HILBERT'S NULLSTELLENSATZ

DANIEL ALLCOCK

This is the simplest proof of the Nullstellensatz that I have been able to come up with. It is meant for students learning commutative algebra for the first time—students perhaps lost in the sea of new vocabulary, with no clear guidance about which concepts are all-important (e.g., Noetherianness, and integrality and finiteness of ring extensions) and which are less so. Accordingly, we use nothing beyond unique factorization in one-variable polynomial rings and the basics of field extensions.

Dan Bernstein led me to some references, and it turns out that my proof is the same in its essentials as one by Zariski [2]. Zariski's proof led to the definition of a class of rings called either Jacobson rings or Hilbert rings, which are defined as "the class of rings to which this argument applies"; see [1] for a discussion. Also, our arguments about denominators motivate the definition of a finite extension of rings, although we avoid using this language explicitly.

I am also grateful to Keith Conrad for his helpful comments.

Theorem. *Let k be a field and K a field extension which is finitely generated as a k-algebra. Then K is algebraic over k.*

Example of Proof. Suppose k is infinite and K is the simple transcendental extension $k(x)$. We claim that if $f_1, \dots, f_m \in K$, then the k-algebra A they generate is smaller than K. To see this, choose $c \in k$ away from the poles of the rational functions f_i. Then no element of A can have a pole at c, so $1/(x-c)$ is not in A, and A is smaller than K. Embellishing this argument yields the full proof:

Proof. We will assume throughout that K is transcendental over k and finitely generated as a k-algebra, and deduce that K is not finitely generated as a k-algebra, a contradiction.

Suppose first that K has transcendence degree one; this means that it contains a subfield $k(x)$ which is a copy of the one-variable rational function field, and that K is algebraic over $k(x)$. This, together with the finite generation of K, shows that K has finite dimension

Date: January 9, 2005.

Partly supported by NSF grants DMS-0245120 and DMS-0231585.

as a $k(x)$-vector space. Choose a basis $e_1, \dots, e_\ell$ and write down the multiplication table for K:

$$e_i e_j = \sum_k \frac{a_{ijk}(x)}{b_{ijk}(x)} e_k \ ,$$

with the a's and b's in $k[x]$. We will show that for any $f_1, \dots, f_m \in K$, the k-algebra A they generate is smaller than K. It is convenient to adjoin $f_0 = 1$ as a generator. Express $f_0, \dots, f_m$ in terms of our basis:

$$f_i = \sum_j \frac{c_{ij}(x)}{d_{ij}(x)} e_j \ ,$$

with the c's and d's in $k[x]$. Now, an element a of A is a k-linear combination of $f_0 = 1$ and products of $f_1, \dots, f_m$. Expanding in terms of our basis, we see that a is a $k(x)$-linear combination of products of the e_i, with the special property that the denominators of the coefficients involve only the d's. Using the multiplication table repeatedly, we see that a is a $k(x)$-linear combination of the e_i, whose coefficients' denominators involve only the b's and d's. A precise way to state the result of this argument is: when a is expressed as a $k(x)$-linear combination of the e_i, with every coefficient in lowest terms, then all its coefficients' denominators' irreducible factors are among the irreducible factors of the b's and d's. Therefore

$$\frac{1}{\text{some other irreducible polynomial}} \quad \text{cannot lie in } A,$$

and A is smaller than K.

This argument requires the existence of infinitely many irreducible polynomials in $k[x]$; to prove this one can mimic Euclid's proof of the infinitude of primes in $\mathbb{Z}$. (If k is infinite then one can just take the infinitely many linear polynomials $x - c$, $c \in k$.)

Now suppose K has transcendence degree > 1 over k, and choose a subextension k' over which K has transcendence degree 1. By the above, K is not finitely generated as a k'-algebra, so it isn't as a k-algebra either. (To build k' explicitly, choose k-algebra generators $x_1, \dots, x_n$ for K over k and set $k' = k(x_1, \dots, x_{\ell-1})$, where x_ℓ is the last of the x's which is transcendental over the field generated by its predecessors.) □

'Weak' Nullstellensatz. *Let k be an algebraically closed field. Then every maximal ideal in the polynomial ring $R = k[x_1, \dots, x_n]$ has the form $(x_1 - a_1, \dots, x_n - a_n)$ for some $a_1, \dots, a_n \in k$. As a consequence,*

a family of polynomial functions on k^n with no common zeros generates the unit ideal of R.

Proof. If $\mathfrak{m}$ is a maximal ideal of R then $R/\mathfrak{m}$ is a field which is finitely generated as a k-algebra. By the previous theorem it is an algebraic extension of k, hence equal to k. Therefore each x_i maps to some $a_i \in k$ under the natural map $R \to R/\mathfrak{m} = k$, so $\mathfrak{m}$ contains the ideal $(x_1 - a_1, \ldots, x_n - a_n)$. This is a maximal ideal, so it equals $\mathfrak{m}$. To see the second statement, consider the ideal generated by some given polynomial functions with no common zeros. If it lay in some maximal ideal, say $(x_1 - a_1, \ldots, x_n - a_n)$, then all the functions would vanish at $(a_1, \ldots, a_n) \in k^n$, contrary to hypothesis. Since it doesn't lie in any maximal ideal, it must be all of R. □

Nullstellensatz. *Suppose k is an algebraically closed field and g and $f_1, \ldots, f_m$ are members of $R = k[x_1, \ldots, x_n]$, regarded as polynomial functions on k^n. If g vanishes on the common zero-locus of the f_i, then some power of g lies in the ideal they generate.*

Proof. Probably no one will ever improve on the trick of Rabinowitsch: the polynomials $f_1, \ldots, f_m$ and $x_{n+1}g - 1$ have no common zeros in k^{n+1}, so by the weak Nullstellensatz we can write

$$1 = p_1 f_1 + \cdots + p_m f_m + p_{m+1} \cdot (x_{n+1} g - 1) \, ,$$

where the p's are polynomials in $x_1, \ldots, x_{n+1}$. Taking the image of this equation under the homomorphism $k[x_1, \ldots, x_{n+1}] \to k(x_1, \ldots, x_n)$ given by $x_{n+1} \mapsto 1/g$, we find

$$1 = p_1\left(x_1, \ldots, x_n, \frac{1}{g}\right) f_1 + \cdots + p_m\left(x_1, \ldots, x_n, \frac{1}{g}\right) f_m \, .$$

After multiplying through by a power of g to clear denominators, we have Hilbert's theorem. □

References

[1] D. Eisenbud, *Commutative Algebra with a View Toward Algebraic Geometry*, Springer-Verlag 1995.

[2] O. Zariski, A new proof of Hilbert's Nullstellensatz, *B.A.M.S.* **53** (1947) 362–368.

Department of Mathematics, University of Texas, Austin
E-mail address: allcock@math.utexas.edu
URL: http://www.math.utexas.edu/~allcock