COURSE NOTES FOR MATH 2520 GRADUATE ALGEBRA

MELODY CHAN

Contents

Date: March 15, 2023.

These are course notes for a second semester graduate algebra course taught at Brown University.

Part 1. Some category theory

1. Category theory basics

Just like mathematics itself, a little bit goes a long way. Source: Riehl p. 3 (modern, great, free), Maclane (old school).

Definition 1.1. A *category* $\mathcal{C}$ is

(1) a collection of *objects* $X, Y, Z, \ldots$
(2) a collection of *morphisms* $f, g, h, \ldots$
(3) for each morphism f a specification of objects X and Y, called *domain* and *codomain*, written $f\colon X \to Y$,
(4) for any pair $f\colon X \to Y$ and $g\colon Y \to Z$, the specification of a morphism $X \to Z$ denoted $g \circ f$ or gf,

such that

- (associativity)
- (existence of identity), denoted $1_X\colon X \to X$ for each object X

Definition 1.2. A morphism $f\colon X \to Y$ is called an *isomorphism* if there is a $g\colon Y \to X$ such that $gf = 1_X, fg = 1_Y$. An isomorphism $X \to X$ is called an automorphism.

Why *collections*? We are tiptoeing around set-theoretic issues e.g., Russell's paradox invoking the set of sets. I will sweep all set-theoretic issues under the rug. But sometimes we are safe:

Definition 1.3. A category $\mathcal{C}$ is called *small* if the collection of morphisms forms a set ("only" a set's worth of morphisms). Weaker, true of most examples of interest to us: $\mathcal{C}$ is *locally small* if for all X, Y, the morphisms $X \to Y$ form a set, denoted $\mathrm{Mor}_{\mathcal{C}}(X, Y)$ or $\mathcal{C}(X, Y)$.

The objects of a small category then form a set too, since objects are in correspondence with the identity morphisms. I am likely to talk about categories as if they were locally small, without further mention.

Example 1.4. Discuss objects, morphisms, isomorphisms. The study of these categories is set theory, linear algebra, group theory, topology. Can skip since Tom did examples

(1) **Set**, **Ens**
(2) $\mathbf{Vect}_k$
(3) **Gp**
(4) **Top**. Isomorphisms are homeomorphisms. Now homeomorphisms make more sense!
(5) **ComRing**. Commutative rings. All my rings have identity element, but 0 ring is not excluded. A morphism/homomorphism is a map $f\colon R \to S$ with
$$f(r + r') = f(r) + f(r'),\ f(rr') = f(r)f(r'),\ f(1_R) = f(1_S)$$
(6) **Fd**. Fields. Here let us agree once and for all that a *field* is defined as a commutative ring in which the nonzero elements form a group. Therefore, the 0 ring is not a field. A morphism of fields is just a ring homomorphism in which source and target happen to be fields.

Here are some more exotic examples close to my heart:

(6) A poset $(P, \leq)$ is a set P and a *partial order* $\leq$, meaning a binary relation satisfying
   - $x \leq x$,
   - $x \leq y$ and $y \leq z$ implies $x \leq z$,
   - $x \leq y$ and $y \leq x$ implies $x = y$.

   Examples: $(\mathbb{Z}, \leq)$, $(\mathbb{Z}, \text{divisibility})$. Draw a picture of Hasse diagram.

   Then view $(P, \leq)$ as a category with objects P and a unique morphism $x \to y$ whenever $x \leq y$.
(7) Groupoids? Get a groupoid from any category by "erasing" non-isomorphisms.
(8) Special case of both: given any set S, regard S as category with objects elements in S and only identity morphisms.

(9) **FI** Finite sets, injections. Popular these days.

2. New categories from old.

Definition 1.5. Let $\mathcal{C}$ be a category.

(1) The opposite category $\mathcal{C}^{\mathrm{op}}$ has same objects, and a morphism $f^*\colon X \to Y$ for every morphism $f\colon X \to Y$ in $\mathcal{C}$, with composition

$$f^* \circ g^* = (g \circ f)^*$$

for $f\colon X \to Y, g\colon Y \to Z$. ("Reverse all arrows")

(2) Slice category: for X an object, the category $(\mathcal{C} \downarrow X)$ has objects resp. morphisms

$$\begin{array}{ccc} Z & & Z \longrightarrow Z' \\ \downarrow{\scriptstyle \phi} & & {\scriptstyle \phi}\searrow \quad \swarrow{\scriptstyle \phi'} \\ X & & X \end{array}$$

("Do everything above X.") The coslice category $(X \downarrow \mathcal{C})$, with objects $X \to Z$, is defined analogously.

3. Initial and final objects

Definition 1.6. Initial, final. Zero object.

Example 1.7.

(1) **Set** has $\emptyset$ initial, singleton sets final.
(2) **ComRing** has $\mathbb{Z}$ initial, 0 final.
(3) **AbGp** has 0 initial and final, hence 0 is a zero object.

Remark 1.8. Initial (resp final) objects are *unique up to unique isomorphism.* What does this mean? It means that given any two initial objects X, X', there is a unique isomorphism $X \to X'$.

Proof. Prove it. □

I used to think that using this phrase was a sign of being uptight, but I've completely changed my mind (or, maybe, I have become uptight). Example: When people say informally "There is a unique group of order three," what do they really mean? They mean "...up to isomorphism." But there is a unique group of order three only up to *nonunique* isomorphism. (Think.) Compare with: there is a unique group of order 2 *up to unique isomorphism.*

Example 1.9. You learned about the product $X \times Y$ in $\mathcal{C}$. The product, if it exists, is *unique up to unique isomorphism*: either argue this directly, or invoke that the product is final in a particular category—which?

4. Functors.

Tom says he covered it, so just review/set notation.

Definition 1.10. Define (covariant) functor $F\colon \mathcal{C} \to \mathcal{D}$: an object FX in $\mathcal{D}$ for each X in $\mathcal{C}$, and a morphism $Ff\colon FX \to FY$ for each $f\colon X \to Y$ in $\mathcal{C}$, satisfying $F(gf) = FgFf$ and $F1_X = 1_{FX}$.

Then a contravariant functor from $\mathcal{C}$ to $\mathcal{D}$ is $F\colon \mathcal{C}^{\mathrm{op}} \to \mathcal{D}$.

Example 1.11. Fundamental group of a based topological space.

Example 1.12. Optional example: Let X a topological space. Define

$$\mathrm{Conf}(X)\colon \mathbf{FI}^{\mathrm{op}} \to \mathbf{Top}$$

$$\mathrm{Conf}(X)(\{1,\dots,n\}) = \mathrm{Conf}_n(X) = X^n \setminus \text{fat diagonals}$$

(Should define slightly more generally, for S finite set.)

5. Adjoint pairs.

Consider the following:

> "A a linear transformation $V \to W$ is freely specified by where it sends a basis of V."

For example, let S a set (for example $S = \{v_1, v_2, v_3\}$). Let

$$\mathrm{FreeV}_k(S) = \{\text{finite sums } \sum \alpha_s \cdot s : \alpha_s \in k\}$$

be the vector space over k freely generated by S. So S itself is a basis. Then saying a linear map $\mathrm{FreeV}(S) \to W$ is the same as saying a *set map* $S \to \underline{W}$, where $\underline{W}$ is the *underlying set* of vectors of W. Notice FreeV is a functor from **Set** to $\mathbf{Vect}_k$.

In other words, consider the *forgetful* functor $\mathbf{Vect}_k \to \mathbf{Set}$ sending a vector space W to its underlying set $\underline{W}$ of vectors. Then given S a set and W a vector space,

$$\mathrm{Mor}_{\mathbf{Vect}_k}(\mathrm{FreeV}_k(S), W) \cong \mathrm{Mor}_{\mathbf{Set}}(S, \underline{W}).$$

Definition 1.13. Let $F\colon \mathcal{C} \to \mathcal{D}$ and $G\colon \mathcal{D} \to \mathcal{C}$ be functors. Then (F, G) is an *adjoint pair* if for every object X of $\mathcal{C}$ and Y of $\mathcal{D}$, there is an isomorphism

$$\mathrm{Mor}_{\mathcal{D}}(FX, Y) \cong \mathrm{Mor}_{\mathcal{C}}(X, GY),$$

which moreover is natural with respect to morphisms in $\mathcal{C}$ and morphisms in $\mathcal{D}$.

Write down what this naturality means (commuting diagram). In practice, the naturality is always fine.

Example 1.14.

(1) Free groups. More "free" constructions in HW.
(2) Many "minimally invasive" functors are adjoints to (fully faithful) inclusions. For example: Say R is a domain, k a field. Then to give an injective map $R \to k$ is to give a map $\mathrm{Frac}(R) \to k$. Phrase this as an adjunction (one of the categories is domains with injective maps.) Think of Frac like a minimally invasive way to make R into a field.

Please treat the rest of the class as an "adjoint pair scavenger hunt."

6. Limits, colimits

First, we are often interested in diagrams, say the following kind of diagram of commutative rings:

$$\begin{array}{ccc} A_1 & \longrightarrow & A_2\ . \\ \downarrow & & \\ A_3 & & \end{array}$$

It will be conceptually useful to break this data into two parts: the shape of the diagram, and the actual objects/maps, e.g., let I be the category

$$\begin{array}{ccc} \bullet_1 & \longrightarrow & \bullet_2\ , \\ \downarrow & & \\ \bullet_3 & & \end{array}$$

then a diagram of rings as in the above is simply a functor $R\colon I \to \mathbf{ComRing}$.

Definition 1.15. A diagram in a category $\mathcal{C}$ indexed by a (small) category I is simply a functor $A\colon I \to \mathcal{C}$. May write $A_i := A(i)$ for $i \in I$.

Example 1.16.

(1) A *commutative square* in $\mathcal{C}$ is a functor to $\mathcal{C}$ from the poset I drawn below.

(All the nonidentity morphisms of I are drawn on the left; in particular going around the upper-right is the same as going around the lower-left. Typically one omits the diagonal arrow from the drawing, as on the right.)

(2) A sequence $A_1, A_2, \ldots$ of objects in $\mathcal{C}$ is a functor $\mathbb{Z}_{>0} \to \mathcal{C}$. (Recall that we can regard a set as a category having only identity morphisms).

Definition 1.17. The *limit* of a diagram $A\colon I \to \mathcal{C}$ is an object of $\mathcal{C}$, denoted $\varprojlim_{\leftarrow I} A_i$, together with a morphism

$$\begin{array}{c} \varprojlim_{\leftarrow I} A_i \\ \downarrow f_i \\ A_i \end{array}$$

for each $i \in I$, such that

- for all arrows $j \to k$ in I the diagram below commutes,

$$\begin{array}{ccc} & \varprojlim_{\leftarrow I} A_i & \\ {\scriptstyle f_i}\swarrow & & \searrow{\scriptstyle f_j} \\ A_j & \longrightarrow & A_k \end{array}$$

and moreover,

- $\varprojlim_{\leftarrow I} A_i$ is final with respect to this property. (Write out what that means.)

So limits, if they exist, are automatically unique up to unique isomorphism.

Example 1.18. The first three examples have indexing category $I = \cdots \to \bullet \to \bullet \to \bullet$.

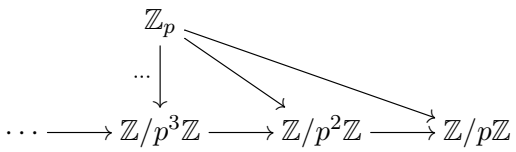
(1) Recall the *ring of formal power series* $R[[x]]$ over ring R has elements

$$\{r_0 + r_1 x + r_2 x^2 + \cdots : r_i \in R\}.$$

It is the limit

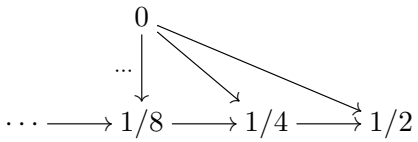
$$\begin{array}{ccccccc} & & & & R[[x]] & & \\ & & & & {\scriptstyle \cdots}\downarrow & \searrow & \searrow \\ \cdots & \longrightarrow & R[x]/(x^3) & \longrightarrow & R[x]/(x^2) & \longrightarrow & R[x]/(x) \end{array}$$

(2) Ring of p-adics for fixed prime p



These are both examples of *I-adic completions*, see [AM69, Ch. 10].

(3) A wackier example: a diagram $I \to (\mathbb{R}, \leq)$ is a sequence of reals weakly decreasing to the left. The limit, if it exists, is exactly the infimum.

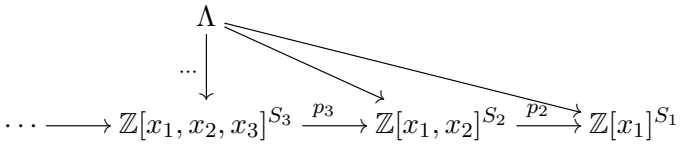


(4) The product $X \times Y$ in $\mathcal{C}$, if it exists, is the limit of the diagram

$$X \qquad Y$$

Here, the indexing category is simply $\bullet \quad \bullet$.

(5) In this example I assume the definition of a graded ring. The *ring of symmetric functions* Λ is defined to be the limit, in the category of graded rings,



of the rings of symmetric polynomials. Here the maps p_i send $x_i \mapsto 0$.

Exercise 1.19. Let Λ^d denote the subgroup of $\mathbb{Z}[[x_1, x_2, \ldots]]$ of homogeneous degree d power series that are invariant on permuting the variables x_i. Then Λ is the graded ring

$$\Lambda = \bigoplus_{d \geq 0} \Lambda^d.$$

The ring of symmetric functions is of central interest in algebraic combinatorics.

Definition 1.20. Dually, define the *colimit* of a diagram $A \colon I \to \mathcal{C}$, denoted $\varinjlim_{\to I} A_i$.

Example 1.21. Coproducts. For example, the coproduct of a bunch of sets $\{X_i\}_{i \in \mathcal{I}}$ is the disjoint union

$$\coprod_{i \in \mathcal{I}} X_i := \{(x, i) : i \in \mathcal{I}, x \in X_i.\}$$

Limits and colimits are formally completely symmetric, but fairly often in practice they have different feels to them. Limits often have the feel of some thing combining all of the increasing complexity of the things in the diagram, and colimits often feel like some kind of side-by-side gluing (give a topological example of a diagram of spaces: gluing two sheets of paper together along an edge.)

Confusingly,

- **Limits** are also called **inverse limits** or **projective limits**.
- **Colimits** are also called **direct limits**.

Precisely because of this confusion, and following the conventions of [**?**], we will stick with *limit* and *colimit* only.

7. RAPL, LAPC

These two statements are unreasonably useful, especially in proportion to how hard they are to prove:

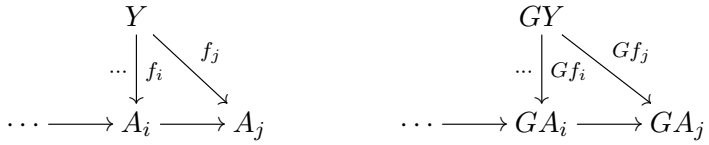
Right adjoints preserve limits, left adjoints preserve colimits.

Please share a good mnemonic device, mathematical or otherwise, with me and the class.

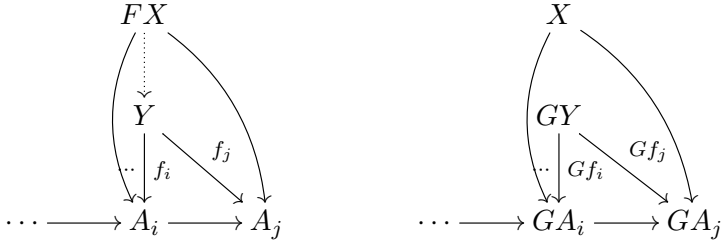
Proof. Let us prove RAPL. Let $(F\colon \mathcal{C} \to \mathcal{D}, G\colon \mathcal{D} \to \mathcal{C})$ be an adjoint pair, and $A\colon I \to \mathcal{D}$ a diagram in $\mathcal{D}$, with limit $Y = \lim_{\leftarrow I} A_i$. Then we claim

$$GY = \lim_{\leftarrow I} GA_i.$$

First we note that the object comes equipped with suitable maps to GA_is:



Now let's test the supposed universal property of GY. Suppose an object X of $\mathcal{C}$ comes along, equipped with suitable maps to the GA_i. We need to find a map $X \to GY$ making everything in the right hand diagram commute.



Exercise 1.22. Find the desired arrow $X \to GY$ by finding an appropriate arrow $FX \to Y$ using the universal property of Y, and using the identification

$$\mathrm{Mor}_{\mathcal{C}}(X, GY) \cong \mathrm{Mor}_{\mathcal{D}}(FX, Y).$$

(The *naturality* of these identifications must come into play.)

□

8. Natural transformations

Definition 1.23. Let $F, G \colon \mathcal{C} \to \mathcal{D}$ be functors. A *natural transformation* $\Phi \colon F \Rightarrow G$ is:

- for every X in $\mathcal{C}$, an arrow $\Phi_X \colon FX \to GX$ in $\mathcal{D}$, such that

for every arrow $f \colon X \to X'$ in $\mathcal{C}$, the following square commutes.

$$\begin{array}{ccc} FX & \xrightarrow{\Phi_X} & GX \\ {\scriptstyle Ff}\downarrow & & \downarrow{\scriptstyle Gf} \\ FX' & \xrightarrow{\Phi_{X'}} & GX' \end{array}$$

Convince yourself that natural transformations may be composed. Thus functors $\mathrm{Fun}(\mathcal{C}, \mathcal{D})$ are the objects of a category whose morphisms are natural transformations. Say $\Phi \colon F \Rightarrow G$ is a *natural isomorphism* if it is an isomorphism in this category.

Exercise 1.24. Check that Φ is a natural isomorphism if and only if all Φ_X are isomorphisms.

Example 1.25. (The determinant, from Maclane) We have

$$\mathrm{GL}_n, (-)^* \colon \mathbf{ComRing} \to \mathbf{Gp},$$

two ways to make groups out of commutative rings. Then $\det \colon \mathrm{GL}_n \Rightarrow (-)^* \colon$ is a natural transformation.

Example 1.26. [**?**, Example 1.4.3] Consider the identity and double dual endofunctors[1] $\mathrm{Id}, (-)^{**} \colon \mathbf{Vect}_k \to \mathbf{Vect}_k$. There is a natural transformation

$$\mathrm{ev} \colon \mathrm{Id} \Rightarrow (-)^{**}$$

given by: $\mathrm{ev}_V \colon V \to V^{**}$ is the linear map $v \mapsto \mathrm{ev}_v \colon V^* \to k$. In other words, given a linear map $V \to W$ with $v \mapsto w$, the following diagram commutes.

$$\begin{array}{ccc} V & \longrightarrow & V^{**} \\ \downarrow & & \downarrow \\ W & \longrightarrow & W^{**} \end{array} \qquad \begin{array}{ccc} v & \longmapsto & \mathrm{ev}_v \\ \downarrow & & \downarrow \\ w & \longmapsto & \mathrm{ev}_w \end{array}$$

[1] A functor from a category to itself.

Exercise 1.27.

(1) In fact ev can be restricted to a natural transformation $\mathrm{Id} \Rightarrow (-)^{**}$ of endofunctors on the category $\mathbf{FdVect}_k$ of *finite dimensional* vector spaces over k. Then ev is a natural isomorphism.
(2) On the other hand, there is no natural transformation $\mathrm{Id} \Rightarrow (-)^{*}$. (Good to think about.)

9. Equivalence of categories

Make up a definition of isomorphism of categories; it is probably right. But surprisingly the notion of isomorphism of categories is often too rigid. An *equivalence* of categories is more useful:

Definition 1.28. An equivalence of categories between $\mathcal{C}$ and $\mathcal{D}$ is a pair of functors

$$F\colon \mathcal{C} \to \mathcal{D}, \qquad G\colon \mathcal{D} \to \mathcal{C}$$

together with natural isomorphisms $GF \simeq 1_{\mathcal{C}}$ and $FG \simeq 1_{\mathcal{D}}$.

The following equivalent characterization of equivalence of categories is useful:

Proposition 1.29. A functor $F\colon \mathcal{C} \to \mathcal{D}$ defines an equivalence of categories if and only if it is full, faithful, and essentially surjective.

(Make sure we know what those three things mean!)

Proof. Try it as an exercise. □

Example 1.30. Skeleton of a category, e.g., skeleton of the category of finite sets.

10. Yoneda lemma

"An object can be remembered by the totality of morphisms it receives."

Or, in the memorable words of an undergraduate when I gave an UG talk on Yoneda: You are what you eat!

Let $\mathcal{C}$ be a locally small category. Then every object X of $\mathcal{C}$ defines a functor

$$h_X\colon \mathcal{C}^{\mathrm{op}} \to \mathbf{Set}$$

given on objects by $h_X(Y) := \mathrm{Mor}_{\mathcal{C}}(Y, X)$, and on morphisms as follows: given $f\colon Y \to Y'$ there is a natural map $- \circ f\colon \mathrm{Mor}_{\mathcal{C}}(Y', X) \to \mathrm{Mor}_{\mathcal{C}}(Y, X)$.

In this way we get a functor

$$h\colon \mathcal{C} \to \mathrm{Fun}(\mathcal{C}^{\mathrm{op}}, \mathbf{Set})$$

sending X to h_X. The following result says that X can be represented by h_X.

Theorem 1.31. Yoneda embedding. The functor h is fully faithful.

(If necessary, review the definition of full and faithful.)

Actually, the full statement of Yoneda's lemma is as follows (see [**?**, Theorem 2.2.4]).

Theorem 1.32. Let $\mathcal{C}$ be locally small. Given a functor $F\colon \mathcal{C}^{\mathrm{op}} \to \mathbf{Set}$ and any object X in $\mathcal{C}$, there is a *natural* bijection between natural transformations $h_X \Rightarrow F$ and FX, sending a natural transformation $\Phi\colon h_X \Rightarrow F$ to the image under $\Phi_X\colon h_X(X) \to FX$ of 1_X. Naturality of the bijection means natural in X and F.

Functors $\mathcal{C}^{\mathrm{op}} \to \mathbf{Set}$ in the essential image of h, i.e., that are isomorphic to h_X for some object X, are called *representable.* In algebraic geometry we often have functors of geometric interest, and one wants to study whether the functor is representable. Ideally it is, but if not, one studies the various functors $\mathcal{C}^{\mathrm{op}} \to \mathbf{Set}$ of interest anyways, viewed as living "just outside" the category $\mathcal{C}$ via the Yoneda embedding.

Example 1.33. Power set functor $\mathcal{P}\colon \mathbf{Set}^{\mathrm{op}} \to \mathbf{Set}$ sending S to $\mathcal{P}(S) = 2^S$. Is this representable? Actually the notation 2^S is suggestive...

Example 1.34. Families of oriented vs. unoriented segments.

11. Reminder: modules

Before we do abelian categories, let us remind ourselves of *modules* over a commutative ring R, which are the primary example.

An R-module is, basically, an abelian group M with an action of R on it. I find it hard to remember all the different compatibilities that are required, so let's derive it as follows.

First, if M is an abelian group, the endomorphisms $\mathrm{End}(M)$ naturally form a (not typically commutative) ring: if $f, g\colon M \to M$ are two such, then $f+g\colon M \to M$ is defined as $(f+g)(x) = f(x) + g(x)$, and $fg = f \circ g$ is the *composition.*

Definition 1.35. Then an R-module is an abelian group M together with a ring homomorphism $R \to \mathrm{End}(M)$.

Exercise 1.36. Write out what that amounts to.

This is a "plug and play" definition of a module. Regard $\mathrm{End}(M)$ as a USB port in M which is ready to receive a ring R.

Example 1.37.

(1) A $\mathbb{Z}$-module is exactly an abelian group, because giving a map $\mathbb{Z} \to \mathrm{End}(M)$ is to give no additional data at all. (Recall $\mathbb{Z}$ is initial in **Ring**.)

(2) A k-module is a vector space over k.
(3) (Dropping the requirement that R is commutative) Recall the group ring $k[G]$, whose elements are finite k-linear combinations of group elements. A $k[G]$-module is exactly a vector space V with a G-action on it, that is, V together with a group homomorphism $G \to \mathrm{GL}(V)$.

12. Towards abelian categories

The source is [**?**, §1.4] of Vakil; basically there are some things that are true of modules that will be automatically true in arbitrary abelian categories, so we may as well. First we define kernels and cokernels. Then we define additive categories, and abelian categories. (Possibly recall the definitions of kernel and cokernel in R-mod.)

Definition 1.38. Let $\mathcal{C}$ be any category with a zero object 0. The *kernel* of a morphism $f\colon B \to C$, if it exists, is a morphism $i\colon A \to B$ such that the following is a pullback diagram:

$$\begin{array}{ccc} A & \xrightarrow{i} & B \\ \downarrow & & \downarrow f \\ 0 & \longrightarrow & C \end{array}$$

What does this mean? First, that $fi = 0$. (What is meant by the 0 map between any two objects? It is the unique morphism $* \to 0 \to *$.) Second, that if $i'\colon A' \to B$ is any other arrow with $fi' = 0$ then i' factors uniquely through i.

Definition 1.39. Similarly, the cokernel of a morphism $i\colon A \to B$ is $f\colon B \to C$ if the diagram above is a pushout.

Definition 1.40. An additive category is a locally small category $\mathcal{A}$ together with the structure of an abelian group on each $\mathrm{Mor}_{\mathcal{A}}(X, Y)$ such that composition distributes over addition, ie

$$f(g + g') = fg + g', \qquad (f + f')g = fg + f'g,$$

and such that in addition

(1) $\mathcal{A}$ has a zero object,
(2) $\mathcal{A}$ admits finite products and coproducts $X \times Y$ and $X \oplus Y$.

Remark 1.41. In fact, $X \times Y = X \oplus Y$. Actually, it is enough to require the existence of one of these, say finite products; then prove that the finite product also functions as coproduct. Or vice versa.

Exercise 1.42. In an additive category, the additive identity in the abelian group $\mathrm{Mor}_{\mathcal{C}}(X, Y)$ is exactly the morphism $X \to 0 \to Y$. We henceforth denote this morphism 0 unambiguously.

Definition 1.43. Monomorphisms, epimorphisms in an arbitrary category. An arrow $f\colon x \to y$ is *monic* if $fg = fg'$ implies $g = g'$. *Epic* if $hf = h'f$ implies $h = h'$.

Exercise 1.44. In an additive category, kernels are monic and cokernels are epic.

Now here is the key definition of the setting in which a lot of homological algebra takes place.

Definition 1.45. An *abelian* category is an additive category $\mathcal{A}$ such that

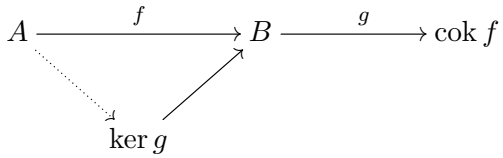
- Every morphism has a kernel and cokernel,
- Every monic in $\mathcal{A}$ is the kernel of its cokernel, and
- Every epi in $\mathcal{A}$ is the cokernel of its kernel.

By the previous exercise, conclude that in an abelian category, monic = "is a kernel" and epic = "is a cokernel."

Example 1.46. The main example of an abelian category is that of R-modules. In some sense[2] this is the only example.

Example 1.47. The category $\mathbf{Sh}_X$ of sheaves of abelian groups on a topological space X, which you learn more about in algebraic geometry for example.

Now we can define the *image* of an arbitrary morphism $f\colon A \to B$ in an abelian category $\mathcal{A}$: it is the kernel of the cokernel of f. So:



Of course, in the category of R-modules we have $\mathrm{im}(f) = \{f(a) : a \in A\}$, with the canonical inclusion into B, as usual.

Remark 1.48. In case the asymmetry of the above bothers you: one could define the *coimage* of f to be $\mathrm{cok}(\ker(f))$. Then it is true, *but this is not easy to prove*, that the dotted arrow

[2]Freyd-Mitchell embedding theorem: every locally small abelian category admits a fully faithful, exact functor into R-mod for some possibly noncommutative R.

above is the coimage. In other words, there is a commutative diagram

$$\begin{array}{ccccccc} \ker f & \xrightarrow{e} & A & \xrightarrow{f} & B & \xrightarrow{g} & \operatorname{cok} f \\ \downarrow & & \downarrow & & \uparrow & & \uparrow \\ 0 & \longrightarrow & \operatorname{coim} f & \overset{\cong}{\cdots\cdots} & \operatorname{im} f & \longrightarrow & 0 \end{array}$$

where the first and last squares are pullback-pushout squares and the dotted arrow is a unique isomorphism. This provides a canonical identification of $\operatorname{coim} f$ and $\operatorname{im} f$ and a unique-up-to-unique isomorphism factorization of an arbitrary morphism f as

$$A \xrightarrow{\text{epic}} C \xrightarrow{\text{monic}} B,$$

where C is precisely the image = coimage.

We will take this as true (it IS true!) from now on.

Definition 1.49. A diagram

$$A \xrightarrow{f} B \xrightarrow{g} C$$

is *exact* at B if $\ker g = \operatorname{im} f$. Say a sequence

$$\cdots A_{i-1} \to A_i \to A_{i+1} \to \cdots$$

is exact if it's exact everywhere.

To be very precise, $\ker g$ and $\operatorname{im} f$ are morphisms to B, unique up to unique isomorphism. (Like everyone else, we will soon stop being so precise and just refer to the objects and not the morphisms to B.) In light of the previous remark, this is equivalent to $\operatorname{cok} f = \operatorname{coim} g$.

Exercise 1.50.

(1) A sequence $0 \to A \xrightarrow{f} B \xrightarrow{g} C$ is exact iff f is the kernel of g.

(2) A sequence $A \xrightarrow{f} B \xrightarrow{g} C \to 0$ is exact iff g is the cokernel of g.

Proof. For (1): Exactness at A means $\ker f = 0$, so $A = \operatorname{coim} f = \operatorname{im} f = \ker g$ by exactness at B. (2) is analogous. □

Definition 1.51. A covariant (additive) functor $F\colon \mathcal{C} \to \mathcal{D}$ on abelian categories is called *left exact* if... A *contravariant* functor $F\colon \mathcal{C} \to \mathcal{D}$ is called *left exact* if

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

exact in $\mathcal{C}$ implies

$$0 \to FA \to FB \to FC$$

is exact. Similarly for *right exact.* Say F is exact if both left/right exact.

Implicit in all this is the claim that an additive functor, i.e., one respecting the group structure on hom-sets, takes 0 to 0. (Proof: show that the zero object Z is characterized by $0_Z = 1_Z \in \mathrm{Mor}(Z, Z)$.)

Let's collect the following useful statement:

Proposition 1.52. Right adjoints are left exact. Left adjoints are right exact.

Proof. That is, if $(F\colon \mathcal{C} \to \mathcal{D}, G\colon \mathcal{D} \to \mathcal{C})$ are an adjoint pair of additive functors on abelian categories, then F is right exact and G is left exact. We have basically already proved all the parts of this. Namely, F, being a left adjoint, preserves colimits, in particular cokernels. As noted above this exactly means that F is right exact. Similarly for G. □

For example, let's go and prove almost everything in A&M about tensor products of modules, without knowing anything except their defining property: there is a natural isomorphism of R-modules

$$\mathrm{Hom}(M \otimes N, P) \cong \mathrm{Hom}(M, \mathrm{Hom}(N, P)).$$

Believe it? Given $\phi\colon M \to \mathrm{Hom}(N, P)$, write $\phi_m = \phi(m)\colon N \to P$. then ϕ defines a map (of sets, so far)

$$\Phi\colon M \times N \to P, \qquad (m, n) \mapsto \phi_m(n)$$

which satisfies:

(1) $\phi_m\colon N \to P$ is R-linear for each m:

$$\Phi(m, n + n') = \Phi(m, n) + \Phi(m, n'), \Phi(m, rn) = r\Phi(m, n)$$

(2) ϕ itself is R-linear:

$$\Phi(m + m', n) = \Phi(m, n) + \Phi(m', n), \qquad r\Phi(m, n) = \Phi(rm, n)$$

(Please study the construction of tensor products if it is unfamiliar. I probably won't do it, since I am mostly trying to avoid it as a "crutch," unless I feel I really need to.) Therefore:

$$\boxed{- \otimes N \text{ and } \mathrm{Hom}(N, -) \text{ are an adjoint pair of functors } R\text{-mod} \to R\text{-mod}.}$$

Corollary 1.53. $- \otimes N$, being a left adjoint, preserves colimits. In particular it preserves cokernels, i.e., is right exact.

Corollary 1.54. $\mathrm{Hom}(N, -)$, being a right adjoint, preserves limits. In particular it preserves kernels, i.e., is left exact.

In general, measuring failure of a left exact/right exact functor to be exact gives rise to *derived functors*. (I have not decided whether to cover that topic—maybe not.)

The situations in which $- \otimes N$, respectively $\mathrm{Hom}(N, -)$, happen to be exact, for a particular N, are also interesting, and get special names:

Definition 1.55. Modules N for which $- \otimes N$ is an exact functor are called *flat*. Modules N for which $\mathrm{Hom}(N, -)$ is an exact functor are called *projective*.

Other standard properties of tensor products, which we read in A&M, can "immediately" be deduced:

Exercise 1.56. We have canonical isomorphisms

(1) $R \otimes M \cong M$.
(2) $M \otimes (\bigoplus_{i \in \mathcal{I}} N_i) \cong \bigoplus_{i \in \mathcal{I}} (M \otimes N_i)$
(3) $M \otimes (N \otimes P) \cong (M \otimes N) \otimes P$

Proof. Prove these, using universal properties and Yoneda as needed, but without referring to the construction of tensor products □

An aside: What about $\mathrm{Hom}(-, P)\colon R\text{-mod}^{\mathrm{op}} \to R\text{-mod}$? It turns out to be *self right-adjoint*:

Definition 1.57. Say functors $F\colon \mathcal{C}^{\mathrm{op}} \to \mathcal{D}$ and $G\colon \mathcal{D}^{\mathrm{op}} \to \mathcal{C}$ are *mutually right-adjoint* of for all X in $\mathcal{C}$ and Y in $\mathcal{D}$ we have natural correspondences

$$\mathrm{Mor}_{\mathcal{D}}(Y, FX) \cong \mathrm{Mor}_{\mathcal{C}}(X, GY).$$

Exercise 1.58.

(1) Given F and G as above, define an appropriate opposite functor $G^{\mathrm{op}}\colon \mathcal{D} \to \mathcal{C}^{\mathrm{op}}$ from G. Then deduce that F and G are mutually right adjoint iff (G^{op}, F) is an adjoint pair of functors $\mathcal{D} \rightleftharpoons \mathcal{C}^{\mathrm{op}}$. (Equivalently, iff (F^{op}, G) is an adjoint pair of functors $\mathcal{C} \rightleftharpoons \mathcal{D}^{\mathrm{op}}$.)
   Conclude that if F and G are mutually right-adjoint then they preserve all limits.
(2) Define mutually left-adjoint contravariant functors, and redo all of the above.

Returning to the case of R-modules now, the natural identification

$$\mathrm{Hom}(M, \mathrm{Hom}(N, P)) \cong \mathrm{Hom}(N, \mathrm{Hom}(M, P))$$

(after all, both are $\mathrm{Hom}(M \otimes N, P) = \mathrm{Hom}(N \otimes M, P)$) quickly shows that $\mathrm{Hom}(-, P)$ is self right-adjoint, hence preserves limits, hence preserves kernels, i.e., is left-exact.

Definition 1.59. An R-module P is called *injective* if $\mathrm{Hom}(-, P)$ is exact.

Part 2. Some commutative algebra

There are a few more topics related to tensors that will be useful to us. Note: at this point I may need to review the construction of tensor product.

13. Extension, restriction of scalars

An R-algebra is a morphism $R \to S$ of rings; morphisms are commuting triangles.

Now given $f\colon R \to S$, there are natural ways to turn R-modules into S-modules and vice versa, called extension and restriction of scalars. Let's start with the easier one:

Definition 2.1. Given N an S-module, we have a natural R-module structure on N called its *restriction* to R, by defining $r \cdot n = f(r) \cdot n$. Another way to say it is via the composition

$$R \xrightarrow{f} S \to \mathrm{End}(N).$$

A special case of restriction of scalars is when $N = S$. In other words, an R-algebra is naturally an R-module.

Definition 2.2. Given M an R-module, consider the R-module $S \otimes_R M$, where S is regarded as an R-module as above. Then notice that $S \otimes_R M$ can be regarded as an S-module, via

$$s \cdot (s' \otimes m) = ss' \otimes m,$$

and this S-module is called the *extension* of N.

Example 2.3. Possibly draw a picture for $\mathbb{Z}^2 \otimes_{\mathbb{Z}} \mathbb{R} = \mathbb{R}^2$ as an $\mathbb{R}$-module.

Exercise 2.4. (Extension, Restriction) are an adjoint pair.

14. Tensor product of R-algebras

Define it and state universal property. We follow [AM69, p. 30].

Let $f\colon A \to B$, $g\colon A \to C$ be two A-algebras. Let $D = B \otimes_A C$, an A-module. We make it an A-algebra by defining a multiplication on D: the A-multilinear map

$$B \times C \times B \times C \to D, \qquad (b, c, b', c') \mapsto bb' \otimes cc'$$

induces an A-linear map

$$B \otimes C \otimes B \otimes C = D \otimes D \to D,$$

which induces an A-bilinear map $D \times D \to D$ given on pure tensors by

$$(b \otimes c, b' \otimes c') \mapsto bb' \otimes cc'.$$

This gives a multiplication on D; check that D becomes a commutative ring, which furthermore has the structure of an A-algebra on D via $a \mapsto f(a) \otimes g(a)$.

Proposition 2.5. State universal property.

Proof. Omitted. □

15. Free modules

Let R be a ring, as usual assumed to be commutative unless I state otherwise. Recall that a free module over R is a module isomorphic to $R^{(\mathcal{I})} := \oplus_{i\in\mathcal{I}} R$. (The "usual" exercise at this point: formulate the construction of $R^{(\mathcal{I})}$ from a set $\mathcal{I}$ as a left adjoint to a forgetful functor.) So a finitely generated free module is isomorphic to R^n. Note $A^n \otimes_A B = (A \otimes_A B)^n = B^n$ (tensor commutes with colimits), so extension of scalars of a free module is a free module. Then note that the *rank* of a free module is well-defined:

Exercise 2.6. (This is an exercise in A&M). Suppose $R \neq 0$. If m and n are numbers with $R^m \cong R^n$ then $m = n$.

Proof. Pick a maximal ideal $\mathfrak{m}$ of R (using exactly that $R \neq 0$.), so $R/\mathfrak{m} = k$ is a field. Obtain

$$R/\mathfrak{m} \otimes_R R^m \cong R/\mathfrak{m} \otimes_R R^n$$

which becomes $k^m \cong k^m$ as k-modules (vector spaces). Done by linear algebra. □

16. Finitely generated modules

One way to describe the condition of an R-module M being *finitely generated* is: M is finitely generated iff it admits a surjection of R-modules

$$\phi\colon R^n \to M.$$

Indeed, a map is given by $e_i \mapsto m_i$, with image $\{\sum_{i=1}^n r_i m_i \colon r_i \in R\}$. Then ϕ is surjective iff the x_i's generate M.

Definition 2.7. M is called *finitely presented* if it fits in an exact sequence

$$R^m \to R^n \to M \to 0.$$

In many cases (but not all!) fg and fp are the same, e.g. in the case of Noetherian rings. Below the reference is [AM69, §6]:

Definition 2.8. Say a module is *Noetherian* if every submodule is finitely generated.

For example, a ring is Noetherian iff every ideal is finitely generated.

Lemma 2.9. Given a short exact sequence of R-modules

$$0 \to M' \xrightarrow{f} M \xrightarrow{g} M'' \to 0,$$

we have that M is Noetherian iff M' and M'' are Noetherian.

Proof. If M Noetherian, then so is M', since submods of M' are submods of M. And so is M'', since submods of M'' lift to submods of M, and generators in the latter give generators in the former.

Conversely, suppose M' and M'' are Noetherian, and let $N \subseteq M$ be a submodule. Then $N' = f^{-1}(N)$ is a f.g. submodule of M', and $g(N) = N''$ is a f.g. submodule of M''. Given generators $x_1, \dots, x_a \in N'$ and given $y_1, \dots, y_b \in N$ whose images generate N'', check $f(x_1), \dots f(x_a), y_1, \dots, y_b$ generate N. □

Corollary 2.10. If R is a Noetherian ring then R^n is a Noetherian module.

Proof. Induction, e.g., $0 \to R \to R^2 \to R \to 0$ shows it for R^2. □

Corollary 2.11. A finitely generated module over a Noetherian ring is Noetherian.

Proof. Such a module is a quotient of some R^n, hence Noetherian since R^n is. □

Hence, for example, fg modules over Noetherian rings are finitely presented:

$$0 \to \ker \to R^n \to M \to 0$$

with ker finitely generated.

17. Jacobson radical

Let R be a ring. Recall nilradical, and define Jacobson radical as the intersection of all maximal ideals. So the Jacobson radical contains the nilradical (the nilradical is the intersection of *more* ideals.) Another characterization of $\mathrm{Jac}(R)$ is:

Proposition 2.12. (See [AM69, Proposition 1.9]) We have

$$\mathrm{Jac}(R) = \{x \in R \colon 1 - xy \in R^* \text{ for all } y \in R.\}$$

Proof. It is helpful to first remind ourselves that an element of R is a unit iff it is in *no* maximal ideals.

Say $x \in \mathrm{Jac}(R)$. Then xy is in all maximal ideals so $1 - xy$ is in none.

Now say $x \notin \mathrm{Jac}(R)$, meaning it fails to be in some maximal ideal $\mathfrak{m}$. Then $(x) + \mathfrak{m} = (1)$ implies $1 = xy + m$ for some $m \in \mathfrak{m}$ and some y. So $1 - xy \in \mathfrak{m}$ is not a unit. □

18. Cayley-Hamilton theorem and Nakayama's Lemma

We follow [AM69, p. 21]. It will be helpful to observe:

Remark 2.13. An $A[t]$-module M is exactly an A-module M together with an A-linear map $\phi\colon M \to M$. Then an $A[t]$-module map $\rho\colon M \to M$ is exactly an A-linear map ρ that commutes with ϕ.

(Do you agree? Recall that an *A-linear map* is simply a morphism of A-modules.)

Theorem 2.14. Let M be a finitely generated A-module, say generated by $x_1, \dots, x_n \in M$. Let $\phi\colon M \to M$ be an A-linear map which may be represented by a matrix $B \in A^{n\times n}$ with respect to the generators $x_1, \dots, x_n$.

Then ϕ is a zero of the *characteristic polynomial*

$$\det(B - tI) \in A[t].$$

Remark 2.15. In general, if ϕ is an A-linear map, it can be represented likely in many different ways as an $n \times n$ matrix with respect to fixed generating set, and furthermore not *all* $n \times n$ matrices represent A-linear maps of M.

Proof. Regard M as an $A[t]$-module, where $t \cdot x = \phi(x)$. Then $\phi\colon M \to M$ is a morphism of $A[t]$-modules, that can be represented both by B and tI; these are $n \times n$ matrices over $A[t]$. Therefore $B - tI_n$ represents the 0 endomorphism of M. Multiplying on the left by the adjugate matrix of $B - tI_n$ yields that $\operatorname{char}(t) := \det B - tI_n \in A[t]$ acts as 0 on each x_i, in other words, is the 0 endomorphism of M. In other words $\operatorname{char}(\phi) = 0 \in \operatorname{End} M$. □

Corollary 2.16. ([AM69, Proposition 2.4] Let M be a finitely generated A-module, and let $\phi\colon M \to M$ be an A-linear map such that $\phi(M) \subseteq IM$ for some ideal $I \subseteq A$. Then ϕ satisfies an equation of the form

$$\phi^n + a_1\phi^{n-1} + \cdots + a_n = 0 \in \operatorname{End}_{A\text{-mod}}(M)$$

for some $a_i \in I$, in fact $a_i \in I^i$.

Proof. This would follow from the previous proposition if we could show that ϕ can be represented by a matrix *all of whose entries are in I*. Do you agree?

Since $\phi(M) \subseteq IM$ by hypothesis, we need only show: given an element $x \in IM$, can we write $x = \sum b_i x_i$ for some $b_i \in I$? This seems very plausible.

Yes: write

$$x = \sum a_i y_i, \qquad a_i \in I.$$

Now each y_i is expressible as an R-linear combination of the generators x_i, so expand everything and collect terms. □

Corollary 2.17. [AM69, Proposition 2.5] Let M be a finitely generated A-module, $I \subseteq A$ an ideal with $IM = M$. Then there exists $x \in R$ such that $x - 1 \in I$ and $xM = 0$.

Remark 2.18. Equivalently, by letting $i = 1 - x$, there exists $i \in I$ such that $im = m$ for all $m \in M$. I learned this helpful mnemonic from reading Math Overflow:

$$\boxed{IM = M \text{ implies } im = m,}$$

again with hypothesis that M is finitely generated.

Proof. Let $\phi = 1 \colon M \to M$. The previous result implies

$$1 + a_1 + \cdots + a_n = 0 \in \operatorname{End} M,$$

for some $a_i \in I$. So $x = 1 + a_1 + \cdots + a_n$ satisfies $xM = 0$. □

Lemma 2.19. (Nakayama's Lemma) Let M be a finitely generated A-module and $I \subseteq \operatorname{Jac}(R)$ an ideal. Then $IM = M$ only if $M = 0$.

Proof. By the mnemonic device, there exists $i \in I$ such that $im = m$ for all $m \in M$. By the characterization of Jacobson radical, $1 - i \cdot 1 = 1 - i \in R^*$, so

$$u(1 - i)m = 1 \cdot m = m.$$

On the other hand, $(1 - i)m = m - m = 0$, thus $M = 0$.

□

It is a bit difficult to internalize Nakayama's Lemma. Here's a useful case of it: Let $(R, \mathfrak{m})$ be a local ring, $k = R/\mathfrak{m}$ its *residue field*. Let M be a finitely generated R-module. Then $M/\mathfrak{m}M$ is an $R/\mathfrak{m}$-module, i.e., a k-vector space, of finite dimension, since generators of M descend to generators of $M/\mathfrak{m}M$.

Then the next proposition claims that a spanning set of $M/\mathfrak{m}M$ can be lifted to a generating set of M. Precisely:

Proposition 2.20. With $(R, \mathfrak{m})$ a local ring and M a finitely generated R-module as above, suppose $x_1, \ldots, x_n \in M$ are such that $\overline{x_1}, \ldots, \overline{x_n}$ span the vector space $M/\mathfrak{m}M$. Then the x_i generate M.

Proof. Consider $N = \langle x_1, \ldots, x_n \rangle \subseteq M$: we wish to show $M/N = 0$. Now $\mathfrak{m} \cdot (M/N) = (\mathfrak{m}M + N)/N$ by an isomorphism theorem.[3] But $\mathfrak{m}M + N = M$ by assumption.[4] Thus

$$\mathfrak{m}(M/N) = M/N,$$

so $M/N = 0$ by Nakayama. □

[3] Think it through: the left hand side consists of expressions of the form $\sum x_i(m_i + N)$ for $x_i \in \mathfrak{m}, m_i \in M$.

[4] "The x_i's generate M up to adding $\mathfrak{m}M$."

19. Localization of rings

Definition 2.21. Recall here the definition of a multiplicative subset $S \subseteq R$. The *localization* $S^{-1}R$ of R along S, the ring given by

$$S^{-1}R = \{(r, s) : r \in R, s \in S\}/\sim,$$

with the equivalence relation $\sim$ defined as follows. Write $r/s = (r, s)$ for psychological convenience; then we declare $r/s \sim r'/s'$ iff $u(rs' - r's) = 0$ for some $u \in S$. We check that this is an equivalence relation, and define addition and multiplication to produce a ring structure on $S^{-1}R$.

There is a natural ring homomorphism $\phi\colon R \to S^{-1}R$ sending $r \mapsto r/1$. In general, ϕ may not be injective. For example $S^{-1}R$ can be the zero ring:

Exercise 2.22. Prove that $S^{-1}R = 0$ iff $0 \in S$.

Proposition 2.23. State the universal property.

Example 2.24. Examples of localizations.

(1) If $f \in R$, define
$$R_f = S^{-1}R$$
for $S = \{1, f, f^2, f^3, \ldots\}$. Subexample: if $R = \mathbb{Z}$ and $f = 2$ then we obtain the dyadics.

(2) If $p \subset R$ prime then define
$$R_p = S^{-1}R$$
for $S := R \setminus p$; note S is multiplicative (do you agree?). Subexample: say $R = k[x, y]$, and $p = (x, y)$. Then R_p is the ring of rational functions defined at the origin, i.e.
$$R_p = \left\{ \frac{f(x,y)}{g(x,y)} : g(0,0) \neq 0 \right\}.$$

20. Localization of modules

Let $S \subset R$ be a multiplicative subset, and M an R-module. We wish to define the localization $S^{-1}M$ of M, which shall be an $S^{-1}R$-module. It can be done in two ways:

Definition 2.25. Explicitly, let

$$S^{-1}M = \{m/s : m \in M, s \in S\}/\sim$$

where $m/s \sim m'/s'$ iff $t(s'm - sm') = 0$ for some $t \in S$. Define addition $m/s + m'/s' = (s'm + sm')/ss'$ and multiplication by elements of $S^{-1}R$; check addition is well-defined and that we obtain an $S^{-1}R$-module structure.

Definition 2.26. Or, use extension of scalars to simply define

$$S^{-1}M := M \otimes_R S^{-1}R,$$

Exercise 2.27. Prove these two definitions are the same.

The second definition is useful to know, since we already know some things about tensor products. In particular, we automatically see that $S^{-1}\colon R\text{-mod} \to S^{-1}R\text{-mod}$ is a functor: it's exactly $- \otimes_R S^{-1}R$, a special case of extension of scalars.

Notation. Let M be an R-module. The notation from localizations of rings carries over: if $f \in R$ then we write

$$M_f = M \otimes_R R_f,$$

and if $p \subset R$ is a prime ideal then we write

$$M_p = M \otimes_R R_p$$

for the localizations.

Proposition 2.28. Localization is exact. That is, $S^{-1}R$ is a flat R-algebra. That is,

$$S^{-1}R \otimes_R -\colon R\text{-mod} \to S^{-1}R\text{-mod}$$

is an exact functor.

Proof. We already know it's right exact, being a tensor product. Now if $\phi\colon M' \to M$ is injective, we want to show $S^{-1}\phi\colon S^{-1}M' \to S^{-1}M$ to be injective. Given $m'/s \in S^{-1}M'$, suppose $\phi(m')/s = 0$. Then $0 = t\phi(m') = \phi(tm')$, so $tm' = 0$ by injectivity of ϕ. So $m'/s = 0$. □

21. Ideals in the localization.

(This is [AM69, Proposition 3.11]) How do the ideals of $S^{-1}A$ relate to the ideals of A? (One could reasonably ask the same thing about modules: how do the submodules of $S^{-1}M$ relate to those of M? Try to generalize everything below to localizing modules.) It's plausible that $S^{-1}A$ could have fewer ideals, since more things are units. For an extreme example, consider fraction fields of integral domains, e.g., $\mathbb{Z} \subset \mathbb{Q}$. These are special cases of localizations: along the multiplicative subset of nonzero elements.

Let $\phi\colon A \to S^{-1}A$ denote the map $a \mapsto a/1$.

Proposition 2.29. Let $J \subset S^{-1}A$ be an ideal. Then $J^{ce} = J$.[5] Therefore $J \mapsto J^c$ is an injection from ideals of $S^{-1}A$ to ideals of A.

[5]Establish contraction, extension notation.

Proof. We always have $J^{ce} \subseteq J$. (Why? $\phi(J^c)$ is certainly contained in J, so J^{ce} is also contained in J.) On the other hand, if $a/s \in J$, then also $a/1 = s/1 \cdot a/s \in J$, so $a \in J^c$ and $a/1 \in J^{ce}$, and hence $a/s = a/1 \cdot 1/s \in J^{ce}$. □

So then, which ideals of A arise as contracted ideals?

Proposition 2.30. Let $I \subseteq A$. Then I is a contracted ideal iff for all $s \in S$ and $a \in A$, $sa \in I$ only if $a \in I$. (This is pronounced "no element of S is a zerodivisor in A/I.")

Proof. First of all, from the previous proposition, if $I = J^c$ is a contracted ideal then $I^{ec} = J^{cec} = J^c = I$, using that $J^{ce} = J$ as previously established. Conversely, if $I^{ec} = I$ then certainly I is a contracted ideal (it's the contraction of its extension). So we have that I is contracted iff $I^{ec} = I$.

Suppose $sa \in I$ but $a \notin I$; think of this like "I gets bigger when s is declared a unit," which makes it plausible that I can't be a contracted ideal. Indeed, we have $sa/1 \in I^e$, so $a/1 \in I^e$, so $a \in I^{ec} \setminus I$.

Conversely, suppose that for all s, we have $sa \in I$ only if $a \in I$. Think of this like "I doesn't get bigger when the elements of S are declared to be units," which makes it plausible that $I = I^{ec}$. Now we'd better actually prove $I = I^{ec}$: suppose $a \in I^{ec}$; we wish to show $a \in I$. Well, we have

$$a/1 \in I^e = \{x/s \colon x \in I, s \in S\}.$$

(Why is this the right description of I^e? Well, it is an ideal, and it is the smallest ideal that contains all $x/1$ for $x \in I$.) So $a/1 = x/s$, so $t(as - x) = 0$ for some $t \in S$. This says $ts \cdot a \in I$, which implies $a \in I$. □

Corollary 2.31. The primes of $S^{-1}A$ are in (inclusion-preserving) correspondence with the primes of A not meeting S.

(Make sure we agree that the inverse image of a prime is a prime.) For example, A_p is always a local ring with maximal ideal pA_p.

Think: "localizing at S gets rid of primes meeting S." This will become quite important when we associate to a ring A its *prime spectrum*, which is the set of prime ideals of A together with a particular topology called the *Zariski topology.*

Proof. We are trying to establish that the image of the injective contraction map

$$\{\text{primes of } S^{-1}A\} \to \{\text{primes of } A\}$$

is exactly the primes of A not meeting S. Certainly a prime p of A that *meets* S can't be the contraction of its extension, since $p^e = (1)$.

On the other hand, if p is a prime of A that *avoids* S, then $sa \in p$ only if $a \in p$ by primeness. So $p = p^{ec}$ is a contracted ideal. Moreover

$$p^e = \{x/s : x \in p, s \in S\}$$

really is prime in $S^{-1}A$: check this directly from the definitions. □

22. Local properties

Definition 2.32. Say M is *locally* $\mathcal{P}$, for $\mathcal{P}$ some property, if M_p has property $\mathcal{P}$ for all prime ideals p in R.

For example, the property of being *locally free* is interesting. Free implies locally free (why?), but not conversely. Locally free modules are closely related to vector bundles, and the fact that vector bundles are not all trivial but can have twists—picture the Moebius band—is related to the fact that locally free modules that are not free exist. We can get a first taste in the following example.

Example 2.33. Let $R = R_1 \times R_2$. What are the prime ideals p of R? Since

$$(1,0) \cdot (0,1) = (0,0) \in p,$$

we have, say, $(1,0) \in p$ so $R_1 \times 0 \subset p$. So p is of the form $p = R_1 \times q_2$ for some $q_2 \subset R_2$: after all, if $(x,y) \in p$ then by adding an appropriate element of p, $(\text{anything}, y) \in p$. And necessarily q_2 is a prime ideal. As an exercise, check that

$$R_p \cong (R_2)_{q_2},$$

which is plausible since the primes of R contained in p are exactly the primes of the form $R_1 \times$ something inside q_2.

Similarly, we could have $p = q_1 \times R_2$ for q_1 a prime of R_1.

Now suppose M_1 is an R_1-module and M_2 is an R_2-module. Then both M_is may be regarded as R-modules, and so also their direct sum $M_1 \oplus M_2$ is an R-module. Given a prime $p = R_1 \times q_2$, say, we have

$$(M_1 \oplus M_2) \otimes_R R_p = M_1 \otimes_R R_p \oplus M_2 \otimes_R R_p$$

but the first summand is 0, and the first summand is $(M_2)_{q_2}$.

This already suggests that locally $\mathcal{P}$ in general is not globally $\mathcal{P}$, since localization can allow you to focus on each M_i individually. For example, let $R = k \times k$ and let $M = k^2 \oplus k^3$ with R-action given coordinatewise: $(a,b) \cdot (v,w) = (av, bw)$. Then M isn't free, but it is locally free: let $p = k \times 0$. Then $R_p \cong k$ and $M_p \cong 0 \oplus k^2$.

The next proposition says "Locally 0 is globally 0."

Proposition 2.34. Let M be an A-module. Then

$$M = 0 \text{ iff } M_p = 0 \text{ for all primes } p \subset A \text{ iff } M_{\mathfrak{m}} = 0 \text{ for all maximal ideals } \mathfrak{m} \subset A.$$

Proof. Suppose $0 \neq x \in M$. Then the *annihilator* ideal

$$\mathrm{Ann}(x) = \{a \in A \colon ax = 0\}$$

is not the unit ideal: for example, it doesn't contain 1. Therefore $\mathrm{Ann}(x) \subseteq \mathfrak{m}$ for some maximal $\mathfrak{m}$, which exactly means $x/1 \neq 0 \in M_{\mathfrak{m}}$. □

From this, and from exactness of localization, we deduce that "locally injective is injective; locally surjective is surjective," as follows:

Proposition 2.35. Let $\phi \colon M \to N$ be a morphism of A-modules. Then TFAE:

(1) ϕ is injective;
(2) $\phi_p \colon M_p \to N_p$ is injective for all primes p of A;
(3) $\phi_{\mathfrak{m}} \colon M_{\mathfrak{m}} \to N_{\mathfrak{m}}$ is injective for all maximal ideals $\mathfrak{m}$ of A.

An analogous statement holds for "surjective."

Proof. The exact sequence of A-modules

$$0 \to \ker(\phi) \to M \xrightarrow{\phi} N$$

yields, for each prime p, an exact sequence of A_p-modules

$$0 \to \ker(\phi)_p \to M_p \xrightarrow{\phi_p} N_p.$$

Now ϕ is injective iff $\ker(\phi) = 0$ iff $\ker(\phi)_p = 0$ for all primes p iff ϕ_p is injective for all primes p. (Same for just maximal ideals $\mathfrak{m}$.) □

An analogous proof, using cokernels, holds for local surjectivity.

Now we deduce that flatness is a local property. But first, "localization commutes with tensor products:"

Proposition 2.36. [AM69, Proposition 3.7] Let M, N be A-modules, $S \subset A$ a multiplicative subset. There is a canonical isomorphism of $S^{-1}A$-modules

$$S^{-1}(M \otimes_A N) \to S^{-1}M \otimes_{S^{-1}A} S^{-1}N.$$

Proof. Shall we do it using universal properties? Let T be an arbitrary $S^{-1}A$-module. Then we have isomorphisms

$$\begin{aligned}
\mathrm{Hom}_{S^{-1}A\text{-mod}}(S^{-1}(M \otimes_A N), T) &\cong \mathrm{Hom}_{A\text{-mod}}(M \otimes_A N, T) \\
&\cong \mathrm{Hom}_{A\text{-mod}}(M, \mathrm{Hom}_{A\text{-mod}}(N, T)) \\
&\cong \mathrm{Hom}_{A\text{-mod}}(M, \mathrm{Hom}_{S^{-1}A\text{-mod}}(S^{-1}N, T)) \\
&\cong \mathrm{Hom}_{S^{-1}A\text{-mod}}(S^{-1}M, \mathrm{Hom}_{S^{-1}A\text{-mod}}(S^{-1}N, T)) \\
&\cong \mathrm{Hom}_{S^{-1}A\text{-mod}}(S^{-1}M \otimes_{S^{-1}A} S^{-1}N, T),
\end{aligned}$$

using repeatedly that

$$\mathrm{Hom}_{A\text{-mod}}(X, T) = \mathrm{Hom}_{S^{-1}A\text{-mod}}(S^{-1}X, T)$$

for X any A-module, by adjunction of extension and restriction of scalars. Now, if you believe that all these identifications are natural, then we are done. □

Ideally, [AM69, Exercise 2.15] should be studied before proving the following lemma.

Lemma 2.37. Let $f\colon A \to B$. Let M be a flat A-module, and N a flat B-module.

(1) $M \otimes_A B$ is a flat B-module. (This is [AM69, Exercise 2.20])
(2) N is a flat A-module, supposing that B is a flat A-algebra.

Proof. For (1), the point is that for any B-module X,

$$X \otimes_B (B \otimes_A M) \cong X \otimes_A M$$

(It is worth thinking this through, using the bimodule structure of the LHS as in Exercise 2.15.)

For (2), if $M' \to M$ is an injection of A-modules, then

$$M' \otimes_A B \otimes_B N \to M \otimes_A B \otimes_B N$$

is injective by flatness first of B and then of N. □

Proposition 2.38. Flatness is local. That is, if M is an A-module, then M is flat iff M_p is flat for all primes p iff $M_{\mathfrak{m}}$ is flat for all maximal ideals $\mathfrak{m}$.

Proof. First of all, if M is flat then M_p is flat: we just showed in the Lemma that the extension of a flat module is flat. That is (1) implies (2), and (2) implies (3) is formally true.

Now for (3) implies (1), say $N' \to N$ is an injective map of A-modules. We want to show $N' \otimes M \to N \otimes M$ is injective. What we know is that $N'_{\mathfrak{m}} \to N_{\mathfrak{m}}$ is injective for all maximals $\mathfrak{m}$, hence

$$N'_{\mathfrak{m}} \otimes_{A_{\mathfrak{m}}} M_{\mathfrak{m}} \to N_{\mathfrak{m}} \otimes_{A_{\mathfrak{m}}} M_{\mathfrak{m}}$$

is injective for all maximals $\mathfrak{m}$, by flatness of $M_{\mathfrak{m}}$. Hence

$$(N' \otimes_A M)_{\mathfrak{m}} \to (N \otimes_A M)_{\mathfrak{m}}$$

is injective for all $\mathfrak{m}$, hence $N' \otimes_A M \to N \otimes_A M$ is injective. □

Later on, we will understand flatness more geometrically.

23. Integral extensions

Let $f\colon A \to B$ a ring homomorphism; commonly an inclusion of $A \subset B$.

Definition 2.39. An element $x \in B$ is *integral* over A if it satisfies a monic polynomial over A:

$$x^n + f(a_1)x^{n-1} + \cdots + f(a_n) = 0 \in B$$

for some $n > 0$ and $a_i \in A$.

We'll just write

$$x^n + a_1 x^{n-1} + \cdots + a_n = 0,$$

viewing this as an equation in B, with A-module structure.

Example 2.40. $f(A)$ integral over A: one may take a monic polynomial of degree 1.

Example 2.41. $\mathbb{Z} \hookrightarrow \mathbb{Q}$. Are there any $\alpha \in \mathbb{Q}$ integral over $\mathbb{Z}$ other than $\alpha \in \mathbb{Z}$?

Write $\alpha = r/s$, $(r, s) = 1$. Then multiply both sides of

$$\alpha^n + a_1 \alpha^{n-1} + \cdots + a_n = 0$$

by s^n to obtain

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

so $s | r^n$ so $s = \pm 1$, so $\alpha \in \mathbb{Z}$.

Example 2.42. In fact, for any unique factorization domain A, the only elements of $\operatorname{Frac} A$ that are integral over A are in A. Why? Well, the proof above works verbatim!

In fact the integral elements of B over A form a *subring* of B. I think this is not really obvious: given x, y satisfying monic polynomials over A, how to cook up a monic polynomial satisfied by $x + y$ or xy? We'll prove this after some supporting propositions, starting with the following.

Let $f \colon A \to B$ a ring homomorphism, and $x \in B$. Let

$$A[x] := \operatorname{im}(A[t] \to B),$$

where $t \mapsto x$; thus $A[t]$ is the smallest sub-A-algebra of B containing x.

Proposition 2.43. [AM69, Proposition 5.1] TFAE:

(1) x is integral over A,
(2) $A[x]$ is a finitely generated A-module,
(3) $A[x]$ is contained in a subring $C \subseteq B$ such that C is a finitely generated A-module,
(4) There exists a faithful $A[x]$-module M which is finitely generated as an A-module.

Definition 2.44. A *faithful* A-module M is one where $A \to \operatorname{End}(M)$ is injective; so the terminology is just like group actions: recall that a group action of G on a set X is faithful if $G \to \operatorname{Sym}(X)$ is injective.

Equivalently, M is a faithful A-module iff its annihilator is trivial. In symbols, $\operatorname{Ann} M = 0$, where $\operatorname{Ann} M = \{x \in A : xM = 0\}$. This equivalence is an exercise.

Example 2.45. If $f \colon A \to B$ is any ring homomorphism then B is faithful as an A-module iff $\ker f = 0$. After all, $A \to \operatorname{End}(B)$ factors as $A \to B \subset \operatorname{End}(B)$, with kernel $\ker f$.

Proof. (Proof of Proposition 2.43)

(1) implies (2): If x satisfies a monic polynomial of degree n, then $A[x]$ fg by $1, x, x^2, \ldots, x^{n-1}$: just keep expanding $x^n = -(a_1 x^{n-1} + \cdots + a_n)$.

(2) implies (3): simply take $C = A[x]$.

(3) implies (4): simply take $M = C$. Then C is a faithful $A[x]$-module, since $A[x]$ is a subring of it.

(4) implies (1): this is the key point: the Cayley-Hamilton theorem. We have an A-linear map $x\colon M \to M$ sending $m \mapsto xm$. Then by C-H,

$$x^n + a_1 x^{n-1} + \cdots + a_n = 0$$

for some $a_i \in A$, *an equality of endomorphisms of* M. But this means $x^n + a_1 x^{n-1} + \cdots + a_n = 0$ *as elements of* $A[x]$, because of faithfulness of M.

□

Corollary 2.46. Let $f\colon A \to B$ and let $x_1, \ldots, x_n \in B$ integral over A. Then $A[x_1, \ldots, x_n]$ is a finitely generated A-module.

Proof. Induction on n, with the base case $n = 0$ being clear (A is a fg A-module). For the inductive step, suppose $A[x_1, \ldots, x_{n-1}]$ is a fg A-module; then x_n is integral over $A[x_1, \ldots, x_{n-1}]$ (it's even integral over A). Then $A[x_1, \ldots, x_{n-1}, x_n]$ is finitely generated as an $A[x_1, \ldots, x_{n-1}, x_n]$-module, so also as an A-module.

(What we used is that if $A \to A'$ is a ring hom making A' a fg A-module, and M is a fg A'-module, then also M is fg as an A-module.) □

Corollary 2.47. Let $f\colon A \to B$ a ring hom. The set C of elements over B that are integral over A is a subring of B, called the *integral closure* of A in B.

Proof. Let $x, y \in C$; we just want to show $x + y, x - y, xy \in C$. Well $A[x, y]$ is a subring of B which is fg A-module as just shown; by (3) implies (1) we get that every element of $A[x, y]$ is integral over A. That includes $x + y, xy$, etc. □

Definition 2.48. Define finite type, finite algebras.

So finite always implies finite type, but not conversely. A lot of the above discussion may be summarized as

$$\boxed{\text{finite type} + \text{integral} = \text{finite}}$$

Proposition 2.49. Let $f\colon A \to B$. Then B is finite over A iff B is finite type and integral.

Proof. If B is finite over A, then B finite type, as already argued. Moreover B is integral over A: any $x \in B$ lives in a subring of B, namely B itself, fg as an A-module.

Conversely, if B is finite type, there exist $x_1, \ldots, x_n \in B$ with $A[x_1, \ldots, x_n] = B$. Since $x_1, \ldots, x_n$ is integral, B is a fg A-module, i.e., a finite A-algebra. □

Some basic properties, that integrality is preserved under quotients and localization, shall be useful shortly:

Proposition 2.50. [AM69, Proposition 5.6] Let $A \subseteq B$ rings, B integral over A.

(1) Then B/q is integral over A/q^c, for q a prime of B.
(2) Let $S \subseteq A$ be a multiplicative subset of A (and hence of B as well.) Then $S^{-1}B$ is integral over $S^{-1}A$.

(Make sure we agree that we have an inclusion $S^{-1}A \subseteq S^{-1}B$ in the first place.)

Proof. (1): Write $p = q^c$. Then in the proposition, we are considering the natural inclusion $A/p \subseteq B/q$, sending $a + p \mapsto a + q$. The point is that for any $x + q \in B/q$, an equation $x^n + a_1 x^{n-1} + \cdots + a_n = 0$ reduces mod q. (in particular the a_i reduce to $a_i + q \in A/p$.)

Similarly, for (2), a monic polynomial for $x \in B$ over A can be massaged into a monic polynomial for $x/s \in S^{-1}B$ over $S^{-1}A$. Precisely,

$$x^n + a_1 x^{n-1} + \cdots + a_n = 0 \in B$$

yields

$$(x/s)^n + (a_1/s)(x/s)^{n-1} + \cdots + a_n/s^n = 0 \in S^{-1}B.$$

□

24. Going up theorem

We continue to follow A&M closely for this section. The goal is to prove the following two results:

Theorem 2.51. ([AM69, 5.10], **Lying over theorem**) Let $A \subseteq B$ integral extension of rings. Then any prime p of A is a contraction of some prime q of B.

This will take a little work. Assuming it for a moment, let us deduce

Theorem 2.52. ([AM69, 5.11], **Going up theorem**)

Let $A \subseteq B$ integral extension of rings. If $p_1 \subseteq p_2$ primes in A and q_1 a prime in B such that $q_1^c = p_1$, the there exists q_2 a prime of B containing q_1 with $q_2^c = p_2$.

The statement in the book is phrased in terms of a chain of n prime ideals; this can be recovered from our statement by applying it repeatedly.

Proof. (Proof of going up theorem, assuming [AM69, 5.10].) Let $\overline{A} = A/p_1$, $\overline{B} = B/q_1$, so $\overline{B}$ is integral over $\overline{A}$ (since integrality preserved by quotients). Then $\overline{p_2}$ is the contraction of some prime r of $\overline{B}$, and $r = \overline{q_2}$ for some prime q_2 of B

Now $q_2^c = p_2$ simply follows from $\overline{q_2}^c = \overline{p_2}$. □

So it remains to prove the lying over theorem.

25. Lying over theorem, proof

A rough summary of the strategy is: we want to know something about all primes. We can turn an arbitrary prime into a maximal ideal by localization. We can turn an arbitrary maximal ideal into 0 of a field by quotienting. Then we just need to study integral extensions of fields, which we do by hand. All along, integrality is preserved since its preserved by localization and quotient. Now we do the steps in the reverse order: fields, maximal ideals, arbitrary primes.

Proposition 2.53. ([AM69, 5.7]) Suppose $A \subseteq B$ is an inclusion of domains and B integral over A. Then B is a field iff A is a field.

Proof. Say A a field, $y \in B$ nonzero. We want to leverage the fact that y satisfies a monic polynomial

$$y^n + a_1 y^{n-1} + \cdots + a_{n-1} y + a_n = 0$$

to find a multiplicative inverse for y. Indeed, we may assume the monic polynomial above is of smallest possible degree. Rearrange:

$$y(y^{n-1} + \cdots + a_{n-1}) = -a_n.$$

Now if $a_n = 0$, then $y \neq 0$ implies y satisfies a monic poly of lower degree, since B is a domain. So a_n is a unit, since A a field. So y·thing is a unit, so y is a unit.

Say B a field, and $x \in A$ is nonzero. We want to show that the inverse x^{-1} of x, an element in B, is actually in A, by using the fact that x^{-1} is *integral* over A. We have

$$x^{-m} + a_1' x^{-m+1} + \cdots + a_m' = 0$$

for $a_i' \in A$. Now multiply by x^{m-1} to get

$$x^{-1} + (\text{something in } A) = 0.$$

□

Corollary 2.54. [AM69, 5.8] For $A \subseteq B$ rings with B integral over A, let $q \subseteq B$ prime and $p = A \cap q$ its contraction (thus p is prime in A). Then q maximal iff p maximal.

Proof. We may as well show that B/q is field iff A/p is a field. But we know that B/q is integral over A/p, so done by the previous proposition. □

Corollary 2.55. (**Incomparability**) Let $A \subseteq B$ be rings, B integral over A. If $q \subseteq q'$ are prime ideals of B with $q^c = q'^c = p$, then $q = q'$.

(The slogan "incomparability" remembers that if two primes of B have the same contraction, they must be incomparable.)

Proof. First observe that if p is maximal then we conclude $q = q'$ by the previous statement (why?), and we are done. So our goal is to reduce to the case that p is maximal using localization. Let $S = A \setminus p$, so $S^{-1}A = A_p$ is local with unique maximal ideal pA_p, and $S^{-1}B =: B_p$ but I find the notation B_p unnecessarily confusing and will avoid it.

We have already shown that the extension of rings $S^{-1}A \subseteq S^{-1}B$ is integral. Moreover $q \subseteq q'$ are in (inclusion-preserving) correspondence with primes of $S^{-1}B$, whose contractions contain the maximal ideal pA_p and hence *are* pA_p. Therefore q and q' correspond to the same prime of $S^{-1}B$, and hence are the same. □

Proof. (Proof of Lying Over Theorem). Remember: given p in A we want to construct q in B "lying over" A. We'll do it in two steps: first, suppose we're in the special case that p is the unique maximal ideal of A. Then *any* maximal ideal q of B lies over p; indeed, q^c is *some* maximal ideal of A, and there's only one of those.

Second, in the general case, use localization to turn an arbitrary ideal p into the unique maximal ideal of A_p. Precisely: Let $S = A \setminus p$. Have commutative square

$$\begin{array}{ccc} A & \longrightarrow & B \\ {\scriptstyle\alpha}\downarrow & & \downarrow{\scriptstyle\beta} \\ S^{-1}A & \longrightarrow & S^{-1}B \end{array}$$

in which both horizontal arrows are integral ring extensions. Let $\mathfrak{n}$ be an ideal of $S^{-1}B$ with $\mathfrak{n} \cap S^{-1}A = pA_p$; we just showed that any maximal ideal of $S^{-1}B$ will do. Then $\beta^{-1}\mathfrak{n}$ contracts to p: go around the diagram the other way to see this. □

Let us discuss the going up theorem for integral extensions a bit. (Then we will hopefully discuss it again once we do some geometry.)

Definition 2.56. Define Krull dimension.

Proposition 2.57. If $A \subseteq B$ is an integral extension, then $\dim A = \dim B$.

Proof. It suffices to be able to produce, given a chain of primes in A, a chain of primes in B of equal length, and vice versa. Going from a chain in A in a chain in B is the Lying Over and Going up theorems, and going from a chain in B to a chain in A is the Incomparability theorem applied to the contractions. □

26. Noether normalization and Nullstellensatz

Theorem 2.58. (**Noether normalization.**) Let A a nonzero fg k-algebra. Then there is a finite injective homomorphism of k-algebras

$$k[T_1, \dots, T_d] \hookrightarrow A$$

for some $d \geq 0$.

Note: "finite" can be equivalently replaced by "integral" since everything is finite type. This is a standard result proved in many algebra books; I'll follow Liu Algebraic Geometry and Arithmetic Curves.

Proof. (Proof of Noether normalization.) Have $A \cong k[x_1, \dots, x_n]/I$. By induction on n, with $n = 0$ done. If $I = 0$ done. Else, pick any nonzero polynomial $P \in I$. What would be lucky is if P were monic as a polynomial in x_n, say: then

$$A' = k[x_1, \dots, x_{n-1}]/(I \cap k[x_1, \dots, x_{n-1}]) \hookrightarrow k[x_1, \dots, x_n]/I = A$$

is an injective integral homomorphism, and now we win by induction.

The general strategy is to prove there is a change of variables to get into the lucky case. suppose we could find integers $m_1, \dots, m_{n-1}$ (think: ridiculously large integers) such that $P(x_1 - x_n^{m_1}, \dots, x_{n-1} - x_n^{m_{n-1}}, x_n)$ is monic in x_n. Then we are done for the same reason as before: consider the map

$$\phi \colon k[s_1, \dots, s_{n-1}] \to k[x_1, \dots, x_n]/I = A$$

sending $s_i \mapsto x_i - x_n^{m_i}$. Factoring out the kernel, get an injective extension

$$A' = k[s_1, \dots, s_{n-1}]/\ker \phi \hookrightarrow A$$

which we claim makes A integral over A'. Indeed, x_n satisfies the monic polynomial P over A', so is integral over A'. And so are each $x_i - x_n^{m_i}$. Hence all x_i are.

The only thing that remains to be shown is that such m_i can actually be chosen. Exercise! But it's a believable exercise. □

Remark 2.59. There is proof for k infinite which is perhaps more intuitive, as it involves linear changes of coordinates rather than monomial changes of coordinates. (Follow [AM69, Exercise 5.16].)

Corollary 2.60. If B a fg k-algebra and $\mathfrak{m}$ a maximal ideal, then $B/\mathfrak{m}$ is a finite extension of k.

Proof. Applying Noether normalization to $B/\mathfrak{m}$, we obtain the existence of an integral extension

$$k[T_1, \dots, T_d] \subseteq B/\mathfrak{m}.$$

But for an integral extension of domains, one is a field iff the other is a field (as we have shown). So $d = 0$. Now an integral extension of k which is finite type as a k-algebra is finite. □

Corollary 2.61. (**Weak Nullstellensatz)** Let k be algebraically closed. The maximal ideals of $k[T_1, \dots, T_d]$ are

$$\{(T_1 - \alpha_1, \dots, T_d - \alpha_d) : (\alpha_1, \dots, \alpha_d) \in k^n.\}$$

Proof. First argue these are maximal; they are kernels of evaluation maps.

Conversely, if $\mathfrak{m} \subset k[T_1, \dots, T_d]$ is maximal, then $\phi\colon k \xrightarrow{\cong} k[T_1, \dots, T_d]/\mathfrak{m}$ is a finite extension of k, hence is k itself. Let $\alpha_i \in k$ such that $\phi(\alpha_i) = \overline{\alpha_i} = \overline{T_i}$; here we used that ϕ is a map of k-algebras, i.e., fixes the field k. Conclude $T_i - \alpha_i \in \mathfrak{m}$ for each i. □

Proposition 2.62. In a nonzero fg k-algebra A, $\operatorname{Jac} A = \operatorname{Nil} A$.

Proof. Suppose $f \in A \setminus \operatorname{Nil} A$. To show $f \notin \operatorname{Jac} A$. Have $\phi\colon A \to A_f \neq 0$, so there is a maximal ideal $\mathfrak{m} \subset A_f$. Then in the inclusion of k-algebras

$$A/\phi^{-1}(\mathfrak{m}) \subseteq A_f/\mathfrak{m}$$

the RHS is a finite field extension of k (Corollary of Weak Nullstellensatz); note A_f is finitely generated over k since A was. Thus LHS is also a finite k-module. But a domain that is a finite k-module is a field. (Indeed, already proved that for an integral extension of domains, field iff field. Alternatively, prove it directly!) □

Part 3. Some algebraic geometry

27. "Elementary" algebraic geometry in a day: Ideals and varieties

Definition 3.1. Let $k = \overline{k}$. Define algebraic subsets of k^n. Give examples of union, intersection. Give examples of two algebraic subsets corresponding to different ideals. Give some nonexamples over $\mathbb{R}$.

Theorem 3.2. (Strong Nullstellensatz). Let $k = \overline{k}$, $J \subseteq k[T_1, \dots, T_n]$ an ideal. If $F \in k[T_1, \dots, T_n]$ with $F(\alpha) = 0$ for all $\alpha \in Z(J)$, then $F \in \sqrt{J}$.

Hence

$$I(Z(J)) = \sqrt{J}.$$

Hence algebraic subsets and radical ideals are in (inclusion-reversing) bijection.

Proof. Want $F \in \operatorname{Nil} k[T_1, \ldots, T_n]/J = \operatorname{Jac} k[T_1, \ldots, T_n]/J$. But by the weak Nullstellensatz, this happens iff $F \in (T_1 - \alpha_1, \ldots, T_n - \alpha_n)$ for $(\alpha_1, \ldots, \alpha_n) \in Z(J)$. This happens iff $F(\alpha_1, \ldots, \alpha_n) = 0$ for each $(\alpha_1, \ldots, \alpha_n) \in Z(J)$. □

Do the basic operations: $\cap Z(I_i) = Z(\sum I_i)$, $Z(I) \cup Z(J) = Z(IJ) = Z(I \cap J)$. Define Zariski topology on $\mathbb{A}^n_k$.

28. Spec

Definition 3.3. Define Spec. Define Zariski topology. Check it's a topology.

Exercise 3.4. A new phenomenon: non-closed points. Check that $\overline{\{p\}} = \{q : q \supseteq p\}$.

Example 3.5. Let $k = \overline{k}$. The plane $\mathbb{A}^2_k$. Recall in this case, a prime $p \subset k[x_1, \ldots, x_n]$ is determined exactly by the maximal ideals containing it: $p = \cap_{\mathfrak{m} \supseteq p} \mathfrak{m}$, since $k[x_1, \ldots, x_n]/p$ has nilradical equal to Jacobson radical.

Definition 3.6. A *base* of a topology on a set X is a subcollection $\mathcal{B}$ of open sets such that every open is a union of elements of the base.

Definition 3.7. Define the base $\mathcal{B}$ of *distinguished opens* D_f of $\operatorname{Spec} A$. Check that an arbitrary open set $V(I)^c$ is a union of elements of the base.

Definition 3.8. A map of rings induces a continuous map of prime spectra. Thus $\operatorname{Spec} \colon \mathbf{Ring}^{\mathrm{op}} \to \mathbf{Top}$ is a functor.

Do examples. Do an example of an integral extension, say $k[x^2] \to k[x]$ which illustrates Noether Normalization.

Definition 3.9. A *presheaf* is nothing but a contravariant functor!

Give an example of presheaves of continuous functions, say.

Definition 3.10. Define the presheaf of rings $\mathcal{O}_{\operatorname{Spec} A} \colon \mathcal{B}^{\mathrm{op}} \to \mathbf{Ring}$ on the distinguished open sets of $\operatorname{Spec} A$.

Remark 3.11. In fact, the presheaf $\mathcal{O}_{\operatorname{Spec} A}$ forms a *sheaf* on $\operatorname{Spec} A$: a presheaf with favorable gluability properties (this will be defined formally in 2050).

In Math 2050, we shall assert that a map $f\colon B \to A$ naturally defines a morphism of *ringed topological spaces* $(\operatorname{Spec} A, \mathcal{O}_{\operatorname{Spec} A}) \to (\operatorname{Spec} B, \mathcal{O}_{\operatorname{Spec} B})$, and in fact

Spec is a fully faithful functor from $\mathbf{Ring}^{\mathrm{op}}$ to ringed topological spaces.

The essential image of this functor are called affine schemes. That is, an *affine scheme* is a ringed topological space isomorphic to some $(\operatorname{Spec} A, \mathcal{O}_{\operatorname{Spec} A})$. Then a *scheme* is a ringed topological space locally isomorphic to an affine scheme. Thus $\operatorname{Spec} A$ for rings A play the role of $\mathbb{R}^n$s in manifolds: they are the local patches!

29. Primary decomposition: existence in Noetherian rings

This follows A&M Chapters 4 and 7 closely.

Definition 3.12. Define primary ideal. Equivalently: I is primary if every zero divisor in A/I is nilpotent.

Example 3.13. Which ideals of $\mathbb{Z}$ are primary?

These are the building blocks of ideals, at least over a Noetherian ring: in such a ring, every ideal has a *primary decomposition*.

Definition 3.14. A *primary decomposition* of an ideal I is an expression of I as an intersection of finitely many primary ideals.

The primary decomposition in general may not be unique, but there are some partial uniqueness statements that can be obtained.

Lemma 3.15. If I is primary then $p := \sqrt{I}$ is prime: if $fg \in p$ then $f^n g^n \in I$. So either $f^n \in I$ or $g^{nN} \in I$. In this situation I is called p-primary.

Example 3.16. The converse is not true: (xy, y^2) is not primary (discuss picture) but the radical is prime. However:

Lemma 3.17. If I is an ideal of A with $\sqrt{I}$ *maximal*, then I is primary.

Proof. By passing to A/I, may as well assume $I = 0$, so $\operatorname{Nil}(A)$ is a maximal ideal. Then $\operatorname{Nil}(A)$, being contained in all primes, is the *unique* maximal ideal, whose complement in A must therefore consist exactly of the units of A. Then a zero divisor of A, not being a unit, must be nilpotent. □

Example 3.18. Now we can exhibit several primary decompositions of (xy, y^2).

Theorem 3.19. In a Noetherian ring, every ideal has a primary decomposition.

Before proving the proposition, it is worth reviewing the equivalent finiteness properties of Noetherian rings:

Lemma 3.20. Let A be a ring. TFAE, and if they hold the ring is called *Noetherian*:

(1) Every ideal is fg.
(2) Every ascending chain $I_1 \subseteq I_2 \subseteq \cdots$ stabilizes.
(3) Every nonempty collection $\mathcal{I}$ of ideals has a maximal element.

Proof. For (2) implies (3): (**Revised from class!**) Suppose $\mathcal{I}$ has no maximal element. Pick any I_1 in $\mathcal{I}$; since it is not maximal, it is strictly contained in some I_2, and so on. Obtain an ascending chain $I_1 \subsetneq I_2 \subsetneq \cdots$ which does not stabilize.

For (3) implies (2): Given an ascending chain $I_1 \subseteq I_2 \subseteq \cdots$, consider a maximal element I_N: then $I_N = I_{N+1} = \cdots$ so the chain stabilizes. □

Definition 3.21. I is called *irreducible* if whenever $I = J \cap L$ then either $J = I$ and $J = L$. Otherwise it is called *reducible*.

Example 3.22. Which ideals of $\mathbb{Z}$ are irreducible?

Lemma 3.23. In a Noetherian ring, every ideal is the intersection of finitely many irreducible ideals.

Proof. Let $\mathcal{I}$ be the collection of *counterexamples*, and assume $\mathcal{I}$ is nonempty, so has a maximal element I. Now I, being a counterexample, is reducible (since it can't be the intersection of *just one* irreducible ideal, I itself). So $I = J \cap L$ where both J, L are strictly larger. Therefore J, L are not in $\mathcal{I}$, and each admit expressions as intersections of finitely many irreducibles. □

Lemma 3.24. In a Noetherian ring, an irreducible ideal is primary.

Proof. ([AM69, 7.12]) Passing to the quotient ring, it suffices to prove that if (0) is irreducible then (0) is primary. Say $xy = 0$, but $y \neq 0$. If we could show that $(0) = (x^n) \cap (y)$ for some n then we'd be done: since (0) is irreducible and $(y) \not\supseteq (0)$ is strictly larger, then $(x^n) = (0)$.

Consider the chain

$$\operatorname{Ann}(x) \subseteq \operatorname{Ann}(x^2) \subseteq \cdots$$

which stabilizes: $\operatorname{Ann}(x^n) = \operatorname{Ann}(x^{n+1})$.

So suppose $a \in (x^n) \cap (y)$, and let's deduce $a = 0$. Since $a \in (y)$, and y annihilates x, so does a. And since $a = bx^n$, bx^n annihilates x: $bx^{n+1} = 0$. So b annihilates x^{n+1}. So b annihilates x^n. So $a = bx^n = 0$. □

Then the theorem follows from the two lemmas: every ideal in a Noetherian ring admits a primary decomposition.

30. Primary decomposition, continued: uniqueness theorems

Following A&M Chapter 4 closely.

Lemma 3.25. ([AM69, 4.3]) The intersection of p-primary ideals is again p-primary.

Proof. Let q_i be p-primary, $i = 1, \ldots, n$. The radical of the intersection is the intersection of the radicals, so $\sqrt{\cap q_i} = p$. It just remains to prove $\cap q_i$ is primary. Let $xy \in \cap q_i$ and $y \notin \cap q_i$. Then $y \notin q_i$ for some i. Then $x \in \sqrt{q_i} = p$, which is all we wanted to show. □

Lemma 3.26. ([AM69, 4.4]) Let q be a p-primary ideal, and let $x \in A$. Then

(1) if $x \in q$ then $(q : x) = (1)$
(2) if $x \notin q$ then $(q : x)$ is p-primary
(3) if $x \notin p$ then $(q : x) = q$.

Example 3.27. Do a monomial example like $q = (x^2, xy, y^2)$.

Proof. We prove (2). First we prove $\sqrt{(q : x)} = p$. Since $(q : x)$ can only be bigger than q, we already have $\sqrt{(q : x)} \supseteq p$. For the other inclusion, if $y^n \in (q : x)$ then $xy^n \in q$ and $x \notin q$ implies $y \in \sqrt{q} = p$.

It remains to prove that $(q : x)$ is primary. Say $yz \in (q : x)$ with $y \notin p$. Then $xyz \in q$ implies $xz \in q$, so $z \in (q : x)$ as desired. □

Next we want to prove a partial uniqueness theorem for primary decompositions. But we want to rule out silly stuff: if $I = q_1 \cap \cdots \cap q_n$ is a primary decomposition of I, say it's *irredundant* if

(1) the primes $p_i = \sqrt{q_i}$ are pairwise distinct, and
(2) $q_i \not\supseteq \cap_{j \neq i} q_j$ for all i.

The primary decomposition is called *redundant* otherwise. The point is that if your pd is redundant, then you can make it smaller. If (1) fails, say q_α and q_β are both p-primary, then replace them by $q_\alpha \cap q_\beta$, which we have already proved is again p-primary. If (2) fails, just drop the q_i from the primary decomposition.

Definition 3.28. (**Associated primes**) Given an ideal I admitting a primary decomposition (for example, any ideal in a Noetherian ring), the *associated primes* of I are the prime ideals in the set

$$\{\sqrt{(I : x)} \mid x \in A\}.$$

Theorem 3.29. ([AM69, 4.5] **First uniqueness theorem of primary decomposition**) Suppose $I = q_1 \cap \cdots q_n$ is an irredundant primary decomposition. Let $p_i = \sqrt{q_i}$ for each i. Then the p_is are exactly the associated primes of I; in particular, they depend only on I, and are independent of choice of primary decomposition.

Example 3.30. Examine this theorem in our favorite example (y^2, xy), which has lots of pds for example

$$(y^2, xy) = (y) \cap (x - ay, y^2), \quad a \in k.$$

We need a lemma:

Lemma 3.31. ([AM69, 1.11]) If a prime p contains an intersection of finitely many ideals $\cap I_i$, then p contains some individual ideal I_i. Hence $p = \cap I_i$ implies $p = I_i$ for some i.

Proof. (Proof of Lemma) If $p \not\supseteq I_i$ for each i, say f_i is a witness; that is, $f_i \in I_i \setminus p$. Then $\prod f_i \in \cap I_i \setminus p$. □

Proof. (Proof of first uniqueness theorem) First let us show that p_1, say, is an associated prime. By irredundancy, there exists $f \in (q_2 \cap \cdots \cap q_n) \setminus q_1$. Then

$$(I : f) = (\cap q_i : f) = \cap (q_i : f) = (q_1 : f) \cap (1) \cap \cdots (1) = (q_1 : f),$$

which we already showed is p_1-primary. So $p_1 = \sqrt{(I : f)}$ is an associated prime.

Second, suppose $\sqrt{(I : f)}$ is prime for some f; let us show that it appears among the p_i. We have

$$\sqrt{(I : f)} = \sqrt{\bigcap (q_i : f)} = \bigcap \sqrt{(q_i : f)}.$$

Remember that we proved that $(q_i : f)$ is (1) if $f \in q_i$ and is p_i-primary otherwise. So the last intersection is

$$\bigcap_{q_i \not\ni f} p_i.$$

So by the lemma, since $\sqrt{(I : f)}$ is prime by assumption, it is equal to some p_i. □

Definition 3.32. Define minimal, embedded primes.

This terminology is completely inscrutable without pictures!

We close by stating the following partial uniqueness theorem. It is good to know, but we will not prove it.

Theorem 3.33. ([AM69, 4.11], Second uniqueness theorem) The *minimal* primary components, i.e., the primary components of an irredundant decomposition which correspond to minimal primes, are independent of choice of primary decomposition.

31. Normal domains; normalization

Definition 3.34. Let A be an integral domain.

(1) The *normalization* of A is its integral closure in $\operatorname{Frac} A$.
(2) We say A is *integrally closed* or *normal* if it is already integrally closed in its fraction field.

Example 3.35. We already proved that UFDs are normal.

Example 3.36. An interesting non-example: The ring

$$A = \frac{\mathbb{C}[x,y]}{(y^2 - x^2 - x^3)}$$

is a domain: $y^2 - x^2 - x^3$ is irreducible. (Can you prove it?) It is not normal: consider $u = y/x \in \operatorname{Frac} A$. Then $u^2 - x - 1 = 0$. So the normalization of A at least contains u.

We claim that $A[u] \cong \mathbb{C}[u]$, more precisely that

$$\begin{array}{ccc} A & \longrightarrow & \operatorname{Frac} A \\ & \searrow \quad \nearrow & \\ & \mathbb{C}[u] & \end{array}$$

is a commuting diagram of injections, where $x \mapsto 1 - u^2,\ y \mapsto u(1-u^2)$ on the left and $u \mapsto y/x$ on the right.

Exercise 3.37. Check all those assertions.

Then $\mathbb{C}[u]$, being a UFD, is integrally closed, so $\mathbb{C}[y/x]$ is the integral closure of A.

Now draw the pictures to see what you got! Here normalization separates analytic branches: the two points $u = \pm 1$ on the u-line map to the node $x = y = 0$ on $\operatorname{Spec} A$.

By the way, there is a universal property: for A a domain, the map $A \to A^\nu$ to the normalization of A is initial among all injections of A to normal domains.

Proposition 3.38. ("Normalization commutes with localization") Let $A \subseteq B$, C the integral closure of A in B. Let $S \subset A$ be a multiplicative subset. Then $S^{-1}C$ is the integral closure of $S^{-1}A$ in $S^{-1}B$.

Proof omitted; see [AM69, 5.12]. Discuss the geometric utility of this.

Part 4. A little homological algebra

We will follow [Wei94], and perhaps [Eis95].

Say $F\colon \mathcal{A} \to \mathcal{B}$ is an additive functor on abelian categories that is *right exact*. We wish it were exact, but it isn't. So we wish to measure failure of left exactness. We will do so

using *left derived functors.* We will study in detail the case of *Tor*, the left derived functor of tensor.

The analogous story for left exact functors is left as an exercise in flipping everything, with projective objects replaced by injective objects. A common one is *Ext*. Another important one arising in geometry is the higher cohomology groups of sheaves.

32. Projective objects

Given an object N in any abelian category, "recall" that the functor

$$\mathrm{Hom}(N, -)\colon \mathcal{A} \to \mathcal{A}$$

is automatically a left exact functor. (We proved this for R-modules by exhibiting it as a right adjoint, in fact).

Definition 4.1. An object P in an abelian category $\mathcal{A}$ is *projective* if $\mathrm{Hom}(P, -)$ is an exact functor.

Example 4.2. In R-mod, free modules are projective. (Check this slowly.) In fact a standard exercise is to show that an R-module is projective if and only if it's a direct summand of a free module.

Remark 4.3. Projective modules are very close to locally free. Exercise: a *finitely presented* module M is projective iff it is locally free. So projective modules over R play the role of algebraic vector bundles over $\operatorname{Spec} R$.

Definition 4.4. Say that an abelian category $\mathcal{A}$ *has enough projectives* if every object A admits an epimorphism $P \to A$ from a projective.

Example 4.5. So, for example, R-mod has enough projectives: every module is the surjective image of a free module.

Note right away that if $\mathcal{A}$ has enough projectives then every object A admits a projective resolution:[6]

Definition 4.6. **(Projective resolution)** A projective resolution of A is a complex

$$\cdots P_2 \to P_1 \to P_0 \to 0 \to \cdots$$

together with a map $P_0 \xrightarrow{\varepsilon} A$ such that the augmented sequence

$$\cdots P_2 \to P_1 \to P_0 \xrightarrow{\varepsilon} A \to 0$$

is an exact complex.

[6]First make sure we agree on what a *complex* is.

Proposition 4.7. If $\mathcal{A}$ has enough projectives then every object A admits a projective resolution.

Proof. Hit A with an epimorphism ε from some projective P_0. Then hit $\ker \varepsilon$ with an epimorphism from some projective P_1, and so on. □

33. Derived functors

Fix $F\colon \mathcal{A} \to \mathcal{B}$ a right exact additive functor of abelian categories, and assume $\mathcal{A}$ has enough projectives. We are going to define

(1) a sequence of functors
$$L_0F = F,\ L_1F,\ L_2F, \ldots : \mathcal{A} \to \mathcal{B}$$
called the *left derived functors* of F;
(2) for every short exact sequence
$$0 \to A \to B \to C \to 0$$
maps
$$\delta_i\colon L_iF(C) \to L_{i-1}F(A),$$

such that

- For every short exact sequence
$$0 \to A \to B \to C \to 0$$
there is a long exact sequence
$$\cdots \xrightarrow{\delta_2} L_1FA \to L_1FB \to L_1FC \xrightarrow{\delta_1} L_0FA \to L_0FB \to L_0FC \to 0 \tag{1}$$
- the δ_i are compatible with morphisms of SES in the sense that whenever you have a morphism of SES
$$\begin{array}{ccccccccc} 0 & \longrightarrow & A' & \longrightarrow & B' & \longrightarrow & C' & \longrightarrow & 0 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 0 & \longrightarrow & A & \longrightarrow & B & \longrightarrow & C & \longrightarrow & 0 \end{array}$$
the following squares commute for all i:
$$\begin{array}{ccc} L_iFC' & \xrightarrow{\delta} & L_{i-1}FA' \\ \downarrow & & \downarrow \\ L_iFC & \xrightarrow{\delta} & L_{i-1}FA \end{array} . \tag{2}$$

The left derived functors of F that we construct satisfy an appropriate universal property, among all such data of the above form. We will not state it precisely.

Now we define the derived functors L_iF, although we will not verify all details. The main thing to know is that they exist, that you will shortly know how to compute them, and that a SES in $\mathcal{A}$ produces a long exact sequence as in Equation (1).

Definition 4.8. **(Definition of left derived functors)** Let $F\colon \mathcal{A} \to \mathcal{B}$ be a right exact additive functor of abelian categories, and suppose $\mathcal{A}$ has enough projectives.

Let A be an object in $\mathcal{A}$. Choose any projective resolution

$$P_\bullet = (\cdots \to P_2 \to P_1 \to P_0)$$

of A. This complex is understood to be 0 in homological degree $-1, -2, \ldots$ Let

$$FP_\bullet = (\cdots \to FP_2 \to FP_1 \to FP_0)$$

Then define

$$L_iF(A) = H_i(FP_\bullet).$$

We omit the following laundry list of things:

(1) Given a map $A \to A'$, there is a natural morphism $L_iFA \to L_iFA'$ in $\mathcal{B}$; in this way, the L_iF are functors.
(2) Independence of choices: different choices of projective resolutions yield functors that are naturally isomorphic to L_iF.
(3) Given a SES $0 \to A \to B \to C \to 0$ in $\mathcal{A}$, there are natural morphisms

$$L_iFC \xrightarrow{\delta_i} L_{i-1}FA,$$

making the two conditions (1) and (2) above hold, and making the universal property of left derived functors (which we never stated precisely) hold.

Proof. Check all of these when you are older. You can read [Wei94, §2.4], for example. □

We will, however, do some more straightforward sanity checks:

Sanity check 1. We have $L_0F = F$.

Proof. At least, we will prove $L_0F(A) \cong F(A)$ for all A. This follows from F being right exact. Namely, choose a projective resolution $P_\bullet$ for A. Since $P_1 \to P_0 \to A \to 0$ is exact, and F is right exact, we have

$$FP_1 \to FP_0 \xrightarrow{\varepsilon} FA \to 0$$

is exact, which says that $FA \cong \operatorname{cok}(FP_1 \to FP_0) = H_0(FP_\bullet)$. □

Sanity check 2. We have $L_iF = 0$ for all $i > 0$ exactly when F is exact. In fact, we have $L_1F = 0$ exactly when F is exact.

Proof. If F is exact, then for a projective resolution $P_\bullet$ of A, we have

$$L_iFA = H_i(\cdots \to FP_2 \to FP_1 \to FP_0 \to 0)$$

but this sequence is exact in homological degree $1, 2, \ldots$ by exactness of F.

Conversely, if $L_iF = 0$ for all $i > 0$, in particular $L_1F = 0$. Then given any SES

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

we get a LES

$$\cdots \to L_1FB \to L_1FC \to FA \to FB \to FC \to 0.$$

But $L_1FC = 0$, so

$$0 \to FA \to FB \to FC \to 0$$

is exact, as desired. □

One more thing to note:

Fact 4.9. If P is a projective object of $\mathcal{A}$ then $L_iF(P) = 0$ for all $i > 0$.

Proof.

$$\cdots \to 0 \to P$$

is a resolution of P, and the complex

$$\cdots \to 0 \to FP$$

has no homology in degrees > 0. □

34. Tor

The left-derived functors of tensor are called Tor.

Definition 4.10. Let N be an R-module. The functor $- \otimes_R N$ from R-mod to R-mod is right exact. We write

$$\mathrm{Tor}_i^R(-, N) \colon R\text{-mod} \to R\text{-mod}$$

for its i^{th} left derived functor.

The name Tor comes from the following special case:

Example 4.11. [Wei94, 3.1.1] For p prime and B an abelian group, let us compute $\mathrm{Tor}_i^{\mathbb{Z}}(\mathbb{Z}/p\mathbb{Z}, B)$. We take a projective (free) resolution

$$0 \to \mathbb{Z} \xrightarrow{\cdot p} \mathbb{Z}$$

of $\mathbb{Z}/p\mathbb{Z}$ and tensor with B to obtain a complex

$$0 \to B \xrightarrow{\cdot p} B.$$

Then $\mathrm{Tor}_i^{\mathbb{Z}}(\mathbb{Z}/p\mathbb{Z}, B)$ can be read off as the homology of this complex:

$$\mathrm{Tor}_i^{\mathbb{Z}}(\mathbb{Z}/p\mathbb{Z}, B) = \begin{cases} B/pB & \text{if } i = 0, \\ \{b \in B : pb = 0\} & \text{if } i = 1, \\ 0 & \text{if } i \geq 2. \end{cases}$$

So $\mathrm{Tor}_1^{\mathbb{Z}}(\mathbb{Z}/p\mathbb{Z}, B)$ is the p-torsion of B.

A useful fact about Tor that we may use but not prove is that, just like the tensor product, it is *symmetric* bilinear:

Proposition 4.12. We have

$$\mathrm{Tor}_i^R(M, N) \cong \mathrm{Tor}_i^R(N, M).$$

Proof. Prove this when you are older, using spectral sequences. (Exercise 23.3.A of Vakil's *The Rising Sea*.) □

35. Tor and flatness

(Recall the definition of a flat module.)

We return to flatness, to try to understand it more geometrically–from its definition, it is quite mysterious. We shall prove a useful characterization of flatness using Tor. We follow [Eis95, Proposition 6.1].

Proposition 4.13. Let M be an R-module, $I \subseteq R$ an ideal. The "multiplication map"

$$I \otimes_R M \to M$$

is injective iff $\operatorname{Tor}_1^R(R/I, M) = 0$.

(Recall the multiplication map, studied on a previous problem set: is obtained by tensoring $I \to R$ with M.)

Proof. The SES

$$0 \to I \to R \to R/I \to 0$$

produces a long exact sequence

$$\cdots \to \operatorname{Tor}_1^R(I, M) \to \operatorname{Tor}_1^R(R, M) \to \operatorname{Tor}_1^R(R/I, M) \to I \otimes M \to M \to M/IM \to 0$$

where the first blue term is 0 since R is projective (indeed free). Therefore $\operatorname{Tor}_1^R(R/I, M) = \ker(I \otimes M \to M)$. □

Proposition 4.14. Let M be an R-module. Then M is flat iff for all finitely generated ideals I, the multiplication map $I \otimes M \to M$ is injective.

Proof. Recall that M is called *flat* if for *all* injections $N' \to N$ of R-modules, the map $M \otimes N' \to M \otimes N$ is injective. So the forward direction follows from considering the injection $I \subseteq R$.

The content of the proposition is the reverse direction. In other words, we need to show that for all injections $N' \subset N$, the map $M \otimes N' \to M \otimes N$ is injective, knowing only that the statement is true for injections of the form $I \subseteq R$ where I is a fg ideal.

First, let's show that for *arbitrary* ideals $I \subseteq R$, the map $I \otimes M \to M$ is injective. Here we actually appeal to the construction of the tensor product[7] Namely, suppose $x = \sum r_i \otimes m_i \in I \otimes M$, with $x \mapsto \sum r_i m_i = 0$. The key point is that x involves only finitely many elements r_i of I. Consider the finitely generated ideal $I' = \langle r_i \rangle$. Then

$$I' \otimes M \to I \otimes M \to M$$

is injective, and takes $\sum r_i \otimes m_i \mapsto x \mapsto 0$. So $x = 0$.

[7] I don't know how to do it only with universal properties!

Second, let's show that for inclusions $N' \subset N$ in which N is *finitely generated*, the map $N' \otimes M \to N \otimes M$ is injective. By throwing generators in one at a time, we may choose a sequence of submodules

$$N' = N_0 \subset N_1 \subset \cdots \subset N_p = N$$

where N_{i+1}/N_i is generated by 1 element. We may as well assume, then, that N/N' itself is generated by 1 element, and show that $N' \otimes M \to N \otimes M$ is injective; then win by induction.

What does it mean for a module M to be generated by 1 element?[8] It means we have a surjection $R \twoheadrightarrow M$, so $M \cong R/I$ for some ideal I.

Now, the SES

$$0 \to N' \to N \to N/N' \to 0$$

produces a LES that ends

$$\cdots \to \operatorname{Tor}_1^R(N/N', M) \to N' \otimes M \to N \otimes M \to N/N' \otimes M \to 0.$$

But $\operatorname{Tor}_1^R(N/N', M) = \operatorname{Tor}_1^R(R/I, M) = 0$ by Proposition 4.13, since we already established that $I \otimes M \to M$ was injective. We are done with the second step.

Third, let's conclude by showing that for *arbitrary* $N' \subseteq N$, with N not necessarily finitely generated, $N' \otimes M \to N \otimes M$ is injective. This is similar in spirit to the first step. Say

$$x = \sum n_i \otimes m_i \mapsto 0 \in N \otimes M.$$

We want to show $x = 0 \in N' \otimes M$.

The *reason* that x is 0 in $N \otimes M$ is that x can be written as an R-linear combination of relations on the symbols $n \otimes m$ that express bilinearity, such as

$$(n + n') \otimes m - n \otimes m - n' \otimes m,$$

et cetera. Let $P' = \langle n_i \rangle$ and let P be generated by the n_i together with the elements of n involved in this finite expression, so P is finitely generated. Then we have $\sum n_i \otimes m_i \mapsto 0 \in P \otimes M$, but $P' \otimes M \to P \otimes M$ is injective by Step 2, so $\sum n_i \otimes m_i = 0 \in P' \otimes M$ and in $N' \otimes M$, done. (Maybe it helps to stare at the following commutative square.)

$$\begin{array}{ccc} P' \otimes M & \longrightarrow & P \otimes M \\ \downarrow & & \downarrow \\ N' \otimes M & \longrightarrow & N \otimes M \end{array}$$

□

Remark 4.15. It is possible to get around directly invoking Tor, at the cost of a clunkier proof. See e.g., [Liu02, Theorem 1.2.4].

[8] Such a module is called a *cyclic* module.

Definition 4.16. An R-module M is *torsion-free* if for all $r \in R$ and $x \in M$, $rx = 0$ only when $r = 0$.

Corollary 4.17. Over a PID R, a module M is flat iff it is torsion-free.

Proof. We proved that M is flat iff for all ideals I, $\operatorname{Tor}_1^R(R/I, M) = 0$. Since $\operatorname{Tor}_1^R(R, M) = 0$, we may restrict our attention to nonzero I, generated by a nonzerodivisor r. Then

$$0 \to R \xrightarrow{\cdot r} R$$

is a resolution of $R/(r)$, so the homology at degree 1 of

$$0 \to M \xrightarrow{\cdot r} M$$

computes $\operatorname{Tor}_1^R(R/(r), M)$. So $\operatorname{Tor}_1^R(R/(r), M) = \{x \in M : rx = 0\}$. Therefore M is flat iff M is torsion-free. □

Example 4.18. Consider $R = k[\varepsilon]/(\varepsilon^2)$. Topologically, $\Delta = \operatorname{Spec} R$ is no different from $\operatorname{Spec} k$, a point. Recall that everything is flat over a field. But unlike over k, flatness over R is not at all an automatic condition: it has to do with *first order deformations*. This will be studied on the homework.

36. Tor and the Hilbert syzygy theorem

I'm using a mix of sources, including [EH00, III.3.3] and [AM69, Chapter 11]. The proof of Hilbert Syzygy Theorem is the one I learned from Adam Boocher, who was my officemate in grad school. It is presumably somewhere in [Eis95, Chapter 19]. We will accept without proof that $\operatorname{Tor}_i^R(M, N) \cong \operatorname{Tor}_i^R(N, M)$.

Let $S = k[x_1, \ldots, x_n]$, regarded as a $\mathbb{Z}$-graded ring with $\deg x_i = 1$, and let M be a graded S-module. This means that $M = \bigoplus_{i \in \mathbb{Z}} M_i$ is $\mathbb{Z}$-graded as an abelian group, with $S_i M_j \subseteq M_{i+j}$. A morphism $\phi : M \to M'$ of graded modules of degree d is a morphism such that $\phi(M_i) \subseteq N_{i+d}$.

For any $b \in \mathbb{Z}$, it will be convenient to define the shifted module $M(b)$ as the graded S-module with

$$M(b)_j = M_{b+j}.$$

This is horribly counterintuitive notation, in that the elements of $M(1)$, say, have degrees shifted *down* by 1.

deg	$\cdots$	-1	0	1	2	$\cdots$
M		$\cdots$	M_0	M_1	M_2	$\cdots$
$M(1)$	$\cdots$	M_0	M_1	M_2	$\cdots$	

We shall be interested in resolutions of finitely generated modules M by graded free modules, i.e., modules that are direct sums of $S(b)$ for various b.

Definition 4.19. A free resolution of M is a complex of graded modules

$$\cdots \to E_2 \to E_1 \to E_0,$$

with each morphism of degree 0 (i.e., degree-preserving), with $E_i = \bigoplus_j S(-b_{ij})$ a direct sum of graded free modules, such that the augmented complex

$$\cdots \to E_2 \to E_1 \to E_0 \to M$$

is exact.

Example 4.20. Let $S = k[x, y, z]$, and let $I = (xy, z)$. Then S/I is a graded S-module. Here's an exact sequence, exhibiting a free resolution of S/I:

$$0 \longrightarrow S(-3) \xrightarrow{\begin{bmatrix} z \\ -xy \end{bmatrix}} S(-2) \oplus S(-1) \xrightarrow{\begin{bmatrix} xy & z \end{bmatrix}} S \longrightarrow S/(xy, z) \longrightarrow 0$$

One can always find a free resolution, in fact a minimal free resolution, of M, greedily. First, identify a minimal set of homogeneous generators for M, say G_i of degree d_i, and hit each G_i with a free module $S(-d_i)$. We get a surjection $\bigoplus_i S(-d_i) \to M$. The kernel is some graded module; now find a minimal set of homogeneous generators for this kernel, hit them all with a big free module with appropriate shifts, and so on. Call such a resolution a *minimal* resolution.

What is not at all obvious is whether this process terminates. In fact, it always terminates after n steps!

Theorem 4.21. (**Hilbert syzygy theorem.**) Every finitely generated graded module M over $k[x_1, \ldots, x_n]$ has a finite free resolution. In fact, every minimal resolution of M has at most length n.

Example 4.22. The Koszul complex. Let $\mathfrak{m} = (x_1, \ldots, x_n)$. Then there is a famous resolution for S/m of length n called the *Koszul complex*. We illustrate it for $n = 3$ explicitly below (in blue); you can write it down for general n as an exercise.

$$0 \longrightarrow S(-3) \xrightarrow{\begin{bmatrix} z \\ -y \\ x \end{bmatrix}} S(-2)^{\oplus 3} \xrightarrow{\begin{bmatrix} y & z & \\ -x & & z \\ & -x & -y \end{bmatrix}} S(-1)^{\oplus 3} \xrightarrow{\begin{bmatrix} x & y & z \end{bmatrix}} S \longrightarrow S/(x, y, z) \longrightarrow 0$$

Proof of Hilbert syzygy theorem. Let

$$\cdots \xrightarrow{\phi_2} E_2 \xrightarrow{\phi_1} E_1 \xrightarrow{\phi_0} E_0$$

be a minimal free resolution of M. In particular, it's a projective resolution, and we can use it to compute Tor functors. First, though, notice that each matrix representing ϕ_i has

entries in $\mathfrak{m} = (x_1, \dots, x_n)$: otherwise the resolution wasn't minimal.[9] Therefore, tensoring with $k = S/\mathfrak{m}$ we obtain a complex

$$\cdots \xrightarrow{0} E_2 \otimes_S k \xrightarrow{0} E_1 \otimes_S k \xrightarrow{0} E_0 \otimes_S k$$

with all maps 0. Thus $\operatorname{Tor}_i^S(M,k) \cong k^{\operatorname{rank}(E_i)}$.

On the other hand, consider the Koszul complex for $k = S/\mathfrak{m}$. Tensoring it with M yields $\operatorname{Tor}_i^S(k,M) = 0$ for $i > n$. But $\operatorname{Tor}_i^S(k,M) = \operatorname{Tor}_i^S(M,k)$. So $E_{n+1} = E_{n+2} = \cdots = 0$. □

This proof shows something interesting: all minimal free resolutions have the same sequence of ranks! After all, those ranks measure dimensions of Tor modules: we showed

$$\operatorname{rank}(E_i) = \dim_k \operatorname{Tor}_i^S(M,k)$$

for *any* free resolution $E_\bullet$ of M.

In fact, you can carry through the whole proof above remembering the $\mathbb{Z}$-grading, to arrive at the concept of the *Betti numbers* of M.

Definition 4.23. Let M be a finitely generated $\mathbb{Z}$-graded module M over $k[x_1, \dots, x_n]$. Let

$$\cdots \to \bigoplus_{j \in \mathbb{Z}_{\geq 0}} S(-j)^{\beta_{2,j}} \to \bigoplus_{j \in \mathbb{Z}_{\geq 0}} S(-j)^{\beta_{1,j}} \to \bigoplus_{j \in \mathbb{Z}_{\geq 0}} S(-j)^{\beta_{0,j}} \tag{3}$$

be any graded free resolution of M. Then the numbers $\beta_{i,j} = \beta_{i,j}(M)$ are called the *Betti numbers* of M.

The point, which we now justify, is that the $\beta_{i,j}$ are independent of choice of resolution, and depend only on M.[10]

Note first that if M, N are graded modules over the graded ring S then $M \otimes N$ has a natural grading, namely put $x \otimes y$ in degree $a + b$ if $\deg(x) = a$ and $\deg(x) = b$. Free resolutions of M, respectively N, can be chosen to be graded, and from this the modules $\operatorname{Tor}_i^S(M,N)$ inherit a grading. Then the free resolution in (3) may be tensored with k (the latter is, as an S-module, concentrated in degree 0) to obtain that

$$\beta_{i,j}(M) = \dim_k (\operatorname{Tor}_i^S(M,k))_j$$

where the subscript denotes "degree j part."

In particular, the Betti numbers are independent of choice of graded free resolution. There is a rich, active study of *Betti tables* of graded modules among present-day algebraists.

---

[9]For example, say M is minimally generated by homogeneous elements $G_1, \dots, G_t$ in degrees $d_1, \dots, d_t$. Say $e_1, \dots, e_t$ is the corresponding basis of $E_0 = \oplus_{i=1}^t S(-d_i)$, with $e_i \mapsto G_i$. Then if ϕ_0 had a column with an element of degree 0 in it, we'd have an expression of the form $\sum a_i e_i \in \ker(E_0 \to M)$ with some $a_i \in k$ a nonzero scalar. That means $\sum a_i G_i = 0 \in M$. Now by dividing by a_i, we may express some G_i as an S-linear combination of othter G_js, contradicting minimality.

[10]This discussion follows [MS05, Lemma 1.32], except that there the finer $\mathbb{N}^n$ grading on S is used; the arguments carry over.

37. Hilbert functions, Hilbert polynomials

Let $A = \bigoplus_{d\geq 0} A_d$ be a $\mathbb{Z}$-graded Noetherian ring. Then A_0, being a quotient of A, is also Noetherian, and A is finitely generated over A_0, as an A_0-algebra [AM69, (10.7)] (not proved in this class), say by homogeneous elements $x_1, \dots, x_n$ in positive degree.

We make two assumptions that are not completely necessary but simplify the discussion: we shall assume that $A_0 = k$ is a field, and that $\deg x_i = 1$ for all i. The most important example is $A = S = k[x_1, \dots, x_n]$.

Let $M = \bigoplus_{d\geq 0} M_d$ be a f.g. graded A-module. Then each $\dim_k M_d$ is finite (why?).

Definition 4.24. The *Hilbert function* of M is the collection of these numbers: it is the function

$$h_M \colon \mathbb{N} \to \mathbb{N}, \qquad h_M(d) = \dim_k M_d.$$

Example 4.25. $S = k[x_1, \dots, x_n]$ itself has Hilbert function

$$h_S(d) = \binom{d+n-1}{n-1}$$

by a "sticks and stones" elementary combinatorics argument: the number of monomials in $k[x_1, \dots, x_n]$ of degree d is equal to the number of arrangements of $n-1$ sticks and d stones. Figure out the bijection: e.g.,

$$\bullet \mid \bullet\ \bullet \mid \mid \bullet\ \bullet \qquad \text{corresponds to} \qquad x_1 x_2^2 x_4^2.$$

Just to be very sure: the binomial coefficient is defined as

$$\binom{d+n-1}{n} = \frac{1}{(n-1)!}(d+n-1)\cdot\dots\cdot(d+1)(d)$$

if $d \geq 0$, and 0 otherwise.

Example 4.26. Then by shifting, the Hilbert function of $S(-j)$ is

$$h_{S(-j)}(d) = \binom{d-j+n-1}{n-1}.$$

One way to arrange all the numbers $h_M(d)$ is to hang them up as coefficients of a power series:

Definition 4.27. The *Poincaré series* or *Hilbert series* of M is the power series

$$F_M(t) = \sum_{d\geq 0} h_M(d) t^d \in \mathbb{Z}[[t]].$$

It turns out that these power series are nice: they are actually rational functions in t, with a pole of order $\leq n$ at $t = 1$ and no other poles.

Example 4.28. The Poincaré series of S itself is $1/(1-t)^n$. Indeed,

$$\frac{1}{(1-t)^n} = (1+t+t^2+\cdots)\cdots(1+t+t^2+\cdots) = \sum_{d\geq 0}\binom{d+n-1}{n-1}t^d. \tag{4}$$

Therefore the Poincaré series of $S(-d)$ itself is $t^d/(1-t)^n$.

Therefore:

Proposition 4.29. For any finitely generated graded module M over a graded Noetherian ring A, we have

$$F_M(t) = \frac{f(t)}{(1-t)^n}$$

for some polynomial $f(t) \in \mathbb{Z}[t]$. Here n is any number such that A may be generated over A_0 by elements $x_1, \ldots, x_n$ of degree 1.

Proof. In general, this can be proven by induction on n; see [AM69, Theorem 11.1]. When $A = k[x_1, \ldots, x_n]$, it already follows from our statement of Hilbert's syzygy theorem, implying the existence of a finite free resolution of M. Indeed, use the fact that if

$$0 \to M_1 \to \cdots \to M_\ell \to 0$$

is any exact sequence of fg graded A-modules, then $\sum(-1)^i F_M(t) = 0$. □

Definition 4.30. Define $d(M)$ to be the order of the pole at $t = 1$ of F_M.

Corollary 4.31. **(Definition of Hilbert polynomial)** There is a (necessarily unique) polynomial $p_M \in \mathbb{Q}[t]$ such that $p_M(d) = h_M(d)$ for all $d >> 0$. This p_M is called the *Hilbert polynomial* of M.

Proof. This follows from (4). □

Corollary 4.32. [AM69, Corollary 11.2] The degree of the Hilbert polynomial p_M is $d(M)-1$.

Proof. Let $d = d(M)$ for short. By canceling factors of $(1-t)$ as needed, we may write the Poincaré series of M as

$$F_M(t) = \frac{g(t)}{(1-t)^d} = \frac{a_0 + \cdots + a_N t^N}{(1-t)^d},$$

where $g(1) = a_0 + \cdots + a_N \neq 0$.

Now recall yet again that

$$\frac{1}{(1-t)^d} = \sum_{j \geq 0} \binom{j+d-1}{d-1} t^j,$$

so the coefficient of t^j in this power series is a polynomial in j, of degree $d-1$ and leading coefficient $1/(d-1)!$.

Therefore, the power series $a_i t^i/(1-t)^d$ has coefficients agreeing, *after a "delay" of i terms,* with a polynomial of degree $d-1$ and leading coefficient $a_i/(d-1)!$.

Therefore $F_M(t)$ also has coefficients agreeing, after N terms, with a polynomial of degree $d-1$ and leading coefficient $\frac{a_0+\cdots+a_N}{(d-1)!}$. The point is that this number is not zero, by the assumption that $g(1) \neq 0$, so the Hilbert polynomial of M really does have degree $d-1$. □

Remark 4.33. Hilbert polynomials are important invariants of projective schemes (the schemey version of zero sets, in projective space, of homogeneous polynomials). Hilbert polynomials and flatness (of projective morphisms) are related; the precise statement is beyond the scope of the course.

Part 5. More algebra and geometry

38. Elementary projective geometry in a day

How do graded rings arise geometrically? There are at least two ways: first, as coordinate rings of projective varieties. Second, as associated graded rings of local rings.

Definition 5.1. Let $k = \overline{k}$. Let $S = k[x_0, \ldots, x_n]$.

Define $\mathbb{P}^n$ as a set and define the projective algebraic subset corresponding to a homogeneous ideal $I \subset S$.

Define $I(Z)$ as the ideal generated by homogeneous polynomials vanishing on Z.

Definition 5.2. The *irrelevant ideal* in S is $\mathfrak{m} = (x_0, \ldots, x_n)$. It is kind of a mean name, but the point is that the affine zero set of $\mathfrak{m}$ is nonempty while its projective zero set is empty.

Proposition 5.3. (Projective Strong Nullstellensatz) For any homogeneous J, excluding when $\sqrt{J} = \mathfrak{m}$, we have $I(Z(J)) = \sqrt{J}$.

Thus, there is a bijective, inclusion-reversing correspondence between radical homogeneous ideals of S *other than the irrelevant ideal* and projective algebraic subsets of $\mathbb{P}^n$.

Proof. Discuss why the projective Nullstellensatz is completely reasonable. □

Remark 5.4. Mention the Proj construction.

One way to *define* the dimension of a projective algebraic subset is via the Hilbert polynomial:

Definition 5.5. Let $S = k[x_0, \dots, x_n]$. Let I be a radical homogeneous ideal of S. The *dimension* of $Z(I)$ is $\deg p_{S/I}(t) = d(S/I) - 1$.

Recall that for M an S-module, the number $d(M)$ is defined to be the order of the pole at $t = 1$ of the Poincaré series $F_M(t)$ of M. Discuss why this definition is reasonable (first agree that no matter what, we should stipulate $\dim \mathbb{P}^n = n$.)

That said, having a local definition of dimension—eventually, the dimension of a scheme X at a point x—would be advantageous.

39. Associated graded rings and the tangent cone

Let A be any ring and I an ideal. The *associated graded ring* will live up to its name: it is a graded ring associated with the pair (A, I). First define the blowup algebra, denoted $\widetilde{A}$ or $\mathrm{Bl}_I(A)$:

Definition 5.6. The *blowup algebra* or *Rees algebra* is the graded ring

$$\mathrm{Bl}_I(A) = \bigoplus_{d \geq 0} I^d = A \oplus I \oplus I^2 \oplus \cdots .$$

Thus $\mathrm{Bl}_I(A)$ is naturally a graded A-algebra.

Make sure we agree on how multiplication works in the blowup ring. The blowup algebra is the algebraic operation behind the blowup in algebraic geometry, namely $\operatorname{Proj} \mathrm{Bl}_I(A)$. But this is beyond the scope of the course...

Definition 5.7. The *associated graded ring* is the graded ring

$$\widetilde{A}/I\widetilde{A} = G_I(A) = A/I \oplus I/I^2 \oplus I^2/I^3 \oplus \cdots$$

The associated graded ring has a nice geometric interpretation in terms of the tangent cone. Forget its grading; then it is just a ring, and you can take its Spec.

Definition 5.8. Let R be a fg k-algebra, $\mathfrak{m}$ a maximal ideal of R, and let $A = R_{\mathfrak{m}}$. The *tangent cone* of $\operatorname{Spec} A$ at $\mathfrak{m}$ is $\operatorname{Spec} G_{\mathfrak{m}}(A)$.

Example 5.9. Draw pictures, showing how the tangent cone looks. The justification for the pictures will be the following exercise, on the homework:

Exercise 5.10. Let $B = k[x_1, \ldots, x_d]/I$ and $m = (x_1, \ldots, x_d)$, and let $A = B_m$. Prove that

$$G_m(A) \cong k[x_1, \ldots, x_d]/\langle \text{in}(f) \colon f \in I \rangle.$$

Here, $\text{in}(f)$ denotes the sum of all terms of f of lowest degree.

40. Dimension theory

We will work with Noetherian rings throughout. Our goal is to state the main theorem of dimension theory of Noetherian local rings. The proof relies on [AM69, §10], so we will only sketch the proof.[11]

I will write $\dim R$ for the Krull dimension of R (make sure we remember what that is.) We may reduce to the local case:

Remark 5.11. For any ring R, we have

$$\dim R = \sup \{\dim R_p : p \text{ prime in } R\}.$$

Define the *dimension* of $\operatorname{Spec} R$ at p to be $\dim R_p$.

Remark 5.12. Talk a little bit about how to think about the local ring R_p, as the stalk of the structure sheaf $\mathcal{O}_{\operatorname{Spec} R}$ at p.

Theorem 5.13. [AM69, Theorem 11.14] **(Dimension theorem for Noetherian local rings.)** Let $(A, \mathfrak{m})$ be a Noetherian local ring. The following three numbers are equal:

(1) $\dim A$,
(2) $d(A) := d(G_{\mathfrak{m}}(A))$, and
(3) $\delta(A) :=$ the smallest number of generators for any $\mathfrak{m}$-primary ideal of A.

Remark 5.14. Which one of the three numbers would you rather compute?

Example 5.15. Draw pictures, e.g., Spec of the localization of $k[x, y, z]/(y^2 - x^2 - x^3)$ at $\mathfrak{m} = (x, y, z)$. Here the chain of primes, e.g., $(x, y, z) \supsetneq (x, y) \supsetneq (y^2 - x^2 - x^3)$ realizes the dimension.

For the third way of computing dimension, notice $\mathfrak{m} = (x, y, z)$ is minimally generated by three elements. But consider, e.g., (z, x) or (z, y). Draw the picture.

Here we will give a sketch of the proof of the Dimension Theorem. For a complete proof, we would need some theorems like the Artin-Rees Lemma from Chapter 10.

Proof. [AM69, Proposition 11.7] **Proof that** $\delta(A) \geq d(G_{\mathfrak{m}}(A))$**.** Pick q a best $\mathfrak{m}$-primary ideal (meaning, smallest possible number of generators, namely $\delta(A)$). Recall

$$G_q(A) = A/q \oplus q/q^2 \oplus \cdots$$

[11] Last year I covered [AM69, §10], but this year I covered more category theory plus derived functors and Tor instead, and I'm very happy with the tradeoff so far.

so actually $d(G_q(A)) \leq \delta(A)$, since $G_q(A)$ is generated in degree 1 by $\delta(A)$ elements hence its Poincaré series has the form polynomial$/(1-t)^\delta$. Here each q^i/q_{i+1} is not quite a vector space, since A/q need not be a field. However, A/q *is* an Artinian ring, and each q^i/q_{i+1} is a finite length A/q-module, and the Hilbert function measures lengths of graded pieces, rather than dimensions of graded pieces, in this case.

Why, then, do we have $d(G_q(A)) = d(G_\mathfrak{m}(A))$? Roughly this is because $\mathfrak{m} \supseteq q \supseteq \mathfrak{m}^r$ for some r, due to Noetherianity. That implies that the rates of growth of the lengths of $A/q, A/q^2, A/q^3, \ldots$ and $A/\mathfrak{m}, A/\mathfrak{m}^2, A/\mathfrak{m}^3, \ldots$ are the same, i.e, governed by polynomials of equal degree. Then the numbers $d(G_q(A))$ and $d(G_\mathfrak{m}(A))$ are both one less than that (and hence are equal), in the same way that if you have a polynomial $f(x)$ of degree d, then the polynomial $f(x) - f(x-1)$ has degree $d-1$. □

For the next step, we need

Proposition 5.16. [AM69, Corollary 11.9] For A a Noetherian local ring and $x \in A$ a NZD, then $d(G_\mathfrak{m}(A/(x))) \leq d(G_\mathfrak{m}(A)) - 1$.

Proof. [AM69, Proposition 11.10] **Proof that** $d(G_\mathfrak{m}(A)) \geq \dim A$**.** By induction on $d = d(A) := d(G_\mathfrak{m}(A))$. For the base case, if $d = 0$ then $\mathfrak{m}^n = \mathfrak{m}^{n+1} = \cdots$ for some n. By Nakayama, that can only happen if $\mathfrak{m}^n = 0$. Therefore A is actually local Artinian, with $\dim A = 0$.

Now for the inductive step, say $p_0 \subset \cdots \subset p_r$ is a chain of primes in A, and let $A' = A/p_0$. So A' is a domain, and the image x' of any $x \in p_1 \setminus p_0$ is a NZD. We will slice by x' and apply induction: we have $d(A'/(x')) \leq d(A') - 1$ using the previous (unproven) proposition. And, we have $d(A') \leq d(A)$ (one line of proof omitted: since A' is a quotient of A, growth in A' can't be faster than growth in A). So

$$r - 1 \leq \dim A'/(x') \leq d(A'/(x')) \leq d(A') - 1 \leq d(A) - 1$$

where the first inequality is because $p_1, \ldots, p_r$ give a chain of primes in $A'/(x')$, and the second inequality is by induction. Now $\dim A - 1$ is the "supremum of all possible $(r-1)$", so conclude $\dim A - 1 \leq d(A) - 1$. □

Definition 5.17. We need to define the *height* of a prime p: the supremum of lengths of chains

$$p_0 \subsetneq \cdots \subsetneq p_r = p.$$

Proof. [AM69, Proposition 11.13] **Proof that** $\dim A \geq \delta(A)$**.** Let $d = \dim A$. We will construct, inductively for each $i = 0, \ldots, d$, a proper ideal $(x_1, \ldots, x_i)$ such that every prime over this ideal has height $\geq i$. If we can do this, then the last ideal $(x_1, \ldots, x_d)$ wins the game for us because it is $\mathfrak{m}$-primary: indeed, its radical is $\mathfrak{m}$, since any prime above it has height d, and the only prime of height d is $\mathfrak{m}$ itself. (Recall that if your radical is a maximal ideal $\mathfrak{m}$ then you're $\mathfrak{m}$-primary.)

Inductively, we've already constructed $(x_1, \ldots, x_{i-1})$, and we want to pick x_i. Pick $x_i \in \mathfrak{m} \setminus \cup p_j$, where the union ranges over all primes p_j above $(x_1, \ldots, x_{i-1})$ of height exactly $i-1$ (if any). This is possible,[12] by [AM69, 1.11] simply because $\mathfrak{m}$, having height d itself, is not among the p_j. Then we claim $(x_1, \ldots, x_i)$ works: let q be any prime over it. Then q must have height $\geq i$: indeed, q is a prime above $(x_1, \ldots, x_{i-1})$, hence lies above some *minimal* prime above $(x_1, \ldots, x_{i-1})$. If that minimal prime is some p_j of height exactly $i-1$, then q has height $\geq i$ since it's different from p_j: after all, it contains x. If that minimal prime is of height $\geq i$, then even better, as immediately we have height $q \geq i$; we're done. □

41. Regular local rings

Let $(A, \mathfrak{m})$ be a Noetherian local ring of dimension d. By the dimension theorem, we know $\mathfrak{m}$ can't be generated by *fewer* than d elements. Notice then, by Nakayama's Lemma, that $\dim_k \mathfrak{m}/\mathfrak{m}^2 \geq d$, where we write $k = A/\mathfrak{m}$.

Definition 5.18. For $(A, \mathfrak{m})$ be a Noetherian local ring of dimension d, say A is *regular* if $\mathfrak{m}$ can be generated by d elements.

This terminology carries over to schemes: let R be a Noetherian ring. We say $p \in \operatorname{Spec} R$ is a *regular* point of $\operatorname{Spec} R$ if R_p is a regular local ring. Otherwise we say p is a *singular* point. The regular points are the "manifold-like" points; see below.

Definition 5.19. With A as above, following terminology is sometimes used: if q is an $\mathfrak{m}$-primary ideal, with $q = (x_1, \ldots, x_d)$, then $x_1, \ldots, x_d$ are called a *system of parameters*. So A is regular if $\mathfrak{m}$ itself has a system of parameters.

Proposition 5.20. [AM69, 11.20, 11.22]Let $(A, \mathfrak{m})$ be a Noetherian local ring of dimension d. TFAE:

(1) $G_{\mathfrak{m}}(A) \cong k[t_1, \ldots, t_d]$,
(2) $\dim_k \mathfrak{m}/\mathfrak{m}^2 = d$,
(3) A is regular.

Remark 5.21. The first characterization of regular local rings is useful for intuition: if $\mathfrak{m}$ is a maximal ideal of A, then $\mathfrak{m}$ is regular if $\operatorname{Spec} A$ looks like a manifold near $\mathfrak{m}$.

[12]Note that in any Noetherian ring, for example $A/(x_1, \ldots, x_{i-1})$ there are only finitely many minimal primes. You can prove it directly following Noether [Eis95, Exercise 1.2]. Or to deduce it from what we have already discussed on homework: argue that Spec of a Noetherian ring is a Noetherian topological space, and hence has finitely many irreducible components, which you have shown in [AM69, Exercise 1.20]correspond to minimal primes.

Proof. (i) implies (ii) since $\mathfrak{m}/\mathfrak{m}^2$ is exactly the degree 1 part of $G_{\mathfrak{m}}(A)$.

(ii) implies (iii) by Nakayama.

For (iii) implies (i): Let $x_1, \ldots, x_d$ be generators for $\mathfrak{m}$. Then the map of graded rings

$$k[t_1, \ldots, t_d] \to G_{\mathfrak{m}}(A)$$

sending $t_i \to \overline{x_i} = x_i + \mathfrak{m}^2$ is a surjection, by choice of x_i. We claim it is an injection. Suppose for a contradiction that $f \in k[t_1, \ldots, t_d]$ is a nonzero element in the kernel. We may as well assume that it is homogeneous, by passing to a homogeneous component. Then $k[t_1, \ldots, t_d]/(f)$ is a graded ring, with

$$d(G_{\mathfrak{m}}(A)) \leq d(k[t_1, \ldots, t_d]/(f) = d(k[t_1, \ldots, t_d]) - 1 = d - 1.$$

The first inequality because $G_{\mathfrak{m}}(A)$ is the homomorphic image of $k[t_1, \ldots, t_d]/(f)$, and the equality is by the lemma below. We have obtained a contradiction to the dimension theorem, however. □

Lemma 5.22. (We could just as easily have proved this earlier...) Let $f \in A$ be a homogeneous element which is a nonzerodivisor on a fg graded S-module M. Here S is a graded Noetherian ring, with the usual assumptions on it. Then

$$d(M/fM) = d(M) - 1.$$

Proof. Let $c = \deg(f)$. We have an exact sequence

$$0 \to M(-c) \xrightarrow{\cdot f} M \to M/fM \to 0.$$

Then $F_{M/fM} = (1 - t^c)F_M$. Note $1 - t^c$ has a simple zero at $t = 1$, so $d(M/fM) = d(M) - 1$. □

Proposition 5.23. Regular local rings are domains.

Proof. This is not at all obvious, but we omit it. See [AM69, 11.23]. □

Example 5.24. Regular local rings of dimension 0 are fields, since here $\mathfrak{m} = 0$.

Example 5.25. Regular local rings of dimension 1 are exactly *discrete valuation rings.*

This can be taken as the definition of DVR. But we'll start by defining DVRs differently, and then deducing that they are exactly regular local rings of dimension 1.

42. Discrete valuation rings

Source is [AM69, p. 94].

Definition 5.26. Let K be a field. A *discrete valuation* is a surjective homomorphism of abelian groups $v\colon K^* \to \mathbb{Z}$ such that

$$v(x+y) \geq \min v(x), v(y).$$

Often set $v(0) = +\infty$. The valuation ring is $\{x \in K \mid v(x) \geq 0\}$. Note this is a subring, by definition of v, and contains contains 1 since $v(1) = 0$.

Definition 5.27. A *discrete valuation ring* is an integral domain A that arises as the valuation ring of some valuation on $\operatorname{Frac} A$.

Example 5.28.

(1) Meromorphic functions on a neighborhood U of x; order of zero or pole at x.
(2) $K = \mathbb{Q}$, p-adic valuation. The valuation ring is $\mathbb{Z}_{(p)}$.
(3) Similarly, $K = k(x)$, $f \in k[x]$ irreducible.

Let v be a discrete valuation on K, with A its valuation ring. Let us make some preliminary observations. First, for nonzero $x \in K$, have $v(x^{-1}) = -v(x)$. So if $x \in A$, then x is a unit iff $v(x) = 0$. The ideal $\mathfrak{m} = \{x \in A \mid v(x) > 0\}$ is therefore the unique maximal ideal of A. Note $\mathfrak{m}^n = \{v(x) \geq n\}$. Furthermore there are no other nonzero ideals: given $x, y \in A$, we have $v(x) = v(y)$ iff $x = yu$ for some unit u. So for any nonzero ideal I, if $x \in I$ is a nonzero element of smallest valuation c, then I contains all elements of valuation $\geq c$ and no others, so $I = \mathfrak{m}^c$.

Here's the main theorem on DVRs. Basically, in the case of a Noetherian local domain of dimension 1, the properties of normality, regularity, and being a DVR all coincide. We'll follow [AM69] closely.

Proposition 5.29. [AM69, 9.2] Let $(A, \mathfrak{m})$ Noetherian local domain of dimension 1. Write $k = A/\mathfrak{m}$. TFAE:

(1) A DVR
(2) A normal
(3) $\mathfrak{m}$ principal
(4) $\dim_k \mathfrak{m}/\mathfrak{m}^2 = 1$
(5) every nonzero ideal is a power of $\mathfrak{m}$
(6) there exists $x \in A$ such that every nonzero ideal is of the form (x^k).

Let $(A, \mathfrak{m})$ Noetherian local domain of dimension 1. Before the proof of the above theorem, some facts.

Fact A. Any nonzero proper ideal I is $\mathfrak{m}$ primary, with $a \supset \mathfrak{m}^n$ for some n. Indeed, $\sqrt{I} = \mathfrak{m}$ (what else could it be? there aren't a lot of prime ideals lying around), and Noetherianness then implies that $\mathfrak{m} \supset I \supset \mathfrak{m}^n$ for some n.

Fact B. Have $\mathfrak{m} \supsetneq \mathfrak{m}^2 \supseteq \cdots$, for otherwise A would have dimension 0, as we learned in the chapter on Artinian rings.

Proof. **(1) implies (2)**. Let $x \in K = \operatorname{Frac} A$ with

$$x^n + a_1 x^{n-1} + \cdots + a_n = 0, \qquad a_i \in A.$$

Then $v(x) \geq 0$, otherwise $v(x^n) < \min v(a_1 x^{n-1}), \ldots, v(a_n)$, contradiction.

(2) implies (3). The most substantial step. Pick any nonzero $a \in \mathfrak{m}$, and let $n > 0$ minimum such that $(a) \supseteq \mathfrak{m}^n$; that's possible by Fact A. By minimality of choice of n, there exists some $b \in \mathfrak{m}^{n-1} \setminus (a)$. Let $x = a/b \in \operatorname{Frac} A$. We **claim** $(x) = \mathfrak{m}$.

To prove the claim, notice $x^{-1} = b/a \notin A$ since $b \notin (a)$. Since A is normal, x^{-1} is not integral over A. Now, consider $x^{-1}\mathfrak{m} = \{(b/a) \cdot y \colon y \in \mathfrak{m}\}$. This is actually a subset of A, since $by \in \mathfrak{m}^{n-1} \cdot \mathfrak{m} = \mathfrak{m}^n \subseteq (a)$. Then in fact $x^{-1}\mathfrak{m}$ is an ideal of A. Which ideal is it? If $x^{-1} \subseteq \mathfrak{m}$ then $\mathfrak{m}$ would be a faithful $A[x^{-1}]$-module, finitely generated as an A-module; then Cayley-Hamilton would imply that x^{-1} is integral over A. Contradiction! Therefore $x^{-1}\mathfrak{m} = A$ is the whole ring. Then $\mathfrak{m} = Ax = (x)$, as desired.

(3) implies (4), we already know this, e.g., from the dimension theorem. Or: any generator for $\mathfrak{m}$ has homomorphic image generating $\mathfrak{m}/\mathfrak{m}^2$, and we don't have $\mathfrak{m}/\mathfrak{m}^2 = 0$ because A would be Artinian.

(4) implies (5): Note Nakayama implies $\mathfrak{m} = (x)$ is principal. Let $I \neq A$ be a nonzero ideal. By Fact A, consider the smallest $n > 0$ with $I \supseteq \mathfrak{m}^n = (x^n)$; we claim $I \subseteq \mathfrak{m}^n$ too, so that $I = \mathfrak{m}^n$. Suppose for a contradiction there is some $z \in I \setminus \mathfrak{m}^n$, and write $z = ax^r$ for r biggest possible; in particular $r < n$. Then $a \notin (x)$ so a is a unit, so then $I \supseteq (z) = (x^r)$, contradicting minimality of n.

(5) implies (6): Here we are assuming that every nonzero ideal is of the form $\mathfrak{m}^n$, and want to show that there exists $x \in A$ such that every nonzero ideal is of the form (x^n). Therefore it suffices to prove $\mathfrak{m} = (x)$ for some x. Indeed, take $x \in \mathfrak{m} \setminus \mathfrak{m}^2$, which is possible since $\mathfrak{m}/\mathfrak{m}^2 \neq 0$ by Fact B, say. Then the ideal (x) is *some* power of $\mathfrak{m}$, but it's not $\mathfrak{m}^2$ or any higher power, so it must be that $(x) = \mathfrak{m}$.

(6) implies (1). We have $\mathfrak{m}$ is one of the ideals in the chain $(x) \supseteq (x^2) \supseteq \cdots$ so it must be the biggest one: $\mathfrak{m} = (x)$. So $(x), (x^2), \ldots$ are all distinct by Fact B. Given $a \in A \setminus \{0\}$ we have $(a) = (x^r)$ for some unique r; set $v(a) = r$, and extend v to $\operatorname{Frac} A$ by setting $v(a/b) = v(a) - v(b)$. Then check v satsfies $v(ab) = v(a) + v(b)$, and $v(a+b) \geq \min v(a), v(b)$, so v is a valuation on K.

Moreover, check that A really is the valuation ring with respect to v: suppose $v(a/b) \geq 0$ for nonzero $a, b \in A$. Then $v(a) \geq v(b)$, so $(a) = (x^{v(a)}) \subseteq (x^{v(b)}) = (b)$. So $a \in (b)$ and $a/b \in A$ after all. $\square$

References

[AM69] M. F. Atiyah and I. G. Macdonald, *Introduction to commutative algebra*, Addison-Wesley Publishing Co., Reading, Mass.-London-Don Mills, Ont., 1969. MR 0242802

[EH00] David Eisenbud and Joe Harris, *The geometry of schemes*, Graduate Texts in Mathematics, vol. 197, Springer-Verlag, New York, 2000. MR 1730819

[Eis95] David Eisenbud, *Commutative algebra*, Graduate Texts in Mathematics, vol. 150, Springer-Verlag, New York, 1995, With a view toward algebraic geometry. MR 1322960

[Liu02] Qing Liu, *Algebraic geometry and arithmetic curves*, Oxford Graduate Texts in Mathematics, vol. 6, Oxford University Press, Oxford, 2002, Translated from the French by Reinie Erné, Oxford Science Publications. MR 1917232

[MS05] Ezra Miller and Bernd Sturmfels, *Combinatorial commutative algebra*, Graduate Texts in Mathematics, vol. 227, Springer-Verlag, New York, 2005. MR 2110098

[Wei94] Charles A. Weibel, *An introduction to homological algebra*, Cambridge Studies in Advanced Mathematics, vol. 38, Cambridge University Press, Cambridge, 1994. MR 1269324

Department of Mathematics, Brown University, Box 1917, Providence, RI 02912
E-mail address: melody_chan@brown.edu