250B: Commutative Algebra

For the Morbidly Curious

Nir Elber

Spring 2022

Contents

THEME 1

HIGHER DIMENSIONS

To deal with a 14-dimensional space, visualize a 3-D space and say 'fourteen' to yourself very loudly. Everyone does it.

—Geoffrey Hinton

1.1 April 19

Welcome back.

1.1.1 The Nullstellensatz Two, Electric Boogaloo

Last time we showed Noether normalization. Today we go over some consequences. Recall the statement of Noether normalization.

Theorem 1.1 (Noether normalization)**.** Fix an affine ring R of dimension d. Given a chain

$$I_1 \subseteq I_2 \subseteq \cdots \subseteq I_m \subseteq R$$

with $d_j := \dim I_j$ such that $\{d_j\}_{j=0}^m$ is strictly decreasing. Then there is a subring $S \subseteq R$ such that

(a) $S \cong k[x_1, \ldots, x_d]$,

(b) R is finite over S, and

(c) any ideal I_j has $S \cap I_j = (x_{d_j+1}, \ldots, x_d)$.

As an example application, we show Hilbert's Nullstellensatz.

Theorem 1.2 (Nullstellensatz)**.** Fix R an (affine) k-algebra.

(a) Given a maximal ideal $\mathfrak{m} \subseteq R$, then $R/\mathfrak{m}$ is a finite extension of k. In particular, if k is algebraically closed, then $R/\mathfrak{m} \cong k$.

(b) The ring R is Jacobson: any prime ideal is the intersection of maximal ideals.

From here one can deduce the usual Nullstellensatz. Anyway, let's prove this.

Proof. We go one at a time.

(a) The dimension of $R/\mathfrak{m}$ is 0 because $R/\mathfrak{m}$ is a field, but $R/\mathfrak{m}$ is an integral extension of k (because R is) while being of finite length (and finitely generated as a k-algebra), so $R/\mathfrak{m}$ is a finite extension of k.

(b) As usual, pick up a prime $\mathfrak{p}$, and we need to show

$$\mathfrak{p} \stackrel{?}{=} \bigcap_{\mathfrak{m}\supseteq\mathfrak{p}} \mathfrak{m}.$$

Certainly we have $\subseteq$, so we show $\supseteq$. As such, for each $f \notin \mathfrak{p}$, we need to show that there exists a maximal ideal $\mathfrak{m}$ containing $\mathfrak{p}$ but not f.

Now, taking the quotient by $\mathfrak{p}$, we may assume that R is an integral domain and that $\mathfrak{p} = (0)$. In particular, we need to show that $f \neq 0$ is avoided by some maximal ideal. However, we showed last time that

$$\dim R/(f) = \dim R - 1.$$

Running through Noether normalization, we can choose $S \cong k[x_1, \ldots, x_d]$ so that $S \cap (f) = (x_1)$. So to get our maximal ideal, we choose

$$(x_1 - 1, x_2, x_3, \ldots, x_d) \subseteq S$$

and then lift to R to some maximal ideal $\mathfrak{n}$. Notably, $f \in \mathfrak{n}$ implies that $\mathfrak{n} \cap S$ contains x_1, which doesn't make sense by the above construction. This finishes. ■

1.1.2 The Geometric $AKLB$ Set-Up

Here is another application.

Proposition 1.3 ($AKLB$ for geometers)**.** Fix an affine domain R over a field k. Now, set L to be a finite extension of $K := K(R)$, and let T be the integral closure of R in L. Then T is a finitely generated R-module; in particular, T is an affine domain.

Proof. Here is the image.

$$\begin{array}{ccc} T & \subseteq & L \\ | & & | \\ R & \subseteq & K \end{array}$$

To begin, we use Noether normalization to force S to be a polynomial ring. Namely, T is still integral over S (because of the chain $S \subseteq R \subseteq T$), and it still suffices to show that T is finite over S.

As such, we may assume that R is a unique factorization domain and in particular is normal. As another reduction, by taking the normal closure of L, we would only make T bigger, so it suffices to take L/K to be a normal extension of fields.

We would like our extension to be Galois, but for this we must fight with the separability condition. In particular, L/K is an inseparable extension if an only if there is an irreducible polynomial $\pi \in K[x]$ with a multiple root α; here, this element α is called purely inseparable. This will in fact mean that $\alpha(\operatorname{char} K)^n \in K$ for some n.

Nonetheless, with L/K any normal extension, we can talk about its automorphism group G and then build the following tower.

$$\begin{array}{l} L \\ \big| \text{ purely insep} \\ L^G \\ \big| \text{ Galois} \\ G \end{array}$$

Namely, we want to not think very hard about L/L^G, but we must.

Example 1.4. The extension $k(t) \subseteq k\left(t^{1/p}\right)$, where $p := \operatorname{char} k > 0$, is a purely inseparable extension.

Anyway, this tower that we may assume that L/K is either Galois or purely inseparable. We do these cases separately.

- Take L/K to be purely inseparable. Here, $K = k(x_1, \ldots, x_d)$. Because L/K is finite and purely inseparable, we can find some q (which is a large power of p) so that L is contained in

  $$k'\left(x_1^{1/q}, \ldots, x_d^{1/q}\right),$$

  where in k' we have to possibly add in some qth roots to make this legal. In particular, we take $L = K\left(\alpha_1^{1/q}, \ldots, \alpha_d^{1/q}\right)$ and then take out the qth roots of variables we need using the fact that $(x+y)^q = x^q + y^q$.

  As such, it suffices to show our result in the case where $L = k'\left(x_1^{1/q}, \ldots, x_d^{1/q}\right)$. But now we can exactly describe our integral closure as

  $$T = k'\left[x_1^{1/q}, \ldots, x_d^{1/q}\right],$$

  which is finite over R because k'/k is finite, and each of the $x_i^{1/q}$ is the root of a monic polynomial $t^q - x_i = 0$ over R. This finishes.

- Now take L/K to be a Galois extension. We pick up the following lemma. We simply outsource the logic here to the following lemma.

Lemma 1.5. Fix a normal Noetherian domain R. Now, set L to be a finite, Galois extension of $K := K(R)$ where $G := \operatorname{Gal}(L/K)$, and let T be the integral closure of R in L. Then T is a finitely generated R-module.

Proof. Note $R \subseteq K = L^G$, and R is normal (i.e., is its own Galois closure in K), so it follows that $R^G = R$. Now, by clearing denominators, we may choose elements $b_1, \ldots, b_n$ to be a basis of L over K. Additionally, we enumerate the elements of G as

$$\{g_1, \ldots, g_n\},$$

where $n := \#\operatorname{Gal}(L/K) = [L : K]$. Now, the Galois action preserves integrality, so the matrix

$$M := \begin{bmatrix} g_1 b_1 & \cdots & g_1 b_n \\ \vdots & \ddots & \vdots \\ g_n b_1 & \cdots & g_n b_n \end{bmatrix}.$$

Now, set $d := \det M$. We make the following observations about d.

- Note that $d \neq 0$ because this would require a relation of the rows

  $$\sum_{i=1}^n a_i g_i b_j = 0$$

  for all j, so in particular $\sum_i a_i g_i = 0$ (as a function $L \to K$!), which contradicts linear independence of automorphisms.[1]

[1] This linear independence is Artin's lemma. As a sketch of the proof, if there is a nontrivial relation, choose the smallest relation, and then rearrange by plugging things in to subtract off and get a smaller relation.

- We do see that $d^2 \in R$ because, picking up any $g \in G$ to the matrix M will merely permute the rows of M, so $gd = \pm d$. In particular, d^2 is fixed by G and hence lives in K. Because d is a linear combination of integral elements (namely, elements that live in T), it is integral over R, so $d \in R$ by normality.

- Lastly, we note that $T \subseteq \frac{1}{d^2}R$. Well, pick up some $b \in T$ and write

$$b = \sum_{i=1}^{n} a_i b_i$$

with $a_i \in K$ using the fact that the $\{b_i\}$ are a basis of L/K. However, pushing this "vector" through M, the ith component comes out to

$$\sum_{j=1}^{n} g_i(b_j) \cdot c_j = g_i\left(\sum_{j=1}^{n} c_j b_j\right) = g_i(b) \in T.$$

In particular, letting M^* denote the adjugate matrix of M, we see that pushing M^* through the above will show that all coefficients live in $\frac{1}{d}R \subseteq \frac{1}{d^2}R$ (because $M^*M = dI$). Thus, we get $c_i \in \frac{1}{d}R$, which is what we wanted.

The last claim shows that T is a submodule of a finitely generated R-module, which shows that T is finite over R, as needed. ■

The above lemma finishes the last case of the proof. ■

Here is an example application.

Exercise 1.6. Fix an algebraically closed field k of characteristic 0. Then consider the fraction field of $k\,[\![x]\!]$ as

$$k\,[\![x]\!] \subseteq k((x)).$$

However, $k((x))$ no longer needs to be algebraically closed, so let L be some finite extension. Then, setting T to be the integral closure of R in L, we get that T is finite over R by Proposition 1.3. In fact, we show $T \cong k\,[\![x^{1/n}]\!]$ for some n.

Proof. Note that T is normal, local, and finitely generated over the ring R. Letting $\mathfrak{m}$ be its maximal ideal, we can get $\mathfrak{m} = (\pi)$ for some element π by pushing a little. As such, T we see that T is a discrete valuation ring. Further, because T is finite over R, we get some n such that

$$\pi^n$$

can be written as lower terms. But this requires $\pi^n = ux$ for some unit u, and the unit u has an nth power by Hensel's lemma (here is where we use $\operatorname{char} k = 0$), so we get that we can replace π by $t^{1/n}$. This finishes. ■

Remark 1.7. This classifies all algebraic extensions of $k((x))$ as $k((x^{1/n}))$, so the algebraic closure of $k((x))$ is simply

$$\bigcup_{n \geq 1} k((x^{1/n})),$$

which is pretty nice.

Example 1.8. Fix some $f \in \mathbb{C}[x, y]$. Writing down $f \in \mathbb{C}[x][y]$ as a polynomial in y, we may write

$$f(x, y) = \sum_{i=1}^{n} p_n(x) y^n.$$

Taking the completion to $\mathbb{C}[\![x]\!][y]$ (i.e., looking locally at $x = 0$), we hope that f is still irreducible; otherwise, we can just take some irreducible factor. Now, we can directly solve for y in this system as some series

$$\sum_{i=-m}^{\infty} c_i x^{i/n}.$$

Now, if p_n is monic, then we can assert that y lives in the integral closure of R, so q is a bona fide power series.

1.1.3 Invariant Theory

Let's return to discussing invariant theory for the end of class; recall that, in an invariant theory, we are interested in studying the group invariants of some group action on an affine ring. We have the following result.

Theorem 1.9. Fix a finite group G and an affine ring T with a G-action. Then T^G is also an affine ring.

Proof. In some sense, we are "quotienting" by the G-action and hoping that we recover an affine ring. Very quickly, note that T is integral over T^G, which we get because G is finite. Namely, for $a \in T$, we simply use the polynomial

$$\prod_{g \in G} (x - ga),$$

which is monic and in $T^G[x]$ because multiplying by some $g \in G$ will merely permute the terms of the product.

We now note that, because T is an affine ring, we suppose that the elements $\{y_1, \ldots, y_m\}$ generate T. Now, we let S be the k-algebra generated by the elementary symmetric polynomials in the $g_i y_j$, of which there are still finitely many while maintaining $S \subseteq T^G$. Now, T is a finitely generated S-module because the generators of S are roots of the polynomials

$$\prod_{g \in G} (x - g y_j) \in S[x],$$

so T is finite over S, meaning that T^G is finite over S. It follows that T^G is an affine ring. ■

Our last topic is on elimination theory, which is what we will spend the next two lectures on. We will have a total of 13 homeworks.