COURSE NOTES: COMMUTATIVE ALGEBRA

AMNON YEKUTIELI

Contents

These are notes for the lectures starting from 3 Jan 2018. Notes for the previous lectures are handwritten, and are available online at [Yek].

comment: Start of Lecture 11, 3 Jan 2018.

1. Noether Normalization

Recall that all rings are commutative, unless explicitly stated otherwise.

The letters t and s will usually refer to variables. Given a nonzero ring A, and a finite sequence of distinct variables $\boldsymbol{t} := (t_1, \ldots, t_n)$, we use the notation

$$A[\boldsymbol{t}] := A[t_1, \ldots, t_n]$$

for the polynomial ring over A in these variables.

Definition 1.1. Let $A \to B$ be a ring homomorphism, and let $\boldsymbol{b} = (b_1, \ldots, b_n)$ be a sequence of elements of B. We say that this sequence is *algebraically independent over A* if the A-ring homomorphism

$$f_{\boldsymbol{b}} : A[\boldsymbol{t}] \to B, \quad t_i \mapsto b_i,$$

from the polynomial ring in the sequence of variables $\boldsymbol{t} = (t_1, \ldots, t_n)$, is injective.

A ring homomorphism $f_{\boldsymbol{b}} : A[\boldsymbol{t}] \to B$ as above can be understood as *substitution* or *evaluation*. A polynomial $p(\boldsymbol{t}) \in A[\boldsymbol{t}]$ is sent by the ring homomorphism $f_{\boldsymbol{b}}$ to the element

$$p(\boldsymbol{b}) = p(b_1, \ldots, b_n) := f_{\boldsymbol{b}}(p(\boldsymbol{t})) \in B.$$

In an explicit formula it looks like this: if

$$p(\boldsymbol{t}) = \sum_{i_1, \ldots, i_n \in \mathbb{N}} a_{i_1, \ldots, i_n} \cdot t_1^{i_1} \cdots t_n^{i_n} \in A[\boldsymbol{t}],$$

with coefficients $a_{i_1,\dots,i_n} \in A$, all but finitely many of them zero, then

$$p(\boldsymbol{b}) = \sum_{i_1,\dots,i_n \in \mathbb{N}} a_{i_1,\dots,i_n} \cdot b_1^{i_1} \cdots b_n^{i_n} \in B.$$

Using the substitution notation, the sequence $\boldsymbol{b}$ in B is algebraically independent over A iff it does not satisfy a nontrivial polynomial equation over A, namely for every nonzero $p(\boldsymbol{t}) \in A[\boldsymbol{t}]$ the substitution $p(\boldsymbol{b}) \in B$ is nonzero.

The substitution notation can also be used to denote the image of the A-ring homomorphism $f_{\boldsymbol{b}} : A[\boldsymbol{t}] \to B$, which is also the A-subring of B generated by the sequence $\boldsymbol{b}$; the notation for this subring is $A[\boldsymbol{b}]$.

Definition 1.2. Let $f : A \to B$ be a ring homomorphism. We call f a *finite homomorphism*, and we say that *B is a finite A-ring*, if f makes B into a finitely generated A-module.

This should not be confused with a *finitely generated A-ring*.

Example 1.3. The polynomial ring $B := A[t]$, in a single variable t over a nonzero ring A, is a finitely generated A-ring, but it is not a finite A-ring, since as an A-module B is free of infinite rank.

Proposition 1.4. *Let $f : A \to B$ and $g : B \to C$ be finite ring homomorphisms. Then $g \circ f : A \to C$ is a finite ring homomorphism.*

Exercise 1.5. Prove the proposition above.

Let A be a nonzero ring. Consider a nonzero polynomial

$$p(t) = \sum_{i=0}^{m} a_i \cdot t^i \in A[t]$$

of degree $m \geq 1$ in a single variable t (this means that $a_m \neq 0$). Recall that $p(t)$ is called *monic* if its leading coefficient is $a_m = 1$. Thus

$$p(t) = t^m + \sum_{i=0}^{m-1} a_i \cdot t^i. \tag{1.6}$$

Definition 1.7. Let $f : A \to B$ be a ring homomorphism.

(1) An element $b \in B$ is said to be *integral over A* if there is a monic polynomial $p(t) \in A[t]$ such that $p(b) = 0$.
(2) B is called an *integral A-ring* if all elements $b \in B$ are integral over A.

Theorem 1.8. *Let $f : A \to B$ be a ring homomorphism. The following two conditions are equivalent:*

(i) *B is a finite A-ring.*
(ii) *B is a finitely generated integral A-ring.*

We won't prove this theorem, nor will we use it (except for the special easy case in the lemma below). The proof of the theorem relies on the "determinant trick", an enhanced version of the Cayley-Hamilton Theorem; see [AlKl, Section 10].

Lemma 1.9. *Let $f : A \to B$ be a ring homomorphism, and assume $B = A[b]$ for some element $b \in B$ that is integral over A. Then f is a finite ring homomorphism.*

Proof. Suppose $p(b) = 0$ for the monic polynomial $p(t)$ of degree $m \geq 1$ from equation (1.6). Then

$$b^m = \sum_{i=0}^{m-1} (-a_i) \cdot b^i,$$

so B is generated as an A-module by $1, b, \ldots, b^{m-1}$. □

Let A be a nonzero ring, and let $B := A[\boldsymbol{t}] = A[t_1, \ldots, t_n]$ be the polynomial ring in n variables. The canonical ring homomorphism $A \to B$ is injective, and we identify A with its image in B. The elements of A are called *constant polynomials*. In case $n = 1$, and writing $t := t_1$, a constant polynomial $b(t)$ is either the zero polynomial, or it has degree 0.

Here is a crucial lemma, due to M. Nagata (1962; see [Nag, Section 14] or [Lang, Section VIII.2]). It is a modification of the original proof by E. Noether (1926, [Noet]).

Lemma 1.10. *Let $\Bbbk$ be a field, let $B := \Bbbk[\boldsymbol{t}] = \Bbbk[t_1, \ldots, t_n]$ be the polynomial ring in $n \geq 1$ variables, and let $b_1 = b_1(\boldsymbol{t}) \in B$ be a nonconstant polynomial. Then there exist elements $b_2, \ldots, b_n \in B$ such that B is finite over the subring $\Bbbk[b_1, \ldots, b_n]$.*

The lemma asserts that the ring homomorphism

$$\Bbbk[\boldsymbol{s}] = \Bbbk[s_1, \ldots, s_n] \to B = \Bbbk[\boldsymbol{t}], \quad s_i \mapsto b_i,$$

where $\boldsymbol{s}$ is another sequence of variables, is finite.

Proof. Let us write the polynomial $b_1(\boldsymbol{t})$ explicitly:

$$b_1(\boldsymbol{t}) = \sum_{\boldsymbol{i} \in \mathbb{N}^n} \lambda_{\boldsymbol{i}} \cdot \boldsymbol{t}^{\boldsymbol{i}} \tag{1.11}$$

where $\boldsymbol{i} = (i_1, \ldots, i_n) \in \mathbb{N}^n$ is a multi-index, $\lambda_{\boldsymbol{i}} \in \Bbbk$ and $\boldsymbol{t}^{\boldsymbol{i}} := t_1^{i_1} \cdots t_n^{i_n} \in B$. Define I to be the support of b_1, when it is viewed as a function $b_1 : \mathbb{N}^n \to \Bbbk$; namely

$$I := \{\boldsymbol{i} \in \mathbb{N}^n \mid \lambda_{\boldsymbol{i}} \neq 0\}.$$

This is a finite set of course; and it is nonempty because $b_1(\boldsymbol{t})$ is a nonzero polynomial. Moreover, I contains some multi-index $\boldsymbol{i} \neq (0, \ldots, 0)$, because $b_1(\boldsymbol{t})$ is a nonconstant polynomial.

Choose a natural number e large enough so that

$$e > \sup \{i_1, \ldots, i_n\}$$

for every multi-index $\boldsymbol{i} \in I$. In particular, $e > 1$. Consider the function

$$\epsilon : I \to \mathbb{N}, \quad \epsilon(\boldsymbol{i}) := i_1 + i_2 \cdot e + \cdots + i_n \cdot e^{n-1}.$$

Thus $\boldsymbol{i}$ is the base e expansion of the natural number $\epsilon(\boldsymbol{i})$. It follows that the function ϵ is injective. Define $\boldsymbol{i}_{\max} \in I$ to be the multi-index for which the function ϵ attains its maximum, and let $\epsilon_{\max} := \epsilon(\boldsymbol{i}_{\max}) \in \mathbb{N}$ and $\lambda_{\max} := \lambda(\boldsymbol{i}_{\max}) \in \Bbbk$. Note that $\lambda_{\max} \neq 0$, $\epsilon_{\max} > 0$ and $\boldsymbol{i}_{\max} \neq (0, \ldots, 0)$.

For $i = 2, \ldots, n$ define

$$b_i(\boldsymbol{t}) := t_i - t_1^{e^{i-1}} \in \Bbbk[\boldsymbol{t}] = B. \tag{1.12}$$

Thus

$$t_i = b_i + t_1^{e^{i-1}} \quad \text{for all } i \geq 2. \tag{1.13}$$

For every multi-index $\boldsymbol{i} \in I$ we have

$$\boldsymbol{t}^{\boldsymbol{i}} = t_1^{i_1} \cdot t_2^{i_2} \cdot \cdots \cdot t_n^{i_n} = t_1^{i_1} \cdot \big(b_2 + t_1^{e}\big)^{i_2} \cdot \cdots \cdot \big(b_n + t_1^{e^{n-1}}\big)^{i_n}$$

in $\Bbbk[\boldsymbol{t}] = B$. Expanding this expression by powers of t_1 we obtain

$$\begin{aligned} \boldsymbol{t}^{\boldsymbol{i}} &= t_1^{i_1 + i_2 \cdot e + \cdots + i_n \cdot e^{n-1}} + (\text{lower degree terms in } t_1) \\ &= t_1^{\epsilon(\boldsymbol{i})} + \sum_{j=0}^{\epsilon(\boldsymbol{i}-1)} c_{\boldsymbol{i},j}(b_2, \ldots, b_n) \cdot t_1^j \end{aligned} \tag{1.14}$$

where

$$c_{\boldsymbol{i},j}(s_2, \ldots, s_n) \in \Bbbk[s_2, \ldots, s_n]$$

are polynomials in a new sequence of variables $\boldsymbol{s} = (s_1, s_2, \ldots, s_n)$, and in (1.14) we substitute $s_i \mapsto b_i$ for $i \geq 2$. Therefore, by combining (1.11) and (1.14), we get

$$b_1(\boldsymbol{t}) = \sum_{\boldsymbol{i} \in I} \lambda_{\boldsymbol{i}} \cdot \boldsymbol{t}^{\boldsymbol{i}} = \lambda_{\max} \cdot t_1^{\epsilon_{\max}} + \sum_{j=0}^{\epsilon_{\max}-1} c_j(b_2, \ldots, b_n) \cdot t_1^j \tag{1.15}$$

in $\Bbbk[\boldsymbol{t}] = B$, where

$$c_j(s_2, \ldots, s_n) := \sum_{\boldsymbol{i} \in I} \lambda_{\boldsymbol{i}} \cdot c_{\boldsymbol{i},j}(s_2, \ldots, s_n) \in \Bbbk[s_2, \ldots, s_n]. \tag{1.16}$$

Define the ring

$$A := \Bbbk[b_1, \ldots, b_n] \subseteq \Bbbk[\boldsymbol{t}] = B \tag{1.17}$$

and the polynomial

$$q(s_1) := s_1^{\epsilon_{\max}} + \Big(\textstyle\sum_{j=0}^{\epsilon_{\max}-1} \lambda_{\max}^{-1} \cdot c_j(b_2, \ldots, b_n) \cdot s_1^j\Big) - \lambda_{\max}^{-1} \cdot b_1 \in A[s_1]. \tag{1.18}$$

Notice that $q(s_1)$ is a monic polynomial in the variable s_1, of degree $\epsilon_{\max}$, with coefficients in the ring A. By formulas (1.14), (1.15) and (1.16) the substitution $s_1 \mapsto t_1$ gives $q(t_1) = 0$ in B. Therefore the element $t_1 \in B$ is integral over the ring A. By Lemma 1.9 the subring $A[t_1] \subseteq B$ is finitely generated as an A-module.

Finally, by formulas (1.17) and (1.13), we have

$$A[t_1] = \Bbbk[b_1, \ldots, b_n, t_1] = \Bbbk[t_1, \ldots, t_n] = B.$$

So B is finite over the subring A. □

comment: Start of Lecture 12, 10 Jan 2018.

Theorem 1.19 (Noether Normalization)**.** *Let* $\mathbb{k}$ *be a field, and let* A *be a nonzero finitely generated* $\mathbb{k}$*-ring. Then there exists a sequence* $\boldsymbol{a} = (a_1, \ldots, a_n)$ *of elements of* A *with these properties:*

- ▹ *The sequence* $\boldsymbol{a}$ *is algebraically independent over* $\mathbb{k}$*.*
- ▹ A *is finite over the subring* $\mathbb{k}[\boldsymbol{a}]$*.*

Proof. Because A is a finitely generated $\mathbb{k}$-ring, there exist finite $\mathbb{k}$-ring homomorphisms

$$f : \mathbb{k}[\boldsymbol{t}] = \mathbb{k}[t_1, \ldots, t_n] \to A$$

from polynomial rings in n variables, for various $n \in \mathbb{N}$; some of these homomorphisms are even surjections. Let us choose such a finite homomorphism f with minimal number of variables n. We will prove that this f is injective. Then the sequence $\boldsymbol{a} = (a_1, \ldots, a_n)$, with $a_i := f(t_i) \in A$, will have the required properties.

Let us write $B := \mathbb{k}[\boldsymbol{t}] = \mathbb{k}[t_1, \ldots, t_n]$, and $\mathfrak{b} := \operatorname{Ker}(f) \subseteq B$. We need to prove that the ideal $\mathfrak{b} = 0$. The proof is by contraposition: we shall assume that $\mathfrak{b} \neq 0$, and arrive at a contradiction.

Take a nonzero element $b_1 \in \mathfrak{b}$. The polynomial b_1 is nonconstant, because otherwise $b_1 \in \mathbb{k}^{\times}$, and then $\mathfrak{b} = B$ and $A = 0$, which is false.

According to Lemma 1.10 there are elements $b_2, \ldots, b_n \in B$, such that the ring homomorphism

$$g : \mathbb{k}[\boldsymbol{s}] = \mathbb{k}[s_1, \ldots, s_n] \to B = \mathbb{k}[\boldsymbol{t}], \quad s_i \mapsto b_i,$$

is finite. Here $\boldsymbol{s} = (s_1, \ldots, s_n)$ is a new sequence of variables. Consider the $\mathbb{k}$-ring homomorphism

$$f \circ g : \mathbb{k}[\boldsymbol{s}] \to A.$$

It is a finite ring homomorphism, and $(f \circ g)(s_1) = f(b_1) = 0$. Define

$$a_i := (f \circ g)(s_i) = f(b_i) \in A;$$

so $a_1 = 0$.

Let

$$h : \mathbb{k}[s_2, \ldots, s_n] \to A$$

be the the restriction of $f \circ g$ to this subring of $\mathbb{k}[\boldsymbol{s}]$, which is a polynomial ring over $\mathbb{k}$ in $n - 1$ variables. The image of h in A is

$$\operatorname{Im}(h) = \mathbb{k}[a_2, \ldots, a_n] = \mathbb{k}[a_1, a_2, \ldots, a_n] = \operatorname{Im}(f \circ g).$$

Because $f \circ g$ is a finite ring homomorphism, so is h. But this contradicts the minimality of n. □

2. Transcendence Degree

In this section we recall without proofs some facts on field extensions.

Exercise 2.1. Read about transcendence degree. Some sources are: [Art], [Lang] or [Jac].

A ring homomorphism $f : K \to L$ between fields is called a *field extension*. Of course f is an injection. Let's fix such a field extension.

An element $b \in L$ is called *algebraic over* K if it satisfies some nonzero polynomial equation over K; namely there is a nonzero polynomial $p(t) \in K[t]$ such that $p(b) = 0$. If b is not algebraic over K then it is called *transcendental over* K. Being transcendental is the same as being algebraically independent (Definition 1.1 with $n = 1$, $A = K$ and $B = L$). It is easy to see that b is algebraic over K iff it is integral over K.

We say that L is an *algebraic extension* of K if every $b \in L$ is algebraic over K. This is equivalent to the condition that

$$L = \bigcup_{i \in I} L_i,$$

where I is an indexing set (possibly infinite), and each L_i is a finite field extension of K.

Definition 2.2. A *transcendence basis* of L over K is a collection $\{b_i\}_{i \in I}$ of elements of L such that:

- The collection $\{b_i\}_{i \in I}$ is algebraically independent over K; i.e. for every finite sequence of distinct indices $(i_1, \ldots, i_n)$ in I, the sequence $(b_{i_1}, \ldots, b_{i_n})$ in L is algebraically independent in the sense of Definition 1.1.
- L is an algebraic extension of the subfield $K(\{b_i\}_{i \in I})$ generated by this collection of elements and K.

Theorem 2.3. *Let $K \to L$ be a field extension.*

1. *There exists a transcendence basis $\{b_i\}_{i \in I}$ of L over K.*
2. *If $\{c_j\}_{j \in J}$ is another transcendence basis of L over K, then the cardinalities satisfy $|J| = |I|$.*

Definition 2.4. The *transcendence degree* of L over K is the cardinality $|I|$ of some transcendence basis $\{b_i\}_{i \in I}$ of L over K. It is denoted by $\operatorname{tr.deg}_K(L)$.

3. Dimension Theory

Some of the proofs in this section are, apparently, new. Certainly they are shorter and claner than what can be found in the textbooks I have seen.

We begin by recalling some definitions from earlier in the course (see page 83.1).

Definition 3.1. Let A be a ring.

1. A *chain of prime ideals* in A is a sequence $\boldsymbol{\mathfrak{p}} = (\mathfrak{p}_0, \ldots, \mathfrak{p}_n)$ of prime ideals $\mathfrak{p}_i$ in A such that $\mathfrak{p}_i \subsetneqq \mathfrak{p}_{i+1}$. The *length* of this chain is n.
2. The (Krull) *dimension* of the ring A is the supremum of the lengths of chains of primes ideals in A, and we denote it by $\dim(A)$.

Note that $\dim(A) \in \mathbb{N} \cup \{\infty\}$.

Lemma 3.2. *Let K be a field, let M be a finiely generated K-module, and let $\phi \in \operatorname{End}_K(M)$. The following three conditions are equivalent.*

(i) *ϕ is injective.*

(ii) *ϕ is surjective.*
(iii) *ϕ is bijective.*

Exercise 3.3. Prove Lemma 3.2. (Hint: translate it to the language of linear algebra.)

Lemma 3.4. *Let K be a field, let A be an integral domain, and let $K \to A$ be a finite ring homomorphism. Then A is a field.*

Exercise 3.5. Prove Lemma 3.4. (Hint: use Lemma 3.2.)

Lemma 3.6 (Going Down)**.** *Let $f : A \to B$ be a finite ring homomorphism, let $\mathfrak{q}_0 \subsetneqq \mathfrak{q}_1$ be prime ideals in B, and let $\mathfrak{p}_i := f^{-1}(\mathfrak{q}_i) \subseteq A$. Then $\mathfrak{p}_0 \subsetneqq \mathfrak{p}_1$.*

Proof. Define $\bar{A} := A/\mathfrak{p}_0$, $\bar{B} := B/\mathfrak{q}_0$, $\bar{\mathfrak{p}} := \mathfrak{p}_0/\mathfrak{p}_0 = (0) \subseteq \bar{A}$ and $\bar{\mathfrak{q}} := \mathfrak{q}_1/\mathfrak{q}_0 = (0) \subseteq \bar{B}$. We get a finite injective ring homomorphism $\bar{f} : \bar{A} \to \bar{B}$ between integral domains, and we have to show that $\bar{f}^{-1}(\bar{\mathfrak{q}}) \neq \bar{\mathfrak{p}}$.

Thus, dropping the bars everywhere, an replacing A with its image $f(A) \subseteq B$, we now have an integral domain B, a subring A over which B is finite, a nonzero prime ideal $\mathfrak{q} \subseteq B$, and $\mathfrak{p} = (0) \subseteq A$. We have to show that $A \cap \mathfrak{q} \neq \mathfrak{p}$.

Let's assume that $A \cap \mathfrak{q} = \mathfrak{p}$, and show that this leads to a contradiction. Consider the local ring $B_{\mathfrak{q}}$, with its maximal ideal $\mathfrak{q}_{\mathfrak{q}}$. In the commutative diagram

$$\begin{CD}
\mathfrak{q} @>{\phi}>> B \\
@V{\psi}VV @VV{g}V \\
\mathfrak{q}_{\mathfrak{q}} @>{\phi_{\mathfrak{q}}}>> B_{\mathfrak{q}}
\end{CD}$$

the homomorphism $\phi : \mathfrak{q} \to B$ is the inclusion, $g : B \to B_{\mathfrak{q}}$ and $\psi : \mathfrak{q} \to \mathfrak{q}_{\mathfrak{q}}$ are is the canonical homomorphisms of localization, and $\phi_{\mathfrak{q}} : \mathfrak{q}_{\mathfrak{q}} \to B_{\mathfrak{q}}$ is the homomorphism induced from ϕ by applying $B_{\mathfrak{q}} \otimes_B (-)$ to ϕ. The homomorphism g is injective, because B is an integral domain. The homomorphism $\phi_{\mathfrak{q}}$ is injective because ϕ is injective and by by the flatness of localization. It follows that the homomorphism ψ is injective, and thus the maximal ideal $\mathfrak{q}_{\mathfrak{q}}$ is nonzero.

On the other hand, letting $K := \operatorname{Frac}(A) = A_{\mathfrak{p}}$, the assumption that $A \cap \mathfrak{q} = \mathfrak{p}$ implies that the inclusion $f : A \to B$ extends to a ring homomorphism $f_{\mathfrak{q}} : K \to B_{\mathfrak{q}}$. The homomorphism $f_{\mathfrak{q}}$ fits into this commutative diagram of injective ring homomorphisms:

$$\begin{array}{ccccccc}
 & & B & & & \xrightarrow{\text{loc}} & \\
 & & \downarrow{\scriptstyle \text{loc}} & & & & \\
K & \xrightarrow{f_{\mathfrak{p}}} & K \otimes_A B & \xrightarrow{\text{loc}} & B_{\mathfrak{q}} & \xrightarrow{\text{loc}} & \operatorname{Frac}(B)
\end{array}
\qquad f_{\mathfrak{q}} : K \to B_{\mathfrak{q}}$$

The homomorphisms marked "loc" are localizations. Because the ring homomorphism $f : A \to B$ is finite, the induced ring homomorphism $f_{\mathfrak{p}} : K \to K \otimes_A B$ is also finite. But $K \otimes_A B$ is an integral domain, so according to Lemma 3.4 the ring $K \otimes_A B$ is a field. We deduce that the localization homomorphisms

$$K \otimes_A B \to B_{\mathfrak{q}} \to \operatorname{Frac}(B)$$

are all bijective. Therefore $B_{\mathfrak{q}}$ is a field, and its maximal ideal $\mathfrak{q}_{\mathfrak{q}}$ is zero. We have a contradiction. □

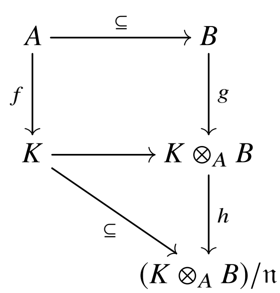
Lemma 3.7 (Going Up)**.** *Let $A \subseteq B$ be integral domains such that B is finite over A, and let $\mathfrak{p} \subseteq A$ be a prime ideal. Then there is a prime ideal $\mathfrak{q} \subseteq B$ such that $A \cap \mathfrak{q} = \mathfrak{p}$.*

Proof. We have an induced finite injective ring homomorphism $A_{\mathfrak{p}} \to A_{\mathfrak{p}} \otimes_A B$; so $A_{\mathfrak{p}} \otimes_A B$ is a nonzero finitely generated $A_{\mathfrak{p}}$-module. Let $K := A_{\mathfrak{p}} / \mathfrak{p}_{\mathfrak{p}}$. By the Nakayama Lemma the ring

$$K \otimes_A B \cong K \otimes_{A_{\mathfrak{p}}} (A_{\mathfrak{p}} \otimes_A B)$$

is nonzero. So there is some maximal ideal $\mathfrak{n} \subseteq K \otimes_A B$. (We will see later, in ???, that here we don't need Zorn's lemma to find a maximal ideal in $K \otimes_A B$, and that there are only finitely many of them.) Let $g : B \to K \otimes_A B$ be the canonical ring homomorphism, and define $\mathfrak{q} := g^{-1}(\mathfrak{n}) \subseteq B$, which is a prime ideal.

There is a commutative diagram of rings



in which h is the canonical surjection. Because the homomorphisms marked "⊆" are injective, and $\operatorname{Ker}(h) = \mathfrak{n}$, we get

$$\mathfrak{p} = \operatorname{Ker}(f) = A \cap \operatorname{Ker}(h \circ g) = A \cap \mathfrak{q}.$$

□

Remark 3.8. Actually there are only finitely many primes $\mathfrak{q}$ satisfying the conditions of the lemma.

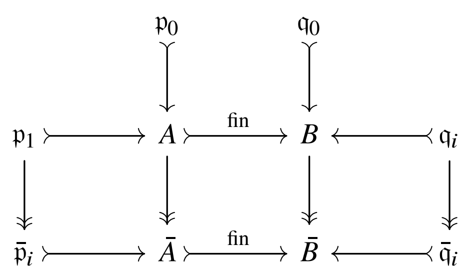
comment: Start of Lecture 13, 17 Jan 2018.

Lemma 3.9. *Let $A \subseteq B$ be integral domains such that B is finite over A, and let $(\mathfrak{p}_0, \ldots, \mathfrak{p}_n)$ be chain of prime ideals in A. Then there is a chain of prime ideals $(\mathfrak{q}_0, \ldots, \mathfrak{q}_n)$ in B such that $\mathfrak{p}_i = A \cap \mathfrak{q}_i$.*

Proof. The proof is by induction on $n \geq 0$. According to Lemma 3.7 there is a prime ideal $\mathfrak{q}_0 \subseteq B$ such that $A \cap \mathfrak{q}_0 = \mathfrak{p}_0$. This takes care of the case $n = 0$.

Now assume that $n \geq 1$, and the result is known for chains of length $n - 1$. Let $\mathfrak{q}_0$ be as above, and define $\bar{A} := A/\mathfrak{p}_0$ and $\bar{B} := B/\mathfrak{q}_0$. So there is a finite injective ring homomorphism $\bar{A} \to \bar{B}$, and in $\bar{A}$ we have a chain of prime ideals $(\bar{\mathfrak{p}}_1, \ldots, \bar{\mathfrak{p}}_n)$, where $\bar{\mathfrak{p}}_i := \mathfrak{p}_i/\mathfrak{p}_0$. By the induction hypothesis there is a chain of prime ideals $(\bar{\mathfrak{q}}_1, \ldots, \bar{\mathfrak{q}}_n)$ in $\bar{B}$ such that $\bar{A} \cap \bar{\mathfrak{q}}_i = \bar{\mathfrak{p}}_i$. Define $\mathfrak{q}_i \subseteq B$ to be the preimage of $\bar{\mathfrak{q}}_i$ under the canonical surjection $B \to \bar{B}$. Then $\mathfrak{q}_i \subsetneq \mathfrak{q}_{i+1}$, and $\mathfrak{p}_i = A \cap \mathfrak{q}_i$. □

The proof of the lemma is illustrated in the diagram below.



The next theorem due to Krull [Kru].

Theorem 3.10. *Let $f : A \to B$ be a finite ring homomorphism.*

(1) *The dimensions satisfy*

$$\dim(B) \leq \dim(A).$$

(2) *If f is injective and B is an integral domain, then*

$$\dim(B) = \dim(A).$$

Proof. (1) Given a chain of prime ideals $(\mathfrak{q}_0, \ldots, \mathfrak{q}_n)$ in B, let $\mathfrak{p}_i := f^{-1}(\mathfrak{q}_i)$. By Lemma 3.6 the sequence $(\mathfrak{p}_0, \ldots, \mathfrak{p}_n)$ is a chain of prime ideals in A. Hence $\dim(B) \leq \dim(A)$.

(2) We may assume that $A \subseteq B$ and f is the inclusion. Note that A is also an integral domain. Given a chain of prime ideals $(\mathfrak{p}_0, \ldots, \mathfrak{p}_n)$ in A, Lemma 3.9 says that there is a chain of prime ideals $(\mathfrak{q}_0, \ldots, \mathfrak{q}_n)$ in B. This implies that $\dim(A) \leq \dim(B)$. □

Notice that so far in this section we did not assume our rings are noetherain.

Theorem 3.11. *Let $\mathbb{k}$ be a field, and let $A := \mathbb{k}[t_1, \ldots, t_n]$, the polynomial ring in n variables. Then* $\dim(A) = n$.

Proof. For every $i = 0, \ldots, n$ the ideal $\mathfrak{p}_i := (t_1, \ldots, t_i) \subseteq A$ is prime, and thus we get a chain of prime ideals $(\mathfrak{p}_0, \ldots, \mathfrak{p}_n)$ in A. This proves that $\dim(A) \geq n$.

For the reverse inequality, we shall prove that if $(\mathfrak{p}_0, \ldots, \mathfrak{p}_m)$ is a chain of prime ideals in A, then $m \leq n$. The proof is by induction on $n \geq 0$. The case $n = 0$ is trivial.

Now take some integer $n \geq 1$. Suppose that there is a chain of prime ideals $(\mathfrak{p}_0, \ldots, \mathfrak{p}_m)$ in $A = \mathbb{k}[t_1, \ldots, t_n]$ of length $m > n$; we will derive a contradiction from this. Choose an element $a_1 \in \mathfrak{p}_1 - \mathfrak{p}_0$. Since $a_1 = a_1(\boldsymbol{t})$ is a nonconstant polynomial, by Lemma 1.10 there are elements $a_2, \dots, a_n$ in A such that A is finite over the subring $\Bbbk[a_1, \dots, a_n]$. Let $s_1, \dots, s_n$ be new variables, and define $B := \Bbbk[s_1, \dots, s_n]$. The ring homomorphism

$$f : B \to A, \quad f(s_i) := a_i,$$

is finite.

Let $\mathfrak{q}_1 := (s_1) \subseteq B$, and define $\bar{B} := B/\mathfrak{q}_1$. Also define $\bar{A} := A/\mathfrak{p}_1$. Since $f(\mathfrak{q}_1) \subseteq \mathfrak{p}_1$, there is an induced finite ring homomorphism $\bar{f} : \bar{B} \to \bar{A}$. Define $\bar{\mathfrak{p}}_i := \mathfrak{p}_i/\mathfrak{p}_1 \subseteq \bar{A}$ for $i \geq 1$. Then $(\bar{\mathfrak{p}}_1, \dots, \bar{\mathfrak{p}}_m)$ is a chain of prime ideals in $\bar{A}$. Let $\bar{\mathfrak{q}}_i := \bar{f}^{-1}(\bar{\mathfrak{p}}_i) \subseteq \bar{B}$. Lemma 3.6 says that $(\bar{\mathfrak{q}}_1, \dots, \bar{\mathfrak{q}}_m)$ is a chain of prime ideals in $\bar{B}$. Its length is $m - 1$. However there is a $\Bbbk$-ring isomorphism $\bar{B} \cong \Bbbk[s_2, \dots, s_n]$, so $\bar{B}$ is a polynomial ring in $n - 1$ variables. By the induction hypothesis we must have $m - 1 \leq n - 1$, i.e. $m \leq n$. This is a contradiction. □

Corollary 3.12. *Let $\Bbbk$ be a field, and let A be a finitely generated $\Bbbk$-ring. Then* $\dim(A) < \infty$.

Proof. There exists a surjective $\Bbbk$-ring homomorphism $B \to A$, where $B := \Bbbk[t_1, \dots, t_n]$ is the polynomial ring in n variables, for some n. By Theorems 3.10(1) and 3.11 we get

$$\dim(A) \leq \dim(B) = n.$$

□

Corollary 3.13 (Dimension Theorem)**.** *Let $\Bbbk$ be a field, and let A be an integral domain that is finitely generated as a $\Bbbk$-ring, with field of fractions K. Then*

$$\dim(A) = \mathrm{tr.deg}_{\Bbbk}(K).$$

Proof. By Noether Normalization (Theorem 1.19) there is a finite injective $\Bbbk$-ring homomorphism $f : B \to A$, where $B := \Bbbk[\boldsymbol{t}] = \Bbbk[t_1, \dots, t_n]$ is the polynomial ring in n variables for some $n \in \mathbb{N}$. We may assume that $B \subseteq A$ and f is the inclusion. Theorems 3.11 and 3.10(2) tell us that $\dim(A) = \dim(B) = n$.

The field of fractions of B is the field of rational functions $L := \Bbbk(\boldsymbol{t})$, and it has $\mathrm{tr.deg}_{\Bbbk}(L) = n$. By Lemma 3.4 there is an isomorphism $L \otimes_B A \cong K$, so $L \to K$ is a finite field extension, and hence $\mathrm{tr.deg}_{\Bbbk}(L) = \mathrm{tr.deg}_{\Bbbk}(K)$. □

Theorem 3.14 (Hilbert Nullstellensatz)**.** *Let $\Bbbk$ be a field, let A be a finitely generated $\Bbbk$-ring, and let $\mathfrak{m}$ be a maximal ideal. Then $A/\mathfrak{m}$ is a finite field extension of $\Bbbk$.*

Proof. The field $K := A/\mathfrak{m}$ is a finitely generated $\Bbbk$-ring, say $K = \Bbbk[a_1, \dots, a_m]$, and it has $\dim(K) = 0$. By Corollary 3.13 we know that $\mathrm{tr.deg}_{\Bbbk}(K) = 0$. Thus K is an algebraic extension of $\Bbbk$. It implies that the elements a_i are all algebraic over $\Bbbk$, and hence $\Bbbk \to K$ is finite. □

Corollary 3.15. *Let $\Bbbk$ be an algebraically closed field, let A be a finitely generated $\Bbbk$-ring, and let $\mathfrak{m}$ be a maximal ideal. Then $\Bbbk \to A/\mathfrak{m}$ is an isomorphism.*

Proof. This is immediate from the theorem. □

Corollary 3.16. *Let $\Bbbk$ be an algebraically closed field, let $A := \Bbbk[t_1, \ldots, t_n]$ be a polynomial ring in n variables, and let $\mathfrak{m}$ be a maximal ideal in A. Then there is a unique sequence of elements $(\lambda_1, \ldots, \lambda_n)$ in $\Bbbk$ such that*

$$\mathfrak{m} = (t_1 - \lambda_1, \ldots, t_n - \lambda_n).$$

Proof. The previous corollary says that the canonical ring homomorphism $\Bbbk \to A/\mathfrak{m}$ is bijective. Let $\lambda_i \in \Bbbk$ be the element that goes to $t_i + \mathfrak{m} \in A/\mathfrak{m}$ under this ring isomorphism. Define the ideal

$$\mathfrak{m}' = (t_1 - \lambda_1, \ldots, t_n - \lambda_n) \subseteq A.$$

Then $\mathfrak{m}' \subseteq \mathfrak{m}$, and $\mathfrak{m}'$ is maximal; so they are equal. □

We end with another variant of the NSZ, that was not done in class.

Let $\Bbbk$ be an algebraically closed field. For $n \geq 1$ we write $\mathbf{A}^n(\Bbbk) := \Bbbk^n$, viewed as a set. It is the *n-dimensional affine space over* $\Bbbk$. The polynomial ring $A = \Bbbk[\boldsymbol{t}] = \Bbbk[t_1, \ldots, t_n]$ is viewed as a ring of functions $\mathbf{A}^n(\Bbbk) \to \Bbbk$, by evaluation. To be explicit, for a point $x = (\lambda_1, \ldots, \lambda_n) \in \mathbf{A}^n(\Bbbk)$ and a polynomial $f(\boldsymbol{t}) \in A$ we have

$$f(x) := f(\lambda_1, \ldots, \lambda_n) \in \Bbbk.$$

Given an ideal $\mathfrak{a} \subseteq A$ we denote by $\mathrm{Z}(\mathfrak{a}) \subseteq \mathbf{A}^n(\Bbbk)$ the *zero locus* of $\mathfrak{a}$, namely

$$\mathrm{Z}(\mathfrak{a}) := \{x \in \mathbf{A}^n(\Bbbk) \mid f(x) = 0 \text{ for all } f \in \mathfrak{a}\}. \tag{3.17}$$

Thus

$$\mathrm{Z}(\mathfrak{a}) = \bigcap_{f \in \mathfrak{a}} \mathrm{Z}(f).$$

Corollary 3.16 can be interpreted as follows: there is a canonical bijection from the set of maximal ideals of A to the set $\mathbf{A}^n(\Bbbk)$. The formula is

$$\mathfrak{m} \mapsto x = (\lambda_1, \ldots, \lambda_n) \in \mathbf{A}^n(\Bbbk), \quad \text{where } \mathrm{Z}(\mathfrak{m}) = \{x\}.$$

Corollary 3.18. *Let $\Bbbk$ be an algebraically closed field, let $A := \Bbbk[t_1, \ldots, t_n]$ be a polynomial ring in n variables, let $\mathfrak{a}$ be an ideal in A, and let $f \in A$. If $\mathrm{Z}(f) \subseteq \mathrm{Z}(\mathfrak{a})$ then $f^j \in \mathfrak{a}$ for some $j > 0$.*

Proof. The proof is by contraposition. Let $\bar{A} := A/\mathfrak{a}$. Assume that $f^j \notin \mathfrak{a}$ for all $j > 0$. Then the element $\bar{f} := f + \mathfrak{a} \in \bar{A}$ is not nilpotent. Therefore the localized ring $\bar{A}_{\bar{f}}$ is nonzero, and it has some maximal ideal $\bar{\mathfrak{m}}$. Let $\mathfrak{m} \subseteq A$ be the preimage of $\bar{\mathfrak{m}}$ under the ring homomorphism $A \to \bar{A}_{\bar{f}}$. So $\mathfrak{m}$ is a prime ideal of A, $\mathfrak{a} \subseteq \mathfrak{m}$, and $\mathfrak{m} \cap \{f^j\}_{j>0} = \varnothing$. Also $\mathfrak{m}_f \subseteq A_f$ is a maximal ideal. Because A_f is a finitely generated $\Bbbk$-ring, Corollary 3.15 says that

$$\Bbbk \to A_f/\mathfrak{m}_f \cong (A/\mathfrak{m})_f$$

is bijective. But $A/\mathfrak{m}$ is a $\Bbbk$-subring of $(A/\mathfrak{m})_f$, so actually $\Bbbk \to A/\mathfrak{m}$ is bijective. We see that $\mathfrak{m}$ is a maximal ideal of A.

By Corollary 3.16 we know that $\mathfrak{m} = x$ for some point $x \in \mathbf{A}^n(\Bbbk)$. The inclusion $\mathfrak{a} \subseteq \mathfrak{m}$ implies $x \in \mathrm{Z}(\mathfrak{a})$. The fact that $f \notin \mathfrak{m}$ means that $f(x) \neq 0$. Hence $x \in \mathrm{Z}(\mathfrak{a}) - \mathrm{Z}(f)$, so $\mathrm{Z}(f) \not\subseteq \mathrm{Z}(\mathfrak{a})$. □

References

[AlKl] A. Altman and S. Kleiman, "A Term of Commutative Algebra", online at http://web.mit.edu/18.705/www.

[Art] M. Artin, "Algebra", Prentice-Hall.

[Eis] D. Eisenbud, "Commutative Algebra", Springer, 1994.

[Har] R. Hartshorne, "Algebraic Geometry", Springer-Verlag, New-York, 1977.

[Jac] N. Jacobson, "Basic Algebra I-II", Freeman.

[Kru] W. Krull, Zum Dimensionsbegriff der Idealtheorie, *Math. Zeit.* **42** (1937), 745-766.

[Lang] S. Lang, "Algebra", Addison-Wesley.

[Mac2] S. Maclane, "Categories for the Working Mathematician", Springer, 1978.

[Mats] H. Matsumura, "Commutative Ring Theory", Cambride University Press, 1986.

[Nag] M. Nagata, "Local Rings", Wiley, 1962.

[Noet] E. Noether, Der Endlichkeitsatz der Invarianten endlicher linearer Gruppen der Charakteristik p, *Nachrichten von der Gesellschaft der Wissenschaften zu Göttingen* (1926), 28-35.

[Row] L.R. Rowen, "Ring Theory" (Student Edition), Academic Press, 1991.

[SP] "The Stacks Project", an online reference, J.A. de Jong (Editor), http://stacks.math.columbia.edu.

[Yek] A. Yekutieli, Course Notes, http://www.math.bgu.ac.il/~amyekut/teaching/2017-18/comm-alg/course_page.html .

Department of Mathematics Ben Gurion University, Be'er Sheva 84105, Israel.
Email: amyekut@math.bgu.ac.il, *Web*: http://www.math.bgu.ac.il/~amyekut.