THE HILBERT NULLSTELLENSATZ

DANIEL R. GRAYSON

1. The proof

The proof of the Hilbert Nullstellensatz below is essentially the same as the first one provided by Zariski in [3], except that the inductive argument in lemma 1.6 below is reversed. Other interesting proofs depending on the notion of *Jacobson* ring or *Hilbert* ring are provided by Krull in [2] and by Goldman in [1]. The main point of all of these proofs is that they do not depend on Noether normalization.

Lemma 1.1. *Suppose K is a field and $R \subseteq K$ is a subring. If K is integral over R, then R is a field.*

Proof. This proof is well known. Suppose $r \in R$. Pick an equation $(1/r)^n = b_{n-1}(1/r)^{n-1} + \cdots + b_0$ of integral dependence with $b_0, \ldots, b_{n-1} \in R$. Multiplying by r^{n-1} gives an equation that shows $1/r \in R$. □

Lemma 1.2. *Suppose K is a field, $R \subseteq K$ is a subring, $x \in K$, and $R[x] = K$. Then for some nonzero $s \in R$ the subring $R[1/s]$ is a field, and x is algebraic over it.*

Proof. Let $F = \mathrm{frac}(R) \subseteq K$ be the fraction field of R. Since $F[x] = K$, we see that x is algebraic over F, with minimal polynomial $x^n + f_{n-1}x^{n-1} + \cdots + f_0$, say. Let $s \in R$ be a common denominator for $f_0, \ldots, f_{n-1}$, so that $f_0, \ldots, f_{n-1} \in R[1/s]$. This makes K integral over $R[1/s]$, so by lemma 1.1, $R[1/s]$ is a field. □

Lemma 1.3. *Suppose $R = \mathbb{Z}$ or $R = F[T]$ is a polynomial ring over a field F. Suppose $u \in R$. Then $R[1/u]$ is not a field.*

Proof. This fact is well known. Since R has an infinite number of prime elements, reciprocals for all of them cannot be provided by inverting just u. □

Lemma 1.4. *Suppose K is a field, $F \subseteq K$ is a subfield, and $x \in K$. Suppose $u \in F[x]$ and $F[x, 1/u] = K$. Then $F[x] = K$ and x is algebraic over F.*

Proof. If x were transcendental over F, then $F[x]$ would be a polynomial ring, and by 1.3, $F[x, 1/u]$ could not be a field. Hence x is algebraic over F, and thus $F[x]$ is already a field, with $1/u \in F[x]$ and $F[x] = F[x, 1/u] = K$. □

Lemma 1.5. *Suppose K is a field, $R \subseteq K$ is a subring, and $x \in K$. Suppose $u \in R[x]$ and $R[x, 1/u] = K$. Then for some nonzero $s \in R$ we have $R[1/s][x] = K$, the subring $R[1/s]$ is a field, and x is algebraic over $R[1/s]$.*

Date: October 23, 2001.
Supported by the NSF.

Proof. Let $F = \mathrm{frac}(R) \subseteq K$. Applying lemma 1.4 we see that $F[x] = K$ and x is algebraic over F. Since $1/u \in K$ we may write it in the form $1/u = f_{n-1}x^{n-1} + \cdots + f_0$ with $f_0, \ldots, f_{n-1} \in F$. Let $t \in R$ be a common denominator for $f_0, \ldots, f_{n-1}$, so that $f_0, \ldots, f_{n-1} \in R[1/t]$; thus $1/u \in R[1/t][x]$ and $R[1/t][x] = K$. Applying lemma 1.2 to $R' = R[1/t]$ we find an element $s' \in R'$ so that $R'[1/s']$ is a field, and x is algebraic over it. Writing $s' = q/t^m$ we see that $R'[1/s'] = R[1/t][1/s'] = R[1/qt]$, so setting $s = qt$ gives what we wanted. □

Lemma 1.6. *Suppose K is a field, $A \subseteq K$ is a subring, $x_1, \ldots, x_n \in K$, and $A[x_1, \ldots, x_n] = K$. Then for some nonzero $s \in A$ the subring $A[1/s]$ is a field and K is a finite algebraic extension of it.*

Proof. If $n \geq 1$ we apply lemma 1.5 with $R = A[x_1, \ldots, x_{n-1}]$, $x = x_n$, and $u = 1$ to get an element $s' \in R$ so that $K' = A[x_1, \ldots, x_{n-1}][1/s']$ is a field and x_n is algebraic over it. If $n \geq 2$ we may apply the lemma again to get $s'' \in R' = A[x_1, \ldots, x_{n-2}]$ so that $K'' = A[x_1, \ldots, x_{n-2}][1/s'']$ is a field and K' is a finite algebraic extension of it. Applying the lemma $n - 2$ more times gives the result. □

Theorem 1.7 (Hilbert Nullstellensatz)**.** *Suppose $F \subseteq K$ are fields, $x_1, \ldots, x_n \in K$, and $F[x_1, \ldots, x_n] = K$. Then K is a finite algebraic extension of F.*

Proof. Apply lemma 1.6 with $A = F$ and observe that $F[1/s] = F$. □

Corollary 1.8. *Suppose F is an algebraically closed field, $R = F[X_1, \ldots, X_n]$ is a polynomial ring, and $M \subseteq R$ is a maximal ideal. Then there exist elements $c_1, \ldots, c_n \in F$ so that $M = (X_1 - c_1, \ldots, X_n - c_n)$.*

Proof. This proof is well known. Let $K = R/M$, and set $x_i = X_i + M \in K$. Applying 1.7 we see that K is an algebraic extension of F; since F is algebraically closed, the map $\theta : F \to K$ is an isomorphism. Setting $c_i = \theta^{-1}(x_i)$, we see that the ideal $(X_1 - c_1, \ldots, X_n - c_n)$ is a maximal ideal contained in M, hence is equal to M. □

Corollary 1.9. *Suppose F is a field, $R = F[X_1, \ldots, X_n]$ is a polynomial ring, $I \subseteq R$ is an ideal, and $r \in R$ is an element contained in every maximal ideal that contains I. Then some power of r is contained in I.*

Proof. This proof is essentially due to Rabinowitch. Form the ring of fractions $S = (R/I)[1/r]$ of the quotient ring R/I. Assuming that no power of r is contained in I, it follows that S is a nonzero noetherian ring, and we may let $N \subseteq S$ be a maximal ideal. The ring $K = S/N$ is a field and is generated as an F-algebra by the images of $X_1, \ldots, X_n, 1/r$, so by 1.7 is a finite algebraic extension of F. The image of the map $\phi : R \to S/N$ is an intermediate ring in a finite algebraic extension, so is itself a field. Letting M be the kernel of ϕ, we see that M is a maximal ideal which does not contain r. □

Corollary 1.10. *Let K be a field which is finitely generated as a $\mathbb{Z}$-algebra. Then K is a finite field.*

Proof. Apply lemma 1.6 with $A = \mathrm{im}(\mathbb{Z} \to K)$ to obtain an element $s \in A$ with $A[1/s]$ a field over which K is finite algebraic. Since $A[1/s]$ is a field, A must be a finite prime field, for otherwise, A would be isomorphic to $\mathbb{Z}$ and lemma 1.3 would apply. Hence $A = A[1/s]$ and K is a finite algebraic extension of A, ensuring it is a finite field, too. □

References

[1] Oscar Goldman. Hilbert rings and the Hilbert Nullstellensatz. *Math. Z.*, 54:136–140, 1951.
[2] Wolfgang Krull. Jacobsonsches Radikal und Hilbertscher Nullstellensatz. In *Proceedings of the International Congress of Mathematicians, Cambridge, Mass., 1950, vol. 2*, pages 56–64, Providence, R. I., 1952. Amer. Math. Soc.
[3] Oscar Zariski. A new proof of Hilbert's Nullstellensatz. *Bull. Amer. Math. Soc.*, 53:362–368, 1947.

University of Illinois at Urbana-Champaign
E-mail address: dan@math.uiuc.edu
URL: http://www.math.uiuc.edu/~dan