250B: Commutative Algebra

For the Morbidly Curious

Nir Elber

Spring 2022

CONTENTS

Theme 1
Working in Chains

But this is like trying to scale a glacier. It's hard to get your footing, and your fingertips get all red and frozen and torn up.

—Anne Lamott

1.1 March 15

Today's notes were transcribed from Mile's notes of the class. We are finishing up completions today.

1.1.1 Lifting Idempotents

We recall the following definitions.

Definition 1.1 (Idempotent)**.** Fix R a ring. An element $e \in R$ is *idempotent* if and only if $e^2 = e$.

Remark 1.2. Equivalently, $e \in R$ is idempotent if and only if e is a root of the polynomial $f(x) = x^2 - x$.

Example 1.3. If $e \in E$ is an idempotent, then $1 - e$ is also an idempotent: we can directly compute

$$(1-e)^2 = 1 - e - e + e^2 = 1 - e - e + e = 1 - e.$$

Lemma 1.4. Fix e an idempotent of a ring R. Then $R \cong Re \times R(1-e)$.

Proof. This was on the homework. ■

We want to lift idempotents, but we will want to keep track of a little more data.

Definition 1.5 (Orthogonal idempotents)**.** Fix R a ring. Then a set $E \subseteq R$ of idempotents of R is *orthogonal* if and only if $ee' = 0$ for any two distinct $e, e' \in E$.

Example 1.6. Fix $e \in R$ an idempotent. Then the elements $\{e, 1-e\}$ are orthogonal. In particular, these are orthogonal because

$$e(1-e) = e - e^2 = e - e = 0.$$

Here are some reasons to care about orthogonal idempotents.

Lemma 1.7. Fix R a ring and $E \subseteq R$ a finite set of idempotents. Then

$$\sum_{e \in E} e$$

is another idempotents.

Proof. This is a direct computation. For concreteness, enumerate $E = \{e_1, \ldots, e_n\}$. Then we can compute

$$\left(\sum_{k=1}^n e_k\right)\left(\sum_{\ell=1}^n e_\ell\right) = \sum_{k,\ell=1}^n e_k e_\ell = \sum_{k=1}^n e_k e_k + \sum_{\substack{k,\ell=1 \\ k \neq \ell}}^n e_k e_\ell.$$

In particular, we note that $e_k^2 = e_k$ for each k because E is only made of idempotents. Further, $e_k e_\ell = 0$ for any $k \neq \ell$ because E is made of orthogonal idempotents. It follows that

$$\left(\sum_{k=1}^n e_k\right)^2 = \sum_{k=1}^n e_k,$$

which is what we wanted. ■

With that definition out of the way, here is our main statement.

Proposition 1.8. Fix a Noetherian, local ring R complete with respect to its maximal ideal $\mathfrak{m}$. Further, take A to be a finite R-algebra (not necessarily commutative!), and pick up a finite set of orthogonal idempotents

$$\overline{E} \subseteq A/\mathfrak{m}A.$$

Then each idempotent $\overline{e} \in \overline{E}$ can be lifted to an idempotent $e \in E$ such that the set of lifts remains an orthogonal

Proof. We divide the proof into two cases. We start with the case where A is a commutative ring. Our starting step is to reduce to the case where $R = A$. Indeed, note that A is complete with respect to the ideal $\mathfrak{m}A$ because

$$\widehat{A}_{\mathfrak{m}A} \cong \widehat{R}_{\mathfrak{m}} \otimes_R A = R \otimes_R A = A,$$

where we are using the tensor-product characterization of the completion; notably, $\widehat{R}_{\mathfrak{m}} = R$ because R is complete with respect to $\mathfrak{m}$. Because A is now complete with respect to an ideal $\mathfrak{m}A$, we might as well ignore R. In particular, A is local with maximal ideal $\mathfrak{m}A$ and Noetherian as a finite algebra over a Noetherian ring.

Now, suppose that we have an idempotent $\overline{e} \in A/\mathfrak{m}A$, and let $e_0 \in A$ be any representative. Set $f(x) := x^2 - x$, and we will use Hensel lifting. In particular,

$$f(e_0) = e_0^2 - e_0 \equiv \overline{e}^2 - \overline{e} \equiv 0 \pmod{\mathfrak{m}},$$

and

$$(f'(e_0))^2 = (2e_0 - 1)^2 = 4\left(e_0^2 - e_0\right) + 1 \equiv 1 \pmod{\mathfrak{m}},$$

so we may use Hensel's lemma to lift $\overline{e}$ to an element $e \in A$ such that $e \equiv e_0 \equiv \overline{e} \pmod{\mathfrak{m}}$ and $f(e) = e^2 - e = 0$.

It remains to preserve orthogonality. For concreteness, enumerate $\overline{E}$ by $\{\overline{e_1},\ldots,\overline{e_n}\}\subseteq A/\mathfrak{m}A$, which we lift to $\{e_1,\ldots,e_n\}\subseteq A$. Now, for $k\ne\ell$, we need to show that $e_ke_\ell=0$. Well,

$$e_ke_\ell\equiv\overline{e_k}\cdot\overline{e_\ell}\equiv 0\pmod{\mathfrak{m}}$$

because the $\overline{e_\bullet}$ are orthogonal. However, we can do better than this because we have idempotents: for any $d\in\mathbb{N}$, we see that

$$e_ke_\ell=e_k^de_\ell^d=(e_ke_\ell)^d\in\mathfrak{m}^d.$$

Notably, this is the point where we are crucially using the fact that A is commutative: we need $e_k^de_\ell^d=(e_ke_\ell)d$. Anyways, it follows that

$$e_ke_\ell\in\bigcap_{\mathfrak{m}}\mathfrak{m}^d.$$

By the Krull intersection theorem (recall A is a Noetherian local ring), we conclude that $e_ke_\ell=0$.

We now add on the case where A is not commutative, by reducing to the commutative case. We proceed by induction on $\#E$. For example, if $\#\overline{E}=1$, then we can still lift our idempotent from A upwards as discussed above, and the ring $R[e]$ is commutative, so we can directly reduce to the commutative case.

More generally, suppose that we have orthogonal idempotents $\{\overline{e_1},\ldots,\overline{e_n}\}\subseteq A/\mathfrak{m}A$. By the inductive hypothesis, we can lift the first $n-1$ of these to orthogonal idempotents

$$\{e_1,\ldots,e_{n-1}\}\subseteq A.$$

Now, we add in the last idempotent by hand: set

$$f:=1-\sum_{i=1}^{n-1}e_i$$

so that $\{e_1,\ldots,e_{n-1},f\}$ is a set of orthogonal idempotents. With this "auxiliary" idempotent, we finish by taking any representative $e_n'\in A$ of $\overline{e_n}$ and then lift fe_nf in the commutative case $R[e_1,\ldots,e_{n-1},fe_n'f]$. This lifted idempotent e_n will work. ■

Being able to lift idempotents gives us the following ring decomposition, akin to Lemma 1.4.

Lemma 1.9. Fix R a Noetherian local ring complete with respect to its maximal ideal $\mathfrak{m}$. Further, given a finite (commutative) R-algebra A, we have that A has only finitely many maximal ideals $\{\mathfrak{m}_1,\ldots,\mathfrak{m}_n\}$, and

$$A\cong\prod_{k=1}^nA_{\mathfrak{n}_k}$$

Notably, $A_{\mathfrak{m}_k}$ is a localization.

Proof. The point is to use the Artinian decomposition from our discussion of modules of finite length and then lift by appealing to idempotents. Namely, $A/\mathfrak{m}A$ is a finite-dimensional $R/\mathfrak{m}$-vector space, so $A/\mathfrak{m}A$ is an Artinian ring. In particular, we can write

$$A/\mathfrak{m}A\cong\prod_{i=1}^n\overline{A_i},$$

where we are writing A_i as our product of the various localizations of $A/\mathfrak{m}A$. Because we have expressed $A/\mathfrak{m}A$ as a product of rings, we can identify the inclusion maps

$$\overline{A_i}\hookrightarrow A/\mathfrak{m}A$$

as taking 1 to some idempotent of $A/\mathfrak{m}A$, which we will call $\overline{e_i}$. For psychological reasons, we will identify $\overline{A_i}$ with its image (via the above inclusion map) in $A/\mathfrak{m}A$ so that $\overline{A_i}=(A/\mathfrak{m}A)\overline{e_i}$.

We now lift. Our idempotents $\{\overline{e_1}, \ldots, \overline{e_n}\}$ are orthogonal, so we can use our lifting to give us a set of orthogonal idempotents

$$\{e_1, \ldots, e_n\} \subseteq A$$

such that $e_1 \equiv \overline{e_1} \pmod{\mathfrak{m}}$. Then these orthogonal idempotents give rise to the ring decomposition

$$A = \prod_{i=1}^{n} A_i,$$

where $A_i = Ae$.

To finish, we need to show that A_i is a localization of A with respect to a maximal ideal. To be explicit, we claim that A_i is local with maximal ideal $\mathfrak{n}_i := A_i \cap \mathfrak{m}A$. For this, we note

$$\frac{R}{\mathfrak{n}_i \cap R} \subseteq \frac{A_i}{\mathfrak{n}_i A_i}$$

is an integral extension (in particular, finite), where $R/(\mathfrak{n}_i \cap R)$ is a field (as an extension of $R/\mathfrak{m}$). From here, we can realize A_i as a localization by setting

$$\mathfrak{m}_i = \prod_{j=1}^{i-1} A_i \times \mathfrak{n}_i \times \prod_{j=i+1}^{n} A_i.$$

Thus, we have forced A to be a product of the localizations of A, from which we conclude that we have found all of our maximal ideals. ■

1.1.2 The Cohen Structure Theorem

We end our discussion of completions with a few works on the Cohen structure theorem. Here is the statement.

Theorem 1.10 (Cohen structure)**.** Fix a Noetherian local ring R complete with respect to its maximal ideal $\mathfrak{m}$. Further, let $\kappa := R/\mathfrak{m}$ be the residue field; if R contains a field, then

$$R \cong \kappa[[x_1, \ldots, x_n]]/I$$

for some ideal $I \subseteq \kappa[[x_1, \ldots, x_n]]$.

Note that the condition that R contains its residue field k is necessary.

Non-Example 1.11. Take $R = \mathbb{Z}_p$ to be the ring of p-adic integers, which has residue field $k = R/\mathfrak{m} = \mathbb{Z}_p/p\mathbb{Z}_p \cong \mathbb{F}_p$. However, $\mathbb{F}_p$ does not contain $\mathbb{F}_p$ because R has characteristic 0.

We'll show Theorem 1.10 in the case where κ is perfect.

Proof of Theorem 1.10 when κ is perfect. Note that, if R contains any field K which surjects onto κ, then we can give $\mathfrak{m}$ generators $\{f_1, \ldots, f_n\}$ over R and then surjecting

$$\pi : K[[x_1, \ldots, x_n]] \twoheadrightarrow R$$

by lifting $K \twoheadrightarrow R/\mathfrak{m}$ and then sending $x_\bullet \mapsto f_\bullet$. From here, we can mod out by the kernel to get an isomorphism of the form

$$R \cong \frac{K[[x_1, \ldots, x_n]]}{\ker \pi},$$

which gives the desired map.

So it suffices to show that, if R contains any field, then R contains a field isomorphic to κ. Well, by modding out by $\mathfrak{m}$, we can at least be sure that the field which R contains can be embedded into κ, so we can build the extension

$$K \subseteq K(\{t_i : i \in I\}) \subseteq \kappa,$$

where $K \subseteq K(\{t_i : i \in I\})$ is a purely transcendental extension and $K(t_i : i \in I) \subseteq \kappa$ is a purely algebraic extension.

Now, the transcendental elements $t_i \in \kappa = R/\mathfrak{m}$ can be lifted arbitrarily to R, which induces an embedding $F \hookrightarrow R$, where F is some very large field. As such, we let K' be the maximal subfield of R which contains F. We would like to show that K' surjects onto κ when taken modulo $\mathfrak{m}$, which will finish by choosing our lifts carefully.

Well, let $\alpha \in \kappa \setminus K'$ be an element of κ such that $\kappa = K'(\alpha)$. However, we can lift the root α up to the root of some polynomial in R, which produces a strictly larger field than K'. This is a contradiction, so we must instead have $K' \twoheadrightarrow R/\mathfrak{m}$. This finishes. ■

Remark 1.12. We used separability at the end of the proof during our use of the Primitive element theorem.

THEME 2
INTRODUCTION TO DIMENSION

In this sense the algebraic geometers have never left paradise: There is no snake (that is, Peano curve) in the garden.

—David Eisenbud

2.1 March 15

We continue today's lecture by transitioning over to dimension theory.

2.1.1 Krull Dimension

Let's talk about some properties that we want out of our dimension. Here's a starting example.

Definition 2.1 (Dimension, vector spaces)**.** The dimension of a (finite-dimensional) vector space V is the length of a maximal chain of distinct subspaces

$$0 = V_0 \subsetneq V_1 \subsetneq \cdots \subsetneq V_n = V.$$

Remark 2.2. To see that these align, suppose that V is finite-dimensional so that the definition makes sense. Then we can give V a basis by choosing a vector from each $V_k \setminus V_{k-1}$. We will not check formally that this works.

What's impressive about this definition is that we have even managed to remove the data of the ground field of our vector space!

In analogy with this, we have the following algebraic definition of dimension.

Definition 2.3 (Krull dimension)**.** Fix a ring R. Then we define the *(Krull) dimension* of R, notated $\dim R$, to be the length of a longest possible chain

$$\mathfrak{p}_0 \subsetneq \mathfrak{p}_1 \subsetneq \cdots \mathfrak{p}_n \subsetneq R,$$

where the $\mathfrak{p}_\bullet$ are prime ideals.

Here are some examples to get used to this definition.

Example 2.4. Fields have dimension 0.

Example 2.5. In general, if a Noetherian ring R has $\dim R = 0$, then all primes are maximal, so we know from our discussion of modules of finite length that R is Artinian. In fact, we know R is Artinian if and only if all primes are maximal and R is Noetherian.

Example 2.6. If R is a principal ideal domain which is not a field, then we showed in our proof that principal ideal domains are unique factorization domains that all nonzero prime ideals are maximal. Thus, the largest possible chain in R takes the form

$$(0) \subsetneq \mathfrak{p} \subsetneq R,$$

so R has dimension 1.

Example 2.7. The ring $k[x]$ is a principal ideal domain and not a field and therefore has dimension 1. More generally,

$$\dim k[x_1, \ldots, x_n] = n,$$

but we will not prove this yet.

2.1.2 Motivating Dimension

One way to be convinced that Definition 2.3 is the right definition of dimension is to write down some axioms that we want out of our dimension and try to use these to characterize dimension. Here are some axioms that Eisenbud provides.

- We want dimension to be a property determined locally; for example, the dimension of the union of a plane and a line should be 2 because of the plane. Because localization and completions are intended to be ways to look very locally at a point (geometrically speaking), we ask for

$$\dim R = \sup_{\mathfrak{p} \in \operatorname{Spec} R} \dim R_{\mathfrak{p}} \qquad \text{and} \qquad \dim R_{\mathfrak{p}} = \dim \widehat{R}_{\mathfrak{p}}.$$

- We don't want to have to deal with nilpotent elements. In some sense, nilpotent elements correspond to differentials, but they shouldn't affect the dimension of our space. As such, if $I \subseteq R$ is a nilpotent ideal, we will require that

$$\dim(R/I) = \dim R.$$

- Small changes in our base ring should not affect the dimension either. For example, the rings k and $k[x]/\left(x^2+1\right)$ should have the same dimension (they are, roughly speaking, just lines), even though the latter ring is certainly bigger in some sense. To codify this, if S is a finite R-algebra containing R, we will require that

$$\dim S = \dim R.$$

- We want the dimension of the coordinate ring of affine n-space to be n; additionally, the dimension should be uniform across all of n-space. So after taking completion at $(x_1, \ldots, x_n)$, this amounts to requiring

$$\dim k[[x_1, \ldots, x_n]] = n.$$

It turns out that these properties completely characterize the dimension.

2.1.3 Other Characterizations

Here are some other characterizations of the dimension.

Theorem 2.8. Fix $R := k[x_1, \ldots, x_n]/\mathfrak{p}$ (i.e., R is a finitely generated k-algebra), where $\mathfrak{p} \subseteq k[x_1, \ldots, x_n]$ is a prime so that R is a domain. Then $\dim R$ is equal to the transcendence degree of $K(R)$ over k. In fact, in this case, $\dim R$ is the length of all maximal chains of distinct primes.

Note that the previous theorem is somewhat agnostic about the case where R is not an integral domain: for example, the ring

$$k[x] \times k[y, z],$$

which can be thought of the ring of functions of the (disjoint) union of a line and a plane. Indeed, in this disjoint union, we wouldn't even expect all maximal chains to have the same length because taking the union along the line should prevent us from being able to see the plane.

We can use the above result in a stronger sense to justify our axioms above.

Theorem 2.9 (Noether Normalization)**.** Fix $R := k[x_1, \ldots, x_n]/\mathfrak{p}$ (i.e., R is a finitely generated k-algebra), where $\mathfrak{p} \subseteq k[x_1, \ldots, x_n]$ is a prime so that R is a domain. Further, fix

$$\mathfrak{p}_0 \subsetneq \mathfrak{p}_1 \subsetneq \cdots \subsetneq \mathfrak{p}_n$$

a maximal chain of primes. Then there exists a subring $S \subseteq R$ such that $S \cong k[x_1, \ldots, x_n]$ and $\mathfrak{p}_k \cap S = (x_1, \ldots, x_k)$.

In particular, finitely generated k-algebras have their dimension intimately connected with some finite subring, akin to our third axiom.

We close with a more computational way to look at the dimension. Recall that if R is a local Noetherian ring with maximal ideal $\mathfrak{m}$, then we can define its Hilbert function by

$$H_R(n) := \dim_{R/\mathfrak{m}} \mathfrak{m}^n/\mathfrak{m}^{n+1},$$

which we know to be equal to a polynomial P_R for sufficiently large values of n. Then the following is true.

Theorem 2.10. Fix R a local Noetherian ring. Then $\dim R = 1 + \deg P_R$.

We can be convinced of this by running the example $R = k[[x_1, \ldots, x_n]]$.

LIST OF DEFINITIONS