Notes for: Noether's normalization lemma & Hilbert's nullstellensatz

[→ compare w/ exercises 16, 17 in ch. 5.]

- We will prove Noether normalization and then deduce a (weak form) of Hilbert's nullstellensatz (or "zero locus theorem"), a result important in algebraic geometry that relates algebraic sets in alg. geometry to ideals in polynomial rings (over an alg. closed field).

- We start with the following lemma that will be key in the proof of Noether normalization:

<u>Lemma</u>: Let k be a field and let $f \in k[x_1, \dots, x_n]$. Let $N =$ highest degree of a variable appearing in f.

Let $\varphi : k[x_1, \dots, x_n] \to k[x_1, \dots, x_n]$ be k-homomorphism defined by $x_i \mapsto x_i + x_n^{N^i}$ for $i = 1, \dots, n-1$ and $x_n \mapsto x_n$.
[This is an iso. by alg. ind. of x_i over k, hence is a change of variables.]

Then $\varphi(f) \in (k[x_1, \dots, x_{n-1}])[x_n]$ is a nonzero scalar times a monic polynomial in x_n (i.e. other coefficients in $k[x_1, \dots, x_{n-1}]$).

<u>Example to give idea of the lemma</u>:

Consider $f = x_1 x_2 \in k[x_1, x_2]$. This is <u>not</u> monic in x_1 or x_2.
Let φ be the automorphism: $\begin{cases} x_1 \mapsto x_1 + x_2 \\ x_2 \mapsto x_2 \end{cases}$ (here $N = 1$).
Then $\varphi(f) = (x_1 + x_2) x_2 = x_2^2 + x_1 x_2$, which, as a polynomial in x_2 over $k[x_1]$, <u>is</u> monic.

Pf of Lemma:

- Each nonzero term of f will have the form

$$c_\alpha X_1^{a_1} X_2^{a_2} \cdots X_n^{a_n},$$

where $\alpha = (a_1, \dots, a_n)$ and $c_\alpha \in k \setminus \{0\}$.

The image of this term under the change of variables φ is:

$$\varphi(c_\alpha X_1^{a_1} \cdots X_n^{a_n}) = c_\alpha (X_1 + X_n^N)^{a_1} (X_2 + X_n^{N^2})^{a_2} \cdots (X_{n-1} + X_n^{N^{n-1}})^{a_{n-1}} X_n^{a_n}.$$

This contains a unique highest degree term:

$$c_\alpha (X_n^N)^{a_1} (X_n^{N^2})^{a_2} \cdots (X_n^{N^{n-1}})^{a_{n-1}} X_n^{a_n}$$

$$= c_\alpha X_n^{a_n + a_1 N + a_2 N^2 + \cdots + a_{n-1} N^{n-1}}$$

- As $\alpha = (a_1, \dots, a_n)$ ranges over all possible values corresponding to the terms in f, these exponents of the variable X_n are all $a_n + a_1 N + a_2 N^2 + \cdots + a_{n-1} N^{n-1}$ distinct by uniqueness of representation of integers in base N.

Thus no two exponents of X_n are the same, so we have no cancellation.

Set $m = \max \{ a_n + a_1 N + a_2 N^2 + \cdots + a_{n-1} N^{n-1} \}_{\alpha = (a_1, \dots, a_n) \text{ occuring as exponent in nonzero term of } f}$.

Say m corresponds to exponent α_0.

Hence m = degree of $\varphi(f)$, and $c_{\alpha_0} X_n^m$ is only term in $\varphi(f)$ of degree m, and $c_{\alpha_0} \in k \setminus \{0\}$, that is $c_{\alpha_0}^{-1} \varphi(f)$ is a monic polynomial in X_n over $k[X_1, \dots, X_{n-1}]$. ∎

A reminder on definitions:

a) If $k \hookrightarrow A$ is a ring homomorphism, then

- A is a <u>finitely generated k-module</u> if there is a finite set $x_1, \dots, x_n \in A$ s.t. every element of A can be written as $\sum_{i=1}^{n} c_i x_i$ for $c_i \in k$ (i.e., $\exists$ surjection $k^n \twoheadrightarrow A$)
- A is a <u>finitely generated k-algebra</u> if there is a finite set $x_1, \dots, x_n \in A$ s.t. every element of A can be written as a <u>polynomial</u> in x_i with coefficients in k (i.e., $\exists$ surjection $k[t_1, \dots, t_n] \twoheadrightarrow A$.)

(For more, see page 30 of A-M.)

b) Elements $y_1, \dots, y_n \in A$ are <u>algebraically independent</u> over a field k if they do <u>not</u> satisfy a nontrivial polynomial equation with coefficients in k, that is, the homomorphism $k[x_1, \dots, x_n] \to A$, $x_i \mapsto y_i$ is an injection.

Noether's normalization lemma

Let k be a field, and let $A \neq 0$ be a finitely generated k-algebra. Then there exist algebraically independent (over k) elements $y_1, \dots, y_r \in A$ such that A is integral over $k[y_1, \dots, y_r]$. (i.e., $k[y_1, \dots, y_r] \subseteq A$ is an integral extension.)

That is, if k is a field, every finitely generated k-algebra A is isomorphic to a f.g. extension over $k[y_1, \dots, y_r]$.

That is, $k[y_1, \dots, y_r] \hookrightarrow A$ is finitely generated as a <u>module</u>. (see Remark page 60).

Proof of Noether normalization

- Induct on the number n of generators for A as a k-algebra. If $n=0$, then $A=k$ and we can take $r=0$ (hence $A=k$ is clearly integral over itself.)

- Suppose $n \geq 1$ and suppose the result holds for k-algebras generated by $n-1$ or fewer elements.

Suppose $A = k[\alpha_1, \dots, \alpha_n]$, $\alpha_i \in A$, has n-generators (there might be relations between these elmts α_i!)

If $\alpha_1, \dots, \alpha_n$ are algebraically independent over k, then we are done: take $r = n$ and $y_i = \alpha_i \ \forall i$.

Otherwise, suppose $\alpha_1, \dots, \alpha_n$ are <u>not</u> alg. independent, so that we have a nonzero polynomial $f(x_1, \dots, x_n) \in k[x_1, \dots, x_n]$ such that

$$f(\alpha_1, \dots, \alpha_n) = 0.$$

Take N as in the previous Lemma for this polynomial, and set

$$\begin{cases} \alpha_i' = \alpha_i - \alpha_n^{N^i}, & \text{for } i = 1, \dots, n-1 \\ \alpha_n' = \alpha_n \end{cases}$$

The elements $\alpha_1', \dots, \alpha_n'$ are also generators for A as a k-algebra.

With φ as defined in the previous Lemma,

$$\varphi(f) = f(X_1 + X_n^N, \dots, X_{n-1} + X_n^{N^{n-1}}, X_n) = c \cdot g$$

for some $c \in k \setminus \{0\}$ and $g \in (k[X_1, \dots, X_{n-1}])[X_n]$ a polynomial that is monic in X_n (by the Lemma).

Moreover, $g(\alpha_1', \dots, \alpha_{n-1}', \alpha_n')$

$$= c^{-1} f(\alpha_1 - \alpha_n^N + \alpha_n^N, \dots, \alpha_{n-1} - \alpha_n^{N^{n-1}} + \alpha_n^{N^{n-1}}, \alpha_n)$$

$$= c^{-1} f(\alpha_1, \dots, \alpha_{n-1}, \alpha_n) = 0.$$

Thus α_n' is integral over $\underbrace{k[\alpha_1', \dots, \alpha_{n-1}']}_{\text{k-alg with } n-1 \text{ generators, so inductive hypothesis applies.}}$.

By (5.3), $A = k[\alpha_1', \dots, \alpha_n'] \left(= (k[\alpha_1', \dots, \alpha_{n-1}'])[\alpha_n'] \right)$ is integral over $k[\alpha_1', \dots, \alpha_{n-1}']$.

By inductive hypothesis, $k[\alpha_1', \dots, \alpha_{n-1}']$ is integral over $k[y_1, \dots, y_r]$ for some alg independent elements $y_1, \dots, y_r \in A$.

By transitivity (5.4), we thus have A is integral over $k[y_1, \dots, y_r]$. ∎

<u>Corollary</u> (Zariski's lemma)

Let A be a f.g. k-algebra, where A and k are <u>fields</u>. Then A is a f.g. k-module (i.e., fin. dim. k-vector space).

<u>Pf</u>:

By Noether normalization, A is integral over a subring $k[y_1, \dots, y_r] \subseteq A$.

If $r \geq 1$, then $p = (y_1) \subseteq k[y_1, \dots, y_r]$ is a nonzero prime ideal. As A is integral over $k[y_1, \dots, y_r]$, the Going-up theorem (5.11) implies that there exists a <u>nonzero</u> prime $q \subseteq A$ such that $q \cap k[y_1, \dots, y_r] = p$. (check this yourself!)

But as A is a field, this is a contradiction (fields only have 0 ideal and entire field).

Thus $r = 0$, and A is f.g. k-module as desired. //

<u>Corollary</u>: If k is alg. closed field and A f.g. k-algebra, and $m \subseteq A$ is max ideal, then the composition $k \to A \twoheadrightarrow A/m$ is an isomorphism.

<u>Pf</u>: A f.g. k-alg $\Rightarrow$ A/m f.g. k-alg that is a field.

Thus $k \to A/m$ is a f.g. k-mod (by previous Cor), that is, a finite algebraic extension of k.

But k alg closed $\Rightarrow$ no proper alg extension $\Rightarrow$ $k \to A/m$ iso. //

<u>Corollary (Hilbert's nullstellensatz, weak form)</u>

Let $A = k[x_1, \dots, x_n]$ be a poly ring over an alg. closed field k. Every max ideal $m \subseteq A$ has the form $m = (x_1 - \lambda_1, \dots, x_n - \lambda_n) \subseteq A$, $\lambda_i \in k$.

<u>Pf</u>: Since $\gamma : k \cong A/m$ by previous corollary, the k-algebra map $\pi : A \twoheadrightarrow A/m$ gives $\gamma^{-1}\pi : A \twoheadrightarrow k$ whose <u>kernel</u> is $= m$ and is of the form $(x_1 - \lambda_1, \dots, x_n - \lambda_n)$ some $\lambda_i \in k$. ∎

<u>Corollary (Hilbert's nullstellensatz, alternate weak form)</u>

Let $f_1, \dots, f_n$ be polynomials in $k[x_1, \dots, x_n]$, k = alg. closed field. Then $f_1, \dots, f_n$ generate the unit ideal of $k[x_1, \dots, x_n]$ $\iff$ the polynomials do <u>not</u> vanish simultaneously (alg set $V(f_1, \dots, f_n) = \emptyset$)

<u>Pf</u>: If $(f_1, \dots, f_n) \neq (1)$, then $(f_1, \dots, f_n) \subseteq m \subseteq k[x_1, \dots, x_n]$ for some max ideal m. But the functions in m all vanish at one point of k^n, a contradiction.

On the other hand, if $f_1, \dots, f_n$ all vanish at a point $(\lambda_1, \dots, \lambda_n) \in k^n$, they are then all in the max ideal of polys that vanish at this point, $(x_1 - \lambda_1, \dots, x_n - \lambda_n)$.

Some more details about:

Hilbert's nullstellensatz, weak form

If $A = k[x_1, \dots, x_n]$, k = alg. closed field, then every max ideal of A has the form $m = (x_1 - \lambda_1, \dots, x_n - \lambda_n)$, $\lambda_i \in k$.

Pf:

Let $m \subseteq A$ be a max ideal.

Let $\varphi : A \to k$ be the composition of $A \twoheadrightarrow A/m$ with the isomorphism (from previous Corollary) $A/m \cong k$.

Note that $\ker(\varphi) = m$.

Let $\lambda_i = \varphi(x_i) \in k$, and so we have

$$\ker(\varphi) = \text{kernel of evaluation map } f(x_1, \dots, x_n) \mapsto f(\lambda_1, \dots, \lambda_n)$$
$$= \{ f(x_1, \dots, x_n) \in A \mid f(\lambda_1, \dots, \lambda_n) = 0 \}.$$

Clearly $(x_1 - \lambda_1, \dots, x_n - \lambda_n) \subseteq \ker(\varphi)$, and since $(x_1 - \lambda_1, \dots, x_n - \lambda_n)$ is itself a maximal ideal (check: $A/(x_1 - \lambda_1, \dots, x_n - \lambda_n) \cong k$ also), we must have equality: $(x_1 - \lambda_1, \dots, x_n - \lambda_n) = \ker \varphi = m$.

//