§3. Proof of the Hilbert K-Nullstellensatz

Objekttyp: **Chapter**

Zeitschrift: **L'Enseignement Mathématique**

Band (Jahr): **33 (1987)**

Heft 1-2: **L'ENSEIGNEMENT MATHÉMATIQUE**

PDF erstellt am: **01.06.2024**

Proof. For $m = 1$ we can use $p(y_1) = y_1$. The heart of the proof is the case $m = 2$. We divide the proof for $m = 2$ into two cases.

Case 1. There exists an element α *in* $\bar{k}\backslash K$ *which is separable over* k. Let L be the normal closure of $k(\alpha)$ in $\bar{k}$. Then L is a finite separable extension of k and thus generated by one element β. That is $L = k(\beta)$. Since L is normal all the conjugates $\beta = \beta_1, \beta_2, \ldots, \beta_n$ of β are in L and clearly $L = k(\beta_i)$ for $i = 1, 2, \ldots, n$. We have that L is not contained in K because $\alpha \notin K$. Hence, none of the roots $\beta_1, \beta_2, \ldots, \beta_n$ of the minimal polynomial $f(x) \in k[x]$ of the element β over k, are in K. Consequently, the homogenization.

$$p(y_1, y_2) = y_2^d \cdot f(y_1 \cdot y_2^{-1})$$

of f, where d is the degree of f, has no non-trivial root in $\mathbf{A}_K^2$.

Case 2. All elements of $\bar{k}\backslash K$ *are purely inseparable over* k. Choose an element $\gamma \in \bar{k}\backslash K$. Then $\gamma^q = a$ is in k for some power q of the characteristics of k and γ is the only root of the polynomial $x^q - a$. Hence

$$p(y_1, y_2) = (y_1 - a\, y_2)^q$$

is a homogeneous polynomial without any non-trivial roots in $\mathbf{A}_K^2$.

The two cases above exhaust all possibilities for elements in $\bar{k}\backslash K$. Hence we have proved the existence of homogeneous polynomials in $k[y_1, y_2]$ without any non trivial zeroes.

We now proceed by induction on m. Assume that $m \geqslant 2$ and that we have proved the existence of a homogeneous polynomial $p(y_1, y_2, \ldots, y_m)$ with only the trivial zero in $\mathbf{A}_K^m$. Let $q(y_1, y_2)$ be a homogeneous polynomial with only the trivial zero in $\mathbf{A}_K^2$. Then, if d is the degree of p, we have that $r(y_1, y_2, \ldots, y_{m+1}) = q(p(y_1, y_2, \ldots, y_m), y_{m+1}^d)$ is a homogeneous polynomial with only the trivial zero in $\mathbf{A}_K^{m+1}$. Indeed, the homogeneity is clear, and if $(a_1, a_2, \ldots, a_{m+1}) \in \mathbf{A}_K^{m+1}$ is a zero of r, we must have that $p(a_1, a_2, \ldots, a_m) = 0$ and $a_{m+1} = 0$ since q has no non-trivial zeroes. Then we must have that $a_1 = a_2 = \ldots = a_m = 0$ since the same is true for p.

§ 3. Proof of the Hilbert K-Nullstellensatz

There exists in the literature a great variety of proofs of the Hilbert Nullstellensatz. Most of them start by proving the weak form and then deducing the Nullstellensatz by localization procedures that are more or less related to a method called Rabinowitz trick. We shall next show that Rabinowitz trick also can be used to deduce the Hilbert K-Nullstellensatz from its weak form.

PROPOSITION 6. *We have that the Hilbert K-Nullstellensatz follows from its weak form.*

Proof. It follows from Proposition 3 (i) that it suffices to prove that, if the weak Nullstellensatz holds, then we have an inclusion

$$\{f \in R \mid Z_K(f) \supseteq Z_K(I)\} \subseteq \sqrt[K]{I}$$

for all ideals I in R.

Let f in R be an element that vanishes on $Z_K(I)$. Choose generators $h_1, h_2, \ldots, h_n$ of I and let J be the ideal, in the polynomial ring $R[x]$ in the variable x over R, which is generated by the elements

$$h_1, h_2, \ldots, h_n, 1 - xf$$

of $R[x]$. Since f vanishes on the common zeroes of $h_1, h_2, \ldots, h_n$ in $\mathbf{A}_K^r$, it follows that the subset $Z_K(J)$ of $\mathbf{A}_K^{r+1}$ is empty. It then follows from the weak K-Nullstellensatz that $\sqrt[K]{J} = R[x]$. Hence there is a polynomial $p \in P_K(m)$ for some natural number m and elements $f_1, f_2, \ldots, f_{m-1}$ in $R[x]$ such that

$$p(f_1, f_2, \ldots, f_{m-1}, 1) \in J .$$

That is, there are polynomials $g_1, g_2, \ldots, g_n, g$ in $R[x]$ such that

$$p(f_1, f_2, \ldots, f_{m-1}, 1) = \sum_{i=1}^{n} g_i h_i + g(1-xf) .$$

We substitute $x = y^{-1}$ in the latter equation and obtain, after multiplying by a sufficiently high power y^N of y and using the homogeneity of p, an equation

$$p(f'_1, f'_2, \ldots, f'_{m-1}, y^N) = \sum_{i=1}^{n} g'_i h_i + g'(y-f)$$

in $R[y]$. If we substitute f for y in the latter equation we obtain that

$$p(e_1, e_2, \ldots, e_{m-1}, f^N) \in I$$

where $e_i = f'_i(x_1, x_2, \ldots, x_{r-1}, f)$ for $i = 1, 2, \ldots, m-1$. Consequently we have that $f^N \in \sqrt[K]{I}$. However, by Proposition 3 we have that $\sqrt[K]{I}$ is K-radical and hence radical by Proposition 2. We conclude that $f \in \sqrt[K]{I}$ as was to be proved.

To prove the Hilbert K-Nullstellensatz we must now prove it in the weak form. We shall here give a proof that emphasizes the difference between the case when K is not algebraically closed, which is the main theme of this article, and the traditional case when K is algebraically closed, for which there exists at least as many presentations as there are textbooks in algebra or geometry.

Proof of the weak Hilbert K-Nullstellensatz when K is not algebraically closed

From Proposition 4 (iii) it follows that it suffices to prove that, if I is and ideal of R such that $Z_K(I) = \emptyset$, then we have that $1 \in \sqrt[K]{I}$.

To this end we choose generators $h_1, h_2, ..., h_m$ of the ideal I. By Proposition 5, there is a homogeneous polynomial $p \in k[y_1, y_2, ..., y_m]$ with only the trivial zero in $\mathbf{A}_K^m$. Since the polynomials h_i have no common zero we see that the polynomial

$$g(x_1, x_2, ..., x_r) = p(h_1, h_2, ..., h_m)$$

in R has no zeroes in $\mathbf{A}_K^r$. We homogenize g by substituting $x_i = y_i \cdot y_{r+1}^{-1}$ for $i = 1, 2 ..., r$ and multiplying by y_{r+1}^d, where d is the degree of g. The resulting polynomial $q(y_1, y_2, ... y_{r+1})$ is then in $P_K(r+1)$. Moreover, we have the equalities

$$q(x_1, x_2, ..., x_r, 1) = g(x_1, x_2, ..., x_r) = p(h_1, h_2 ..., h_m)$$

Since p is homogeneous and the h_i are in I, all the members of the latter equalities are in I. Since $q \in P_K(r+1)$ we conclude that $1 \in \sqrt[K]{I}$ as we wanted to prove.

Proof of the weak Hilbert Nullstellensatz

For completeness we give one of the many short proofs of the weak Nullstellensatz. It is based upon the following two elementary results

(a) Let $L[x]$ be a polynomial ring in the variable x over a field L and f a non-zero element of $L[x]$. Then $L[x]_f$ is not a field.

(b) Let A be an integral domain and x an element that is integral over A. If $A[x]$ is a field, then A is a field.

Of these results the second is trivial and the first follows immediately from the existence of infinitely many irreducible polynomials over L.

The weak Nullstellensatz is a consequence of the following more general result.

PROPOSITION 7. *The following two assertions hold.*

(i) *Let P be a prime ideal in R. If $(R/P)_g$ is a field for some element g in R/P, then P is maximal.*

(ii) *Let M be a maximal ideal in R. Denote by S the polynomial ring $k[x_1, x_2, ..., x_{r-1}]$ and let $Q = M \cap S$. Then Q is a maximal ideal in S and the class x of x_r in R/M is algebraic over S/Q.*

Proof. We shall prove the two assertions of the Proposition simultaneously by induction on r. For $r = 1$ the Proposition is assertion (a) above. Assume that the assertions of the Proposition hold for S. We shall prove that they hold for R.

Let P be a prime ideal of R and let $g \in R/P$. We let $Q = P \cap S$ and denote by L the field of fractions of S/Q.

Assume that $(R/P)_g$ is a field. If x denotes the class of x_r in R/P we then obtain that

$$(R/P)_g = (S/Q[x])_g = L[x]_g .$$

From assertion (a) above it follows that x is algebraic over L. Hence $L[x]$ is a field and in particular $L[x] = L[x]_g$.

We obtain on the one hand a relation

$$g^{-1} = a^{-1}(a_0 + a_1 x + ... + a_n x^n)$$

with a and a_i in S/Q for $i = 0, 1, ..., m$ and consequently equalities

$$(R/P)_g = (R/P)_a = (S/Q)_a[x] .$$

On the other hand we obtain a relation

$$bx^n + b_{n-1} x^{n-1} + ... + b_0 = 0$$

with b and b_i in S/Q for $i = 0, 1, ..., n$ and consequently that x is integral over $(S/Q)_{ab}$. Since $(S/Q)_{ab}[x] = (S/Q)_a[x]$ is a field it follows from assertion (b) above that $(S/Q)_{ab}$ is a field. By the induction assumption we then have that Q is maximal. In particular we have that a is invertible in $(S/Q) = L$, so that $(R/P)_g = (R/P)_a = R/P$. Hence the ideal P is maximal. This proves assertion (i) of the Proposition. However, the above proof applied to M gives assertion (ii) so that we have proved the Proposition.

To prove that, if $K = \bar{k}$ and I is a proper ideal of R, we have that $Z_K(I) \neq \emptyset$, we choose a maximal ideal M containing I. By repeated application of assertion (ii) of Proposition 7 we see that there is a k-homomorphism

$$a \colon R/M \to \bar{k} = K$$

Hence, if $\alpha_1, \alpha_2, \ldots, \alpha_r$ are the classes of $x_1, x_2, \ldots, x_r$ in R/M we have that $(a(\alpha_1), a(\alpha_2), \ldots, a(\alpha_n)) \in Z_K(M) \subseteqq Z_K(I)$ and $Z_K(I) \neq \emptyset$ as we wanted to prove.

§ 4. Connections with previous results

A less elegant form of the Hilbert K-Nullstellensatz, that do not involve the K-radical explicitely, is the following:

Let J *be an ideal of* R. *The following two assertions are equivalent:*

(i) *If* $f \in R$ *vanishes on* $Z_K(J)$, *then* $f \in J$.

(ii) *If* $f_1, f_2, \ldots, f_m$ *are polynomials in* R *such that* $p(f_1, f_2, \ldots, f_m) \in J$ *for some* p *in* $P_K(m)$, *then* $f_m \in J$.

From Proposition 4 (ii) it follows that assertion (i) can be stated as

$$J = \{f \in R \mid Z_K(f) \supseteqq Z_K(J)\}$$

and from the definition of the K-radical assertion (ii) can be stated as $J = \sqrt[K]{J}$. Hence the equivalence of the two assertions is the Hilbert K-Nullstellensatz for K-radical ideals. However, if I is any ideal of R, we have that $J = \sqrt[K]{I}$ is K-radical by Proposition 3 and that $Z_K(I) = Z_K(J)$ by Proposition 4 (i). Hence, the above result is equivalent to the Hilbert K-Nullstellensatz

$$\sqrt[K]{I} = \{f \in R \mid Z_K(f) \supseteqq Z_K(I)\}$$

for I.

The sets $P_K(m)$ in the particular case $k = K$, were introduced by Adkins, Gianni and Tognoli [1] in order to prove the above result when $k = K$. As a consequence they obtained the Hilbert Nullstellensatz in the particular case $k = K = \bar{k}$. The reason for introducing the sets $P_K(m)$ in general is to formulate the above more general result, that is a true generalization of the Hilbert Nullstellensatz.