

Math 428, Homework: Completing the Proof of Nullstellensatz

The purpose of this homework set is to complete the proof of Hilbert's Nullstellensatz. Recall that, in class, we reduced it to the following:

Theorem 1. *Suppose that k is an algebraically closed field and $J \subset k[z_1, \dots, z_n]$ is a maximal ideal. Then the "canonical" composite homomorphism*

$$k \rightarrow k[X_1, \dots, X_n] \rightarrow k[X_1, \dots, X_n]/J = L$$

gives an isomorphism of the fields k and L .

Note that this isn't true if k is not algebraically closed: for example if $k = \mathbb{R}$, then $\mathbb{R}[X]/(X^2+1) = \mathbb{C}$ and the map given above is the usual inclusion of \mathbb{R} in \mathbb{C} .

We start with two definitions. Let $\phi : A \rightarrow B$ be a homomorphism of rings. We say B is a *finitely generated A -algebra* if there exist finitely many elements $b_1, \dots, b_n \in B$ such that the homomorphism $A[x_1, \dots, x_n] \rightarrow B$ that takes x_i to b_i is surjective. In this case, if ϕ is injective, we write (slightly abusively) $B = A[b_1, \dots, b_n]$, meaning " B is generated as a ring by A and b_1, \dots, b_n ". For our second definition, we say B is a *finite A -algebra* if there exist $b_1, \dots, b_n \in B$ such that

$$B = \phi(A)b_1 + \dots + \phi(A)b_n \stackrel{\text{def}}{=} \{c_1b_1 + \dots + c_nb_n \mid c_1, \dots, c_n \in \phi(A)\}.$$

As an example, note that $\mathbb{C}[x]$ is a finitely generated \mathbb{C} -algebra; but saying that $\mathbb{C}[x]$ was a finite \mathbb{C} -algebra would be saying that it is finite-dimensional as a complex vector space, which it is not!

Proposition 2. *Let $A \subseteq B \subseteq C$ be subrings.*

- (a) *If B is a finite A -algebra and C is a finite B -algebra then C is a finite A -algebra.*
- (b) *If B is a finite A -algebra and $b \in B$ then there is an equation*

$$(1) \quad b^n + a_{n-1}b^{n-1} + \dots + a_0 = 0$$

that holds in A , where $a_0, \dots, a_{n-1} \in A$.

- (c) *Conversely, if $b \in B$ satisfies an equation of the form (1), then the image of the homomorphism $\psi : A[x] \rightarrow B$ for which $\psi(x) = b$ is a finite A -algebra.*

Problem 3. Prove parts (a) and (c) of the proposition.

The proof of part (b) goes as follows. Suppose that $B = \sum Ab_i$. For each i we have $bb_i \in B$, so there exist elements $a_{ij} \in A$ such that $bb_i = \sum a_{ij}b_j$, i.e. so that $(b\delta_{ij} - a_{ij}b_j = 0$ (where δ_{ij} is the usual Kronecker delta). We can think of this as a matrix equation,

$$M \cdot \begin{pmatrix} b_1 \\ b_2 \\ \vdots \\ b_n \end{pmatrix} = 0$$

where M is the $n \times n$ matrix with values in A whose i, j entry is

$$(2) \quad M_{ij} = b\delta_{ij} - a_{ij}.$$

Now let Δ be the determinant of the matrix M . Standard linear algebra tells you that, if $\text{adj}(M)$ denotes the adjoint matrix of M (that is, the matrix of cofactors), then $\text{adj}(M) \cdot M = \Delta \cdot I$. [The computations that give this are completely formal and work in any commutative ring with 1.] So, we find that, if \mathbf{b} denotes the column vector whose entries are b_1, \dots, b_n , then

$$0 = \text{adj}(M) \cdot M \cdot \mathbf{b} = \Delta \cdot \mathbf{b},$$

which implies $\Delta b_i = 0$ for all i . Now, finally, we use the hypothesis: since $B = \text{sum} Ab_i$, we may write $1 = c_1 b_1 + \cdots + c_n b_n$ for some $c_1, \dots, c_n \in A$. Then $0 = \Delta \cdot \sum c_i b_i = \Delta \cdot 1 = \Delta$. But now, Formula (2) tells us that the determinant Δ is an expression of the form (1). This completes the proof of the Proposition. \square

The next step in the proof is called the “Noether normalization lemma:”

Theorem 4. *Let k be an infinite field and A a finitely generated k -algebra, say $A = k[a_1, \dots, a_n]$ for $a_1, \dots, a_n \in A$. Then there exist $m \leq n$ and $y_1, \dots, y_m \in A$ such that*

- (1) *the natural homomorphism $k[x_1, \dots, x_m] \xrightarrow{\Phi} A$ for which $\Phi(x_i) = y_i$ is injective (here $k[x_1, \dots, x_m]$ is a polynomial ring), and*
- (2) *A is a finite $k[x_1, \dots, x_m]$ -algebra.*

To prove Noether normalization, we proceed by induction on n (that’s right, *not* on m). If $n = 0$ there is nothing to prove.

For the inductive step, assume that the theorem holds whenever the algebra is generated by $n - 1$ or fewer elements; we need to prove that it then holds for $A = k[a_1, \dots, a_n]$. Let

$$I = \ker(k[X_1, \dots, X_n] \rightarrow k[a_1, \dots, a_n] = A).$$

If $I = \{0\}$ we are done, so we may assume $I \neq 0$.

Let $0 \neq f \in I$. We will replace the variables X_1, \dots, X_{n-1} by other variables X'_1, \dots, X'_{n-1} so that f becomes a monic equation for a_n , and then use an induction on n . To fix notation, let’s write $f = F_d + G$ where F_d is *homogeneous of degree d* (that is, it is a sum of monomials of degree d) and G_d has degree at most $d - 1$ (so, we write f as its “degree d part F_d plus the rest”).

Consider the new polynomial

$$H(X'_1, \dots, X'_{n-1}, X_n) = f(X'_1 + \alpha_1 X_n, \dots, X'_{n-1} + \alpha_{n-1} X_n, X_n)$$

in the new variables $(X'_1, \dots, X'_{n-1}, X_n)$; here $\alpha_1, \dots, \alpha_{n-1}$ are constants (i.e. elements of k) that we’ll choose carefully in a moment. Note that we have

$$f(X'_1 + \alpha_1 X_n, \dots, X_n) = F_d(\alpha_1, \alpha_2, \dots, \alpha_{n-1}, 1)X_n^d + \text{stuff}$$

where the “stuff” has X_n appearing to at most the $n - 1$ st power.

Suppose we can make a choice of $\alpha_1, \dots, \alpha_{n-1}$ such that $c = F_d(\alpha_1, \dots, \alpha_{n-1}, 1) \neq 0$. Let $a'_i = a_i - \alpha_i a_n$. Then we get

$$0 = \frac{1}{c} f(a_1, \dots, a_n) = \frac{1}{c} H(a'_1, \dots, a'_{n-1}, a_n),$$

and $\frac{1}{c} H(a'_1, \dots, a'_{n-1}, X_n)$ is a monic polynomial in X_n . So a_n satisfies a monic polynomial relation with coefficients in $A' = k[a'_1, \dots, a'_{n-1}] \subset A$. By our inductive hypothesis, there are elements $y_1, \dots, y_m \in A'$ such that the natural map $k[x_1, \dots, x_m] \rightarrow A'$ that takes x_i to y_i is injective, and such that A' is a finite $k[y_1, \dots, y_m]$ -algebra. But now part (a) of our proposition implies that A is a finite $k[y_1, \dots, y_m]$ -algebra (WHY?) and we are finished.

Well, finished except that we haven’t proven that we can make a choice of $\alpha_1, \dots, \alpha_{n-1}$ such that $F_d(\alpha_1, \dots, \alpha_{n-1}, 1) \neq 0$.

Problem 5. Prove that such $\alpha_1, \dots, \alpha_{n-1}$ exist.

Note that we haven’t yet used that the field k is infinite, and this is where you’ll need it! Anyway, this proves Noether normalization. \square

Finally, on to our proof of the Key Theorem: let $a_1, \dots, a_n \in L$ be the images of z_1, \dots, z_n . Then $L = k[a_1, \dots, a_n]$ is a finitely generated k -algebra. By Noether normalization, there are elements

$y_1, \dots, y_m \in L$ such that the natural homomorphism $k[x_1, \dots, x_m] \rightarrow L$ that takes x_i to y_i is injective, and L is a finite $k[y_1, \dots, y_m]$ -algebra.

Problem 6. Prove that if L is a field and $B \subset L$ is a subring such that L is a finite B -algebra, then B must also be a field.

Using the result of this problem, we discover that $k[y_1, \dots, y_m] \cong k[x_1, \dots, x_m]$ must be a field, which implies $m = 0$. So $m = 0$, and L is a finite k -algebra, i.e. a finite-dimensional k -vector space.

We proved in class that this implies that $L = k$: if $\ell \in L$, then finite-dimensionality of L implies that $1, \ell, \ell^2, \dots, \ell^p$ are linearly dependent for some $p > 0$. So we get an equation $c_0 + c_1\ell + \dots + c_p\ell^p = 0$ in L with not all of c_0, \dots, c_p equal to zero. So ℓ is a root of the polynomial $f = c_0 + c_1x + \dots + c_px^p$, hence, since k is algebraically closed, $\ell \in k$. This proves the Key Theorem! \square

What is the meaning of Noether normalization? Let I be as in the proof, and assume for simplicity that I is a prime ideal. Let $V = V(I) \subset \mathbf{A}_k^n$. Let Y_1, \dots, Y_m be elements of $k[X_1, \dots, X_n]$ whose images in $k[X_1, \dots, X_n]/I = A$ are y_1, \dots, y_m . Then $Y = (Y_1, \dots, Y_m)$ determines a polynomial map $\pi : \mathbf{A}_k^n \rightarrow \mathbf{A}_k^m$. The statement that A is a finite $k[y_1, \dots, y_m]$ -algebra implies that for each $a \in \mathbf{A}_k^m$ there are only finitely many different points $v \in V$ for which $\pi(v) = a$.