

A NEW PROOF OF HILBERT'S NULLSTELLENSATZ

OSCAR ZARISKI

Introduction. A number of proofs of Hilbert's Nullstellensatz can be found in the literature. One, based on elimination theory and due to A. Rabinowitsch, is reproduced in van der Waerden's *Moderne Algebra*, vol. 2, p. 11. In a later chapter van der Waerden gives another proof which is based on the method of specialization in fields of algebraic functions (pp. 59–61). The finishing touches to this proof (p. 65) presuppose the decomposition theorem for polynomial ideals. In his *Ergebnisse* monograph *Idealtheorie*, p. 46, Krull gives an ideal-theoretic proof which, while it is based on the simple remark by Rabinowitsch, is of an advanced nature, since the proof makes use of the full dimension theory of algebraic varieties developed in §17, pp. 41–43. The main "Dimensionsatz" of p. 43 is based on a result which is proved only in §48, pp. 129–134. Moreover, the concept of integral dependence and the "Normalization theorem" of Emmy Noether are used in Krull's proof.

In the present note we give first of all a short proof of Hilbert's Nullstellensatz which makes use only of the rudiments of field theory and ideal theory. Actually we give two new proofs of the Nullstellensatz. A lemma used in the second proof enables us to establish a result on finite integral domains which we were not able to find in the literature. This result is as follows:

If $R = K[\xi_1, \xi_2, \dots, \xi_n]$ is a finite integral domain over a field K and if \bar{K} is the algebraic closure of K in R , then \bar{K} contains all the fields which are contained in R .

1. First proof of the Nullstellensatz. Let \mathfrak{P}_n denote the polynomial ring $K[x_1, x_2, \dots, x_n]$ in n indeterminates x_i , over a given ground field K . By a point $\alpha = (\alpha_1, \alpha_2, \dots, \alpha_n)$ we mean an ordered n -tuple of algebraic quantities α_i over K . Our convention will be that conjugate n -tuples over K represent the same point over K . Let S_n denote the (linear) space of all points. By a zero α of an ideal \mathfrak{A} in \mathfrak{P}_n we mean a point α such that $f(\alpha) = 0$ for every polynomial $f(x) [=f(x_1, x_2, \dots, x_n)]$ in \mathfrak{A} . The totality of zeros of \mathfrak{A} is the algebraic variety in S_n determined by the ideal \mathfrak{A} and shall be denoted by $\mathcal{U}(\mathfrak{A})$.

If W is an algebraic variety in S_n , we shall denote by $\mathfrak{I}(W)$ the ideal in \mathfrak{P}_n consisting of all polynomials which vanish on W (that is, at every point of W). The Hilbert Nullstellensatz asserts the following:

Received by the editors November 4, 1946.

H_1 : If \mathfrak{A} is an ideal in \mathfrak{F}_n then $\mathfrak{J}(\mathcal{U}(\mathfrak{A})) = \text{radical of } \mathfrak{A}$.

It has been shown by Rabinowitsch that the following special case of Hilbert's Nullstellensatz is equivalent to the full Nullstellensatz:

H_2 : If $\mathcal{U}(\mathfrak{A})$ is an empty set then \mathfrak{A} is the unit ideal.

For the convenience of the reader we reproduce here the original proof of Rabinowitsch. Let x_{n+1} be an extra indeterminate and let \mathfrak{F}_{n+1} be the polynomial ring $\mathbb{K}[x_1, x_2, \dots, x_{n+1}]$. If $f(x)$ is any polynomial in \mathfrak{F}_n which vanishes on $\mathcal{U}(\mathfrak{A})$ and if we set $g = 1 + x_{n+1}f$, then the ideal \mathfrak{B} generated in \mathfrak{F}_{n+1} by \mathfrak{A} and g is such that $\mathcal{U}(\mathfrak{B})$ is empty. Hence by the special case H_2 of the Nullstellensatz it follows that $\mathfrak{B} = (1)$. There exists therefore an identity of the form

$$\sum_i A_i h_i + gh = 1, \quad A_i \in \mathfrak{A}; h_i, h \in \mathfrak{F}_{n+1}.$$

On replacing x_{n+1} in this identity by $-1/f$ and clearing the denominators we find a relation of the form $\sum A_i B_i = f^\rho$, where $B_i \in \mathfrak{F}_n$ and ρ is a non-negative integer. Hence f belongs to the radical of \mathfrak{A} , and since the inclusion: radical of $\mathfrak{A} \subseteq \mathfrak{J}(\mathcal{U}(\mathfrak{A}))$ is trivial, this establishes the Nullstellensatz.

Let R_n denote any finite integral domain over \mathbb{K} which can be obtained from \mathbb{K} by an n -fold ring extension: $R_n = \mathbb{K}[\xi_1, \xi_2, \dots, \xi_n]$. To prove H_2 we first show that H_2 is an immediate consequence of the following statement:

H_3^n : If a finite integral domain R_n (over \mathbb{K}) is a field then it is an algebraic extension of the field \mathbb{K} .

For if \mathfrak{A} is an ideal in \mathfrak{F}_n , different from the unit ideal, then \mathfrak{A} is contained in some maximal ideal of \mathfrak{F}_n . If \mathfrak{p} is such a maximal ideal and if we set $R_n = \mathfrak{F}_n/\mathfrak{p} = \mathbb{K}[\alpha_1, \alpha_2, \dots, \alpha_n]$, then R_n is a field and, therefore, if we assume H_3^n , it follows that the α_i are algebraic over \mathbb{K} , that is, $\alpha = (\alpha_1, \alpha_2, \dots, \alpha_n)$ is a point. This point is a zero of \mathfrak{p} and hence a fortiori a zero of \mathfrak{A} , since $\mathfrak{A} \subseteq \mathfrak{p}$. We have thus shown that if $\mathfrak{A} \neq (1)$ then $\mathcal{U}(\mathfrak{A})$ is not empty, and this establishes H_2 .

The proof of Hilbert's Nullstellensatz is thus reduced to proving H_3^n . We shall prove H_3^n by induction with respect to n , since H_3^1 is trivial (if $\mathbb{K}[\xi_1]$ is a field, then $1/\xi_1 = f(\xi_1) \in \mathbb{K}[\xi_1]$ and hence ξ_1 is a root of the polynomial $xf(x) - 1$).

Granted that H_3^{n-1} is true, let R_n be a given finite integral domain $\mathbb{K}[\xi_1, \xi_2, \dots, \xi_n]$ and let it be assumed that R_n is a field. Under this assumption we shall have $R_n = \mathbb{K}(\xi_1)[\xi_2, \xi_3, \dots, \xi_n]$, where $\mathbb{K}(\xi_1)$ is the field generated over \mathbb{K} by ξ_1 . Hence if we apply H_3^{n-1} to R_n thought of as an R_{n-1} over the field $\mathbb{K}(\xi_1)$, we conclude that R_n is an algebraic extension of $\mathbb{K}(\xi_1)$. To complete the proof of H_3^n it remains only to

show that ξ_1 is algebraic over K .

Each $\xi_i, i=2, 3, \dots, n$, is a root of a polynomial $f_i(X)$ with coefficients in $K[\xi_1]$. Let b_i be the leading coefficient of $f_i(X), b_i \neq 0$. If ω is any element of R_n , there will exist an integer ρ (depending on ω) such that the product $\omega \cdot (b_2 b_3 \dots b_n)^\rho$ can be expressed as a linear combination, with coefficients in $K[\xi_1]$, of the $m_2 m_3 \dots m_n$ power products $\xi_2^{j_2} \xi_3^{j_3} \dots \xi_n^{j_n}, 0 \leq j_i \leq m_i - 1$, where m_i is the degree of $f_i(X)$.

Let ν be the relative degree of R_n over $K(\xi_1)$ and let $\omega_1=1, \omega_2, \dots, \omega_\nu$ be a linear basis of R_n over $K(\xi_1)$. We can find an element b_1 in $K[\xi_1], b_1 \neq 0$, such that for each of the above $m_2 m_3 \dots m_n$ power products $\xi_2^{j_2} \xi_3^{j_3} \dots \xi_n^{j_n}$ the following is true: in the expression of $b_1 \cdot \xi_2^{j_2} \xi_3^{j_3} \dots \xi_n^{j_n}$ as a linear combination of the elements $\omega_1, \omega_2, \dots, \omega_\nu$, with coefficients in $K(\xi_1)$, the coefficient of ω_1 is in $K[\xi_1]$. It follows that if we set $b = b_1 b_2 \dots b_n$ then b is an element of $K[\xi_1]$, different from zero, having the following property: for any element ω in R_n there exists an integer ρ such that if $\omega b^\rho = a_1 + a_2 \omega_2 + \dots + a_\nu \omega_\nu, a_i \in K(\xi_1)$, then $a_1 \in K[\xi_1]$. Now let ζ be an arbitrary element of $K[\xi_1], \zeta \neq 0$, and let us apply this result to $\omega = 1/\zeta$. Since $1, \omega_2, \dots, \omega_\nu$ are independent over $K(\xi_1)$ and since $b^\rho/\zeta \in K(\xi_1)$, it follows then that $b^\rho/\zeta = a_1$, that is, any element ζ of $K[\xi_1], \zeta \neq 0$, divides some power of the fixed element b of $K[\xi_1]$. The existence of an element $b \neq 0$ with this property clearly implies that $K[\xi_1]$ cannot be a ring of polynomials in one indeterminate over K . Hence ξ_1 is algebraic over K , and this completes the proof of H_3^2 .

2. Second proof. In this section we shall give a second proof of the Nullstellensatz. If we take for \mathfrak{A} a prime ideal then H_1 yields the following result:

H_4^2 : If \mathfrak{p} is a prime ideal in \mathfrak{P}_n then $\mathfrak{J}(\mathcal{U}(\mathfrak{p})) = \mathfrak{p}$.

This is the most important consequence of the Nullstellensatz, since it shows that there exists a one-to-one correspondence between the irreducible varieties in S_n and the prime ideals in \mathfrak{P}_n . It is therefore desirable to prove H_4^2 directly. On the other hand it is easy to deduce from H_4^2 the full Nullstellensatz. In fact, H_4^2 implies that if $\mathfrak{p} \neq (1)$ then $\mathcal{U}(\mathfrak{p})$ is not empty. Since any ideal \mathfrak{A} in \mathfrak{P}_n which is different from the unit ideal is contained in some prime ideal $\mathfrak{p} \neq (1)$ (for instance in a maximal ideal), we see that from H_4^2 follows H_2 , that is, the full Nullstellensatz.

We shall prove H_4^2 by induction with respect to n , since H_4^1 is trivial. The proof will be based on the following lemma:

LEMMA 1. Let Ω be an integral domain and let R be an integral domain contained in Ω . If Ω is a simple ring extension of $R: \Omega = R[\omega]$, then there

exists in R an element $a \neq 0$ with the following property: if \mathfrak{p} is a prime ideal in R such that $a \notin \mathfrak{p}$, then $\Omega \cdot \mathfrak{p} \neq (1)$.

PROOF. We shall use small Latin and Greek letters to indicate respectively elements of R and Ω . In the proof we may assume that ω is algebraic over R , since otherwise the assertion of the lemma is trivial (if ω is transcendental over R then $\Omega \mathfrak{A} \neq (1)$ for any ideal \mathfrak{A} in R , $\mathfrak{A} \neq (1)$). Let

$$(1) \quad b_0 \omega^\nu + b_1 \omega^{\nu-1} + \cdots + b_\nu = 0, \quad b_0 \neq 0, b_i \in R,$$

be an equation of least degree ν which ω satisfies over R . If \mathfrak{A} is any ideal in R then any element ζ of $\Omega \mathfrak{A}$ is of the form: $\zeta = f(\omega)$, where f is a polynomial with coefficients in \mathfrak{A} . If we use (1) to reduce the degree of f we see that there exists an integer ρ (depending on ζ) such that

$$(2) \quad \zeta \cdot b_0^\rho = c_1 \omega^{\nu-1} + c_2 \omega^{\nu-2} + \cdots + c_\nu, \quad c_i \in \mathfrak{A}.$$

If the element ζ also belongs to R , say $\zeta = z$, then (2) is a relation of algebraic dependence for ω over R , of degree less than ν . Hence necessarily $c_1 = c_2 = \cdots = c_{\nu-1} = 0$ and

$$(3) \quad z b_0^\rho = c_\nu \in \mathfrak{A}.$$

If $z = 1$ then (3) yields $b_0^\rho \in \mathfrak{A}$, that is, b_0 is in the radical of \mathfrak{A} . Hence if the radical of \mathfrak{A} does not contain b_0 then $\Omega \mathfrak{A} \neq (1)$. It follows that the element b_0 is an element a the existence of which is asserted in the lemma.

We now come to the proof of H_4^n . Let $f(x)$ be an element of $\mathfrak{U}(\mathcal{U}(\mathfrak{p}))$. We have to show that

$$(4) \quad f(x) \in \mathfrak{p}.$$

We pass to the ring of residual classes $\Omega = \mathfrak{P}_n/\mathfrak{p} = \mathbb{K}[\xi_1, \xi_2, \cdots, \xi_n]$, where ξ_i is the \mathfrak{p} -residue of x_i . Let $\zeta = f(\xi)$. We have to show that

$$(5) \quad \zeta = 0.$$

The case $\mathfrak{p} = (0)$ is trivial. Hence we may assume that $\mathfrak{p} \neq (0)$. In this case there exists a non-identical algebraic relation between the elements $\xi_1, \xi_2, \cdots, \xi_n$, with coefficients in \mathbb{K} . We may therefore assume that ξ_n is algebraically dependent on $\xi_1, \xi_2, \cdots, \xi_{n-1}$, over \mathbb{K} . We set $R = \mathbb{K}[\xi_1, \xi_2, \cdots, \xi_{n-1}]$. To our present two rings R and Ω we apply Lemma 1. Let a be an element of R , $a \neq 0$, the existence of which is asserted in the lemma.

We shall now show that if H_4^{n-1} is granted, then the hypothesis that (5) is not satisfied leads to a contradiction. Every element of Ω

is algebraic over R . In particular, let

$$(6) \quad d_0 \zeta^s + d_1 \zeta^{s-1} + \dots + d_s = 0, \quad d_i \in R,$$

be a relation of algebraic dependence for ζ over R . Let us assume that (5) is false: $\zeta \neq 0$. Then we may also assume that $d_s \neq 0$. Since a and d_s are in R , these elements can be expressed as polynomials in $\xi_1, \xi_2, \dots, \xi_{n-1}$, with coefficients in K :

$$(7) \quad a = g(\xi_1, \xi_2, \dots, \xi_{n-1}), \quad a \neq 0;$$

$$(7a) \quad d_s = h(\xi_1, \xi_2, \dots, \xi_{n-1}), \quad d_s \neq 0.$$

Let $f_1(x) = g(x)h(x) \in \mathfrak{P}_{n-1}$, and let $\mathfrak{p}_1 = \mathfrak{p} \cap \mathfrak{P}_{n-1}$. It is clear that $R \cong \mathfrak{P}_{n-1}/\mathfrak{p}_1$ and that $\xi_1, \xi_2, \dots, \xi_{n-1}$ are the \mathfrak{p}_1 -residues of x_1, x_2, \dots, x_{n-1} . We shall show now that

$$(8) \quad f_1(x) \in \mathfrak{J}(\mathcal{U}(\mathfrak{p}_1)).$$

Let $P_1(\alpha_1, \alpha_2, \dots, \alpha_{n-1})$ be any point of $\mathcal{U}(\mathfrak{p}_1)$. If P_1 is a zero of the polynomial $g(x)$ there is nothing to prove. Assume then that P_1 is not a zero of $g(x)$. The ideal $\mathfrak{J}(P_1)$ is a maximal (prime) ideal in \mathfrak{P}_{n-1} which contains \mathfrak{p}_1 , since $P_1 \in \mathcal{U}(\mathfrak{p}_1)$. Hence if we set $\mathfrak{p}_0 = \mathfrak{J}(P_1)/\mathfrak{p}_1$, then \mathfrak{p}_0 is a maximal prime ideal in R , and the assumption that P_1 is not a zero of $g(x)$ signifies, in view of (7), that $a \notin \mathfrak{p}_0$. Hence, by Lemma 1, the ideal $\Omega \cdot \mathfrak{p}_0$ is not the unit ideal. Let \mathfrak{p}'_0 be a maximal prime ideal in Ω which contains the ideal $\Omega \cdot \mathfrak{p}_0$. Since $\mathfrak{p}_0 \subseteq \mathfrak{p}'_0$ and since \mathfrak{p}_0 is maximal in R , it follows that $\mathfrak{p}'_0 \cap R = \mathfrak{p}_0$. Hence the \mathfrak{p}'_0 -residues of $\xi_1, \xi_2, \dots, \xi_{n-1}$ can be identified with their \mathfrak{p}_0 -residues, that is, with the algebraic quantities $\alpha_1, \alpha_2, \dots, \alpha_{n-1}$ respectively. Let α_n be the \mathfrak{p}'_0 -residue of ξ_n . Since $K[\alpha_1, \alpha_2, \dots, \alpha_{n-1}, \alpha_n] = \Omega/\mathfrak{p}'_0$ is a field, α_n is algebraically dependent on $K[\alpha_1, \alpha_2, \dots, \alpha_{n-1}]$, whence also α_n is algebraic over K . Hence $\alpha = (\alpha_1, \alpha_2, \dots, \alpha_{n-1}, \alpha_n)$ is a point P of S_n . Since the coördinates of this point are residues of $\xi_1, \xi_2, \dots, \xi_n$ and since $K[\xi_1, \xi_2, \dots, \xi_n] = \mathfrak{P}_n/\mathfrak{p}$, it follows that the point P belongs to $\mathcal{U}(\mathfrak{p})$. Hence P is also a zero of the polynomial $f(x)$, since, by hypothesis, $f(x)$ vanishes on $\mathcal{U}(\mathfrak{p})$. This implies that $f(\xi)$, that is, ζ , belongs to \mathfrak{p}_0 . But then, in view of (6), also d_s belongs to \mathfrak{p}_0 , and therefore, by (7a), $h(\alpha) = 0$, and this establishes (8).

3. An application. By the hypothesis H_4^{n-1} of our induction it follows from (8) that $f_1(x)$ belongs to \mathfrak{p}_1 . Hence $f_1(\xi) = 0$, that is, $ad_s = 0$, in contradiction with $a \neq 0$ and $d_s \neq 0$. This completes the proof of H_4^n .

We shall now proceed to the proof of the theorem stated in the introduction. Let R be a finite integral domain over K : $R = K[\xi_1, \xi_2, \dots, \xi_n]$, and let K' be the set of elements of R which

are algebraic over K . It is clear that K' is not only a ring but also a field, since if $\alpha \in K'$ then $K(\alpha) = K[\alpha]$. Since we have $R = K'[\xi_1, \xi_2, \dots, \xi_n]$, we shall replace K by K' . We assume therefore that K is maximally algebraic in R (that is, $K = K'$).

LEMMA 2. K is a maximal subfield of R .

PROOF. Let \mathfrak{p} be a fixed maximal prime ideal in R and let x be any element of R which does not belong to K . By H_3^2 the field R/\mathfrak{p} is an algebraic extension of K . Hence x satisfies a congruence of the form: $f(x) \equiv 0 \pmod{\mathfrak{p}}$, where f is a polynomial with coefficients in K , not all zero. Since $\mathfrak{p} \neq (1)$, $f(x)$ is not a unit in R . On the other hand since K is maximally algebraic in R and since $x \notin K$, x is transcendental over K . Hence $f(x) \neq 0$. This shows that $K(x)$ is not contained in R . Since this is true for any element x of R which is not in K , the lemma follows.

COROLLARY. If F is any subfield of K such that R is a finite integral domain over F , then the algebraic closure of F in R coincides with K .

For the algebraic closure of F in R is contained in K and on the other hand it must be a maximal subfield of R , in view of Lemma 2.

We shall need the following generalization of Lemma 1:

LEMMA 3. If an integral domain Ω is a finite ring extension of an integral domain R , then for any element α in Ω , $\alpha \neq 0$, there exists a corresponding element a in R , $a \neq 0$, having the following property: if the radical of an ideal \mathfrak{A} in R does not contain a , then the radical of $\Omega\mathfrak{A}$ does not contain α .

PROOF. Let Ω be an n -fold ring extension of R . We shall prove the lemma by induction with respect to n .

Case $n=1$. We use the notation of the proof of Lemma 1 and we consider separately two cases, according as ω is transcendental or algebraic with respect to R .

(a) ω is algebraic over R . We have $\alpha = g(\omega)$, where g is a polynomial with coefficients in R . Let a be the leading coefficient of g , $a \neq 0$. If \mathfrak{A} is an ideal in R and if some power of α belongs to $\Omega \cdot \mathfrak{A}$, then the same power of a must belong to \mathfrak{A} . Hence this element a has the desired property.

(b) ω is transcendental over R . In this case also α is algebraic over R . Let $d_0\alpha^n + d_1\alpha^{n-1} + \dots + d_n = 0$, $d_i \in R$, $d_n \neq 0$, be an equation of algebraic dependence for α over R . If some power α^σ of α belongs to $\Omega \cdot \mathfrak{A}$, then also d_n^σ belongs to $\Omega \cdot \mathfrak{A}$, since α divides d_n in Ω . It follows from (3), for $z = d_n^\sigma$, that $d_n^\sigma b_0^\rho \in \mathfrak{A}$, where ρ is a suitable integer. Therefore if some power of α belongs to $\Omega\mathfrak{A}$ then some power of

d_*b_0 belongs to \mathfrak{A} . Consequently the element $a = d_*b_0$ has the desired property.

Case $n > 1$. Let $\Omega = R[\xi_1, \xi_2, \dots, \xi_n]$, $\Omega_1 = R[\xi_1, \xi_2, \dots, \xi_{n-1}]$, so that $\Omega = \Omega_1[\xi_n]$. By the case $n = 1$, the lemma is applicable if we replace R by Ω_1 . Let α_1 be an element of Ω_1 which plays now the role of a . By the case $n - 1$, the lemma is applicable if we replace Ω by Ω_1 and α by α_1 . This yields an element a of R , $a \neq 0$, which has the desired property in relation to the rings R , Ω and the given element α of Ω . The proof of Lemma 3 is now complete.

We now go back to our original finite integral domain $R = K[\xi_1, \xi_2, \dots, \xi_n]$, where we assume that K is maximally algebraic in R . We have to show that if F is a field contained in R then F is already contained in K . Let x be an arbitrary element of R which does not belong to K . We apply Lemma 3 to the two integral domains $K[x]$ and R (these two rings now play respectively the role of the rings R and Ω of the lemma). We take for α the element 1 of R (nevertheless it is clear that our inductive proof of Lemma 3 could not have been carried out if we had restricted ourselves to the special case $\alpha = 1$). In this special case, Lemma 3, and the fact that x is a transcendental over K , yield the following result: there exists a polynomial $g(x)$ in $K[x]$ such that any irreducible polynomial in $K[x]$ which does not divide $g(x)$ is a nonunit in R . Now let Δ be the intersection of the two fields K and F (the two fields have in common at least the prime subfield of K). We can certainly find a polynomial in $\Delta[x]$ which is relatively prime to $g(x)$ in $K[x]$. If $f(x)$ is such a polynomial, then by the preceding result $f(x)$ is a nonunit in R . Consequently $f(x)$ does not belong to the field F , and since the coefficients of $f(x)$ are in F it follows that x is not in F . Since x was an arbitrary element of R not belonging to K , we conclude that $F \subseteq K$, q.e.d.

From the theorem just proved and from the corollary to Lemma 2 we draw immediately the following consequence:

If R is a finite integral domain over a field K and if F is any subfield of R such that R is a finite integral domain also over F , then R has the same degree of transcendency over K as it has over F .

This result is of course also a consequence of the fundamental theorem in the dimension theory of ideals in finite integral domains: *if r is the degree of transcendency of R over K then every minimal prime ideal in R is of dimension $r - 1$.* On the other hand, the above result gives an a priori reason for the fact that when the dimension of a prime ideal in R is defined *relative to K as ground field*, the resulting dimension theory is intrinsically related to R .