes_R B) \otimes_S C \simeq A \otimes_R (B \otimes_S C).$$

Proof. The isomorphism is by $(a \otimes b) \otimes c \mapsto a \otimes (b \otimes c)$. ∎

Proposition 1.200. 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,

$$\begin{aligned}(S \otimes_R M) \otimes_S (S \otimes_R N) &\cong (M \otimes_R S) \otimes_S (S \otimes_R N) \\ &\cong (M \otimes_R (S \otimes_S (S \otimes_R N))) \\ &\cong (M \otimes_R ((S \otimes_S S) \otimes_R N)) \\ &\cong (M \otimes_R (S \otimes_R N)),\end{aligned}$$

which becomes $S \otimes_R (M \otimes_R N)$ after more association. ■

1.5.2 Artinian Rings

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

Artinian module

Definition 1.201 (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 1.202. 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 1.203. 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 1.204. More generally, any finite-dimensional k-algebra is an Artinian ring.

Example 1.205. 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 1.45.

Proposition 1.206. 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 1.45. ■

1.5.3 Composition Series

The main character in our story on Artinian rings will be the "module of finite length."

Composition series

Definition 1.207 (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.

Length

Definition 1.208 (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.

Finite length

Definition 1.209 (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 1.210. 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 legnth. ∎

Non-Example 1.211. 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 1.212. 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 a 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[6]
$$\frac{A \cap B_k}{A \cap B_{k+1}} \cong \frac{(A \cap B_k) + B_{k+1}}{B_{k+1}},$$
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[7]
$$\frac{(B_k + A)/A}{(B_{k+1} + A)/A} \cong \frac{B_k + A}{B_{k+1} + A}.$$
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 thereofre 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. ∎

[6] 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 $A \cap B_k$.

[7] 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 1.213 (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 1.214. 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. ∎

1.5.4 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 1.212; we will use it as a technical lemma in the proof.

Lemma 1.215. 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 1.212, 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 of the 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 redundences 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 1.216 (Jordan–Hölder)**.** Fix M an R-module which has a composition series. Then all composition series of M have the same length. Namelt, any strictly descending chain of submodules of M can be refined into a composition series of length equal to the length of M.

Proof. Omitted. This is Eisenbud and in fact essentially the same as the proof for groups if one has seen the corresponding proof for groups. ■

1.5.5 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 1.217. Fix M an R-module. Them M is of finite length if and only if M is both Artinian and Noetherian.

Proof. We will be brief; the backwards direction is Lemma 1.210. For the forwards direction, suppose M has a composition series with n composition factors. The point is that composition series are maximal among all chains of distinct submodules, so any chain of submodules can have at most $n+1$ distinct submodueles. In particular, any ascending or descending chain must stabilize. ■

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 1.218. Fix M an R-module with a finite composition series

$$M := M_0 \supsetneq M_1 \supsetneq \cdots \supsetneq M_0 := \{0\}.$$

Then $\operatorname{Supp} M$ is the composition factors.

Proof. The point is to turn the composition series into a whole bunch of short exact sequence, from which we can read off the support. Namely, we have the short exact sequences

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

from which we can read off the support inductively. ■

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

Theorem 1.219. Fix M a 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 computatin. ■

1.5.6 Artinian Grab-Bag

We are now able to give the following classification.

Theorem 1.220. 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 1.220. Suppose R is neither Artinian nor Noetherian. It will suffices 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 1.206. 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 1.221. 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, $\varphi(r_1 x_1 + r_2 x_2) = ar_1 x_1 + ar_2 x_2 = r_1 \varphi(x_1) + r_2 \varphi(x_2)$. 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 maximlity 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 1.220. For the other direction, we note that we can show all primes are maximal without tears.

Lemma 1.222. 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.

Jacobson radical

Definition 1.223 (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

$$R \to \prod_{\mathfrak{m}} R,$$

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 1.224. 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.

Indeed this chain is infinite, and to see that it is a composition series, we have to check that

$$\frac{\mathfrak{m}_1 \cap \cdots \mathfrak{m}_k}{\mathfrak{m}_1 \cap \cdots \mathfrak{m}_k \cap \mathfrak{m}_{k+1}}$$

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.

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

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 1.181. ∎

Remark 1.225. 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 1.226 (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 1.220. The main idea is to try to make Lemma 1.224 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 1.227 (Serganova)**.** Here is alternate motivation for the below claim: the payoff to Lemma 1.224 is that the Chinese remainder theorem gives us right-exactness of the short exact sequene

$$0 \to J \to R \to \prod_{\mathfrak{m}} R/\mathfrak{m} \to 0.$$

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 1.228. Fix R an Artinian ring. Then the Jacobson radical J is nilpotent.

Proof. Observe that we have a descending chain

$$J \supseteq J^2 \supseteq J^3 \subseteq \cdots,$$

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 Zorn's lemma 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 1.224, 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 1.214, 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.[8] This finishes. ∎

1.5.7 Geometry of Artinian Rings

While we're here, we provide some more nice facts.

Proposition 1.229. 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 1.230. Fix $I \subseteq k[x_1, \ldots, x_n]$. Then the following are equivalent.

- The ring $R := k[x_1, \ldots, x_n]/I$ is Artinian.
- The set $Z(I) \subseteq \mathbb{A}^n(k)$ is finite.
- The ring R is a finite-dimensional k-algebra.

Proof. Omitted. See Eisenbud. ∎

1.5.8 The Radical, Returned

And we end our discussion with the following miscellaneous result.

Proposition 1.231. 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.

Proof. The main point is the following lemma.

[8] 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.

Lemma 1.232. 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 $I \subseteq \mathfrak{p}$.[9]

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

$$\langle a \rangle := \{a^n : n \in \mathbb{N}\}.$$

Indeed, such an ideal $\mathfrak{p}$ by the discussino 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 1.233. 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 1.231, 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. ■

[9] This set is nonempty because $I \cap U = \varnothing$ and $I \subseteq I$. All ascening chains have an upper bound by taking the union along the chain.