RADICALS AND HILBERT NULLSTELLENSATZ FOR NOT NECESSARILY ALGEBRAICALLY CLOSED FIELDS

L'Enseignement Mathématique, t. 33 (1987), p. 323-338

RADICALS AND HILBERT NULLSTELLENSATZ FOR NOT NECESSARILY ALGEBRAICALLY CLOSED FIELDS

by Dan LAKSOV

§ 1. THE MAIN RESULT AND DEFINITIONS

We shall in the following fix a (commutative) field k and denote by $\bar{k}$ the algebraic closure of k. Moreover, we shall denote by K a subfield of $\bar{k}$ containing k. The polynomial ring $k[x_1, x_2, ..., x_r]$ in r variables over k we denote by R. Given an ideal I in R, we denote by $Z_K(I)$ the algebraic subset of the r-dimensional affine space $\mathbf{A}_K^r$ which consists of the common zeroes of the polynomials in I. That is

$$Z_K(I) = \{(a_1, a_2, ..., a_r) \mid a_i \in K \quad \text{for} \quad i = 1, 2, ..., r \quad \text{and} \quad f(a_1, a_2 ..., a_r) = 0 \quad \text{for all} \quad f \in I\} .$$

The HILBERT NULLSTELLENSATZ is usually stated as follows:

Given an ideal I in R and a polynomial f of R, then f vanishes at all points of $Z_{\bar{k}}(I)$ if and only if $f^n \in R$ for some positive integer n.

In symbols the Hilbert Nullstellensatz can be written in the form:

$$\sqrt{I} = \{f \in R \mid Z_{\bar{k}}(f) \supseteq Z_{\bar{k}}(I)\} .$$

Here $\sqrt{I}$ denotes the *radical* of I, defined as the intersection of all prime ideals containing I, or equivalently by

$$\sqrt{I} = \{f \in R \mid f^n \in R \quad \text{for some positive integer} \quad n\} .$$

As an immediate consequence of the Hilbert Nullstellensatz we obtain the following result which is often referred to as the WEAK HILBERT NULLSTELLENSATZ:

Given an ideal I in R, then I is not all of R if and only if $Z_{\bar{k}}(I)$ is non-empty.

The Hilbert Nullstellensatz is one of the fundamental algebraic tools in geometry because it leads to a dictionary between algebraic subsets of $\mathbf{A}_k^r$ on the one hand and radical ideals in R on the other. In algebraic geometry over a not-necessarily algebraically closed field K the main objects of study are the algebraic subsets of the affine space $\mathbf{A}_K^r$. However, if K is not algebraically closed, there always exists ideals in R with no zeroes in $\mathbf{A}_K^r$. Hence the above correspondence between radical ideals and algebraic sets fails, even in the sence of the weak Nullstellensatz.

The purpose of this article is to prove a generalization of the Hilbert Nullstellensatz which makes it possible to set up a dictionary between the algebraic subsets of $\mathbf{A}_K^r$ on the one hand and certain ideals of R, that we shall call *K-radical*, on the other.

To state our main result it is convenient to introduce the following notation:

Let $y_1, y_2, \ldots$ be a countably infinite set of elements that are algebraically independent over k. We denote by $P_K(m)$ the set of homogeneous polynomials in $k[y_1, y_2, \ldots, y_m]$ whose zeroes in $\mathbf{A}_K^m$, if any, are of the form $(a_1, a_2, \ldots a_{m-1}, 0)$. That is,

$$P_K(m) = \{p \in k[y_1, y_2, \ldots, y_m] \mid p \quad \text{is homogeneous and} \quad Z_K(p) \subseteqq Z_K(y_m)\}$$

Let A be a k-algebra and I an ideal of A. We denote by $\sqrt[K]{I}$ the subset $\{a \in A \mid$ for some positive integer m there exists a polynomial $p \in P_K(m)$ and elements $a_1, a_2, \ldots, a_{m-1}$ of A such that $p(a_1, a_2, \ldots, a_{m-1}, a) \in I\}$.

Below we shall prove that $\sqrt[K]{I}$ is an ideal in A which we call the *K-radical of I*. We can now state the main result of this article, which we shall refer to as the HILBERT K-NULLSTELLENSATZ as follows:

Given an ideal I of R, then

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

As an immediate consequence of the Hilbert K-Nullstellensatz we obtain the following result which we refer to as the WEAK HILBERT K-NULLSTELLENSATZ:

Given an ideal I of R, then $\sqrt[K]{I}$ is not all of T if and only if $Z_K(I)$ is non-empty.

We observe that the Hilbert Nullstellensatz and its weak form are the Hilbert $\bar{k}$-Nullstellensatz and the weak Hilbert $\bar{k}$-Nullstellensatz. Indeed, it is clear that we have

$$P_{\bar{k}}(m) = \{1, y_m, y_m^2, y_m^3, \ldots\} \quad \text{for} \quad m = 1, 2 \ldots$$

Hence it follows from the definition of $\sqrt[K]{I}$ that, *if* $K = \bar{k}$ *then* $\sqrt[K]{I} = \sqrt{I}$ is the usual radical of I.

A result in the direction of the Hilbert Nullstellensatz was given by D. W. Dubois [2] and J. J. Risler [7] when k is ordered and K the real closure of k. A similar weaker result, which is however valid for any field k, when $k = K$, was given by W. A. Adkins, P. Gianni and A. Tognoli [1]. We shall return to these results in § 4 and see how they relate to the results of this article. In that section we also discuss some open problems related to the previous work.

In the process of generalizing the Hilbert Nullstellensatz we introduce, for each pair of fields k and K with $k \subseteqq K$, the K-*radical* of an ideal in any k-algebra. The K-radical of ideals in R makes it possible to give a treatment of the Nullstellensatz over an arbitrary field which is analogous to the traditional presentation over algebraically closed fields. Most properties that hold for the usual radical of an ideal can be seen to hold for the K-radical and the K-radical merits some interest of its own. Below we shall however only give those properties needed in our presentation of the Nullstellensatz. These properties we have collected in § 2. For a more complete treatment see Laksov [4] and [5].

The results of Dubois and Risler strongly suggest that the K-radical of an ideal can be defined by much smaller sets of polynomials than the sets $P_K(m)$. Restricting the set of polynomials used to define the K-radical would be the first step towards generalizing Hilberts 17'th problem and would give extremely interesting information about the fields involved. We shall however show that even modest advances in this direction may be very difficult. To be more precise we introduce, for each natural number m a set

$$P_K^0(m) = \{p \in k[y_1, y_2, ..., y_m] \mid p \text{ is homogeneous and the only zero of } p \text{ in } \mathbf{A}_K^m \text{ is the origin}\}$$

and for any ideal I in R we define a subset I_T of R by

$$I_T = \{f_i \in R \mid \text{for some positive integer } m \geqslant i \text{ there exists a polynomial } p \in P_K^0(m) \text{ and elements } f_1, f_2, ..., f_m \text{ in } R \text{ such that } p(f_1, f_2, ..., f_m) \in I\}$$

Then $P_K^0(m) \subseteq P_K(m)$ and consequently $I_T \subseteq \sqrt[K]{I}$. Moreover we have that $I \subseteq I_T$. The definition of I_T is apparently more natural and symmetric than that of $\sqrt[K]{I}$.

An intriguing problem raised by Tognoli is:

For which pair of fields $k \subseteq K$ *do we have that* $I_T = \sqrt[K]{I}$ *for all ideals* I *of* R?

It was long conjectured that equality holds for all pairs of fields (at least when the characteristics of k is zero). We shall however, in section 5, give examples showing that one may have strict inequality $I_T \subset \sqrt[K]{I}$ for the two pairs $k = K = \mathbf{Z}/2\mathbf{Z}$ and $k = K = \mathbf{Q}$.

Before we proceed (in § 3) to prove the Hilbert K-Nullstellensatz we shall in § 2 collect all the results that we need about the K-radicals and the polynomials $P_K(m)$ in the next section.

§ 2. Some properties of the K-radical

We shall denote by $S(m)$ the polynomial ring $k[y_1, y_2, ..., y_m]$.

LEMMA 1. *Let* $p \in P_K(m)$ *and* $q \in P_k(n)$. *For each polynomial* $s = s(y_1, y_2, ..., y_{m+n}) \in S(m+n)$ *of degree one less than* q, *we have that,*

$$r = p(y_1 \cdot s, y_2 \cdot s, ..., y_{m-1} \cdot s, q(y_{m+1}, y_{m+2}, ..., y_{m+n})) \in P_K(m+n) .$$

Proof. It is clear that r is a homogeneous polynomial in $S(m+n)$. Let $(a_1, a_2, \ldots, a_{m+n}) \in \mathbf{A}_K^{m+n}$ be a zero of r. Since $p \in P_K(m)$, we have that $q(a_{m+1}, a_{m+2}, ..., a_{m+n}) = 0$. However, we have that $q \in P_K(m)$ so that $a_{m+n} = 0$. Consequently $r \in P_K(m+n)$ as asserted.

PROPOSITION 2. *Let* A *be a k-algebra and* I *an ideal of* A. *Then the K-radical* $\sqrt[K]{I}$ *of* I *is an ideal of* A *(possibly* A *itself) which contains the radical of* I.

Proof. Since $P_K(1) = \{1, y_1, y_1^2, ...\}$ it is clear that the set $\sqrt[K]{I}$ contains $\sqrt{I}$.

Let f and g be elements in $\sqrt[K]{I}$. Then by the definition of the K-radical there are positive integers m and n, polynomials $p \in P_K(m)$ and $q \in P_K(n)$ and elements $f_1, f_2, ..., f_{m-1}$ and $g_1, g_2, ..., g_{n-1}$ of A such that

$$p(f_1, f_2, ..., f_{m-1}) \in I \quad \text{and}$$
$$q(g_1, g_2, ..., g_{n-1}, g) \in I$$

Let h be an element of A and let d be the degree of p. Then we have that

$$p(hf_1, hf_2, ..., hf_{m-1}, hf) = h^d p(f_1, f_2, ..., f_{m-1}, f) \in I .$$

Consequently it follows from the definition of K-radicals that $h \cdot f \in \sqrt[K]{I}$.

In order to prove the Proposition it remains to prove that $(f+g) \in \sqrt[K]{I}$.

To this end we rewrite the polynomial $q(y_{m+1}, y_{m+2}, \ldots, y_{m+n})$ in the following form

$$q(y_{m+1}, y_{m+2}, \ldots, y_{m+n-1}, y_{m+n} - y_m) + y_m s(y_m, y_{m+1}, \ldots, y_{m+n}),$$

where s is a homogeneous polynomial of $S(m+n)$ of degree one less than the degree of q.

By Lemma 1 we have that

$$r = r(y_1, y_2, \ldots, y_{m+n}) = p(y_1 \cdot s, y_2 \cdot s, \ldots, y_{m-1} \cdot s, q(y_{m+1}, y_{m+2}, \ldots y_{m+n}))$$

is in $P_K(m+n)$. However, from the above form of $q(y_{m+1}, y_{m+2}, \ldots y_{m+n})$, it follows that r can be rewritten as

$$p(y_q \cdot s, y_2 \cdot s, \ldots, y_{m-1} \cdot s, y_m \cdot s) + q(y_{m+1}, y_{m+2}, \ldots, y_{m+n-1}, y_{m+n} - y_m) \\ \cdot t(y_1, y_2, \ldots, y_{m+n}),$$

where $t(y_1, y_2, \ldots, y_{m+n})$ is a homogeneous polynomial in $S(m+n)$ of degree equal to $(d-1) \cdot \deg(q)$.

From the latter form of r we obtain that, if we write $l = s(f, g_1, g_2, \ldots, g_n)$, then $h = r(f_1, f_2, \ldots, f_{m-1}, f, g_1, g_2, \ldots, g_{n-1}, f+g)$ can be written as

$$l^d p(f_1, f_2, \ldots, f_{m-1}, f) \\ + q(g_1, g_2, \ldots, g_{n-1}, g) \cdot t(f_1, f_2, \ldots, f_{m-1}, f, g_1, g_2, \ldots, g_{n-1}, f+g).$$

The latter element is in I and since $r \in P_K(m+n)$ it follows from the definition of the K-radical that $f + g \in \sqrt[K]{I}$, as we wanted to prove.

We shall call an ideal I of a k-algebra A, K-radical, if $\sqrt[K]{I} = I$.

The next result shows that $\sqrt[K]{I}$ is always K-radical.

PROPOSITION 3. *Let A be a k-algebra and I an ideal of A. Moreover, let $J = \sqrt[K]{I}$. Then we have that $\sqrt[K]{J} = J$.*

Proof. Let f be in $\sqrt[K]{J}$. We shall prove that $f \in J$. By definition of the K-radical, there is a positive integer n, a polynomial $q \in P_K(n)$ and elements $f_1, f_2, \ldots f_{n-1}$ in A such that

$$g = q(f_1, f_2, \ldots, f_{n-1}, f) \in J.$$

Now, since $g \in \sqrt[K]{I}$, there is furthermore a positive integer n, a polynomial $p \in P_K(m)$ and elements $g_1, g_2, \ldots g_{m-1}$ in A such that

$$p(g_1, g_2, ..., g_{m-1}, g) \in I .$$

Let d be the degree of q. Then by Lemma 1 with $s = y_n^{d-1}$ we have that

$$\begin{aligned} &r(y_1, y_2, ..., y_{m+n}) \\ &= p(y_1 \cdot y_m^{d-1}, y_2 \cdot y_m^{d-1}, ..., y_{m-1} \cdot y_m^{d-1}, q(y_{m+1}, y_{m+2}, ..., y_n)) \end{aligned}$$

is in $P_K(m+n)$. However, we have that the element

$$\begin{aligned} &r(g_1, g_2, ..., g_{m-1}, 1, f_1, f_2, ..., f_{n-1}, f) \\ &= p(g_1, g_2, ..., g_{m-1}, q(f_1, f_2, ..., f_{n-1}, f)) = p(g_1, g_2, ..., g_{m-1}, g) \end{aligned}$$

is in I. Hence f is in $\sqrt[K]{I} = J$ as we wanted to prove.

As in the traditional case, one of the two assertions of the Hilbert K-Nullstellensatz and of its weak form is easy.

PROPOSITION 4. *Let* I *be an ideal of* R *and* $J = \sqrt[K]{I}$. *Then the following assertions hold:*

(i) $Z_K(J) = Z_K(I)$,

(ii) $J \subseteqq \{f \in R \mid Z_K(f) \supseteqq Z_K(I)\}$,

(iii) if $Z_K(I) \neq \emptyset$ then $J \neq R$.

Proof. Since J contains I we have the inclusion $Z_K(J) \subseteqq Z_K(I)$. To prove the opposite inclusion as well as assertion (ii) it suffices to prove that for each point $a = (a_1, a_2, ..., a_r) \in \mathbf{A}_K^r$ of $Z_K(I)$, we have that $f(a) = 0$ for all $f \in J$. However if $f \in T$ then there exists a polynomial p in $P_K(m)$ for some natural number m and elements $f_1, f_2, ..., f_{m-1}$ in R such that

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

Since a is in $Z_K(I)$ we obtain that

$$p(f_1(a), f_2(a), ..., f_{m-1}(a), f(a)) = 0 .$$

However, we have that $p \in P_K(m)$ so that $f(a) = 0$.

The last assertion of the Proposition follows from assertion (ii).

The crucial tool in our proof of the Hilbert K-Nullstellensatz is the following result, which certainly is well known, but for which we have no reference.

PROPOSITION 5. *Assume that* K *is not algebraically closed. Then, for each positive integer* m, *there is a homogeneous polynomial* $p \in k[y_1, y_2, ..., y_m]$ *with only the trivial zero in* $\mathbf{A}_K^m$. *That is,* $Z_K(p) = (0, 0, ..., 0)$.

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 $\beta = \beta_1, \beta_2, ..., \beta_n$ of β are in L and clearly $L = k(\beta_i)$ for $i = 1, 2, ..., n$. We have that L is not contained in K because $\alpha \notin K$. Hence, none of the roots $\beta_1, \beta_2, ..., \beta_n$ 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 $p(y_1, y_2, ..., y_m)$ 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 $r(y_1, y_2, ..., y_{m+1}) = q(p(y_1, y_2, ..., y_m), y_{m+1}^d)$ is a homogeneous polynomial with only the trivial zero in $\mathbf{A}_K^{m+1}$. Indeed, the homogeneity is clear, and if $(a_1, a_2, ..., a_{m+1}) \in \mathbf{A}_K^{m+1}$ is a zero of r, we must have that $p(a_1, a_2, ..., a_m) = 0$ and $a_{m+1} = 0$ since q has no non-trivial zeroes. Then we must have that $a_1 = a_2 = ... = a_m = 0$ 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

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

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 $k[x_1, x_2, \ldots, x_{r-1}]$ 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

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

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

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

On the other hand we obtain a relation

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

with b and b_i in S/Q for $i = 0, 1, \ldots, n$ 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

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

Hence, if $\alpha_1, \alpha_2, ..., \alpha_r$ are the classes of $x_1, x_2, ..., x_r$ in R/M we have that $(a(\alpha_1), a(\alpha_2), ..., a(\alpha_n)) \in Z_K(M) \subseteqq Z_K(I)$ 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 $f_1, f_2, ..., f_m$ are polynomials in R such that $p(f_1, f_2, ..., f_m) \in J$ 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.

In the case that k is an ordered field results similar to the Hilbert K-Nullstellensatz were proved by Dubois [2] and Risler [7]. To state their results we introduce the following notation:

Assume that k is an ordered field. Given an ideal I in R we let

$$I_D = \{f \in R \mid \text{there exists an integer } m, \text{ positive elements } a_1, a_2, ..., a_m \text{ of } k \text{ and rational functions } u_1, u_2, ..., u_m \text{ in } k(x_1, x_2, ..., x_r) \text{ such that } f^n(1 + \sum_{i=1}^{m} a_i u_i^2) \in I\} \text{ and}$$

$$I_R = \{f \in R \mid \text{there are positive elements } a_2, a_3, ..., a_m \text{ of } k \text{ and elements } f_2, f_3, ..., f_m \text{ of } R \text{ such that } f^2 + \sum_{i=1}^{m} a_i f_i^2 \in I\}.$$

It is fairly easy to see that I_R and I_D are radical ideals and clearly $I_R \subseteqq I_D$. The Hilbert Nullstellensatz of Risler [7] states that, if $k = K = R_k$ where we denote by R_k the real closure of k, then

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

and the Nullstellensatz of Dubois [2] that, if $K = R_k$, then

$$I_D = \{f \in R \mid Z_K(f) \supseteqq Z_K(I)\}.$$

In particular it follows from these results that in the above cases I_R or I_D are equal to the K-radical $\sqrt[K]{I}$. From our point of view it is more satisfactory to proceed in the opposite direction and first prove directly, in the above cases, that the ideals I_D or I_R are equal to the K-radical and thus obtain the results of Dubois and Risler as a consequence of our K-Nullstellensatz. This can be done, however in order to prove that the various ideals are equal we need to use S. Lang's [6] version of Hilbert Nullstellensatz for real closed fields or Artin's solution of Hilbert's 17th problem (see [6], § 3 in particular Theorem 5 and Corollary 2 p. 279), so that this procedure is too close to the methods of Dubois and Risler to merit a separate presentation here.

§ 5. Two examples

In the introduction we associated to each ideal I of R a subset I_T of R such that $I \subseteq I_T \subseteq \sqrt[K]{I}$. For the two pairs of fields $k = K = \mathbf{Z}/2\mathbf{Z} = GF(2)$ and $k = K = \mathbf{Q}$ we give, in this section, examples of ideals I such that we have a strict inclusion $I_T \subset \sqrt[K]{I}$.

Example 1. Let k be the field with two elements and let $K = k$. Consider the ideal $I = (x_1) \subsetneqq k[x_1, x_2] = R$. The following three assertions hold:

(i) We have that

$$Z_K(I) = \{(0,0), (0,1)\} \subsetneqq \mathbf{A}_K^2 \text{ and}$$
$$\{f \in R \mid f \text{ vanishes on } Z_K(I)\} = (x_1, x_2(x_2+1)).$$

(ii) $\sqrt[K]{I} = (x_1, x_2(x_2+1))$.

(iii) $I_T = (x_1) = I$.

In particular we have a strict inequality $I_T \subset \sqrt[K]{I}$.

Of the three assertions (i) is obvious and the second follows from (i) and the Hilbert K-Nullstellensatz. To prove assertion (iii) we let $p \in P_K^0(m)$ and $f_1, f_2, \ldots, f_m$ be elements in R such that $p(f_1, f_2, \ldots, f_m) \in I$. We shall prove that $f_i \in I$ for $i = 1, 2, \ldots, r$. Assume to the contrary that not all the f_i are in I. Then the polynomials $f_i(0, x_2)$ are not all identically zero. Let d be the non-negativ integer such that

$$f_i(0, x_2) = x_2^d g_i(x_2) \quad \text{for} \quad i = 1, 2, \ldots, m$$

and x_2 does not divide $g_j(x_2)$ for some index j. Since $p(f_1, f_2, \ldots, f_m) \in I$ we have that

$$p(f_1(0, x_2), f_2(0, x_2), \ldots, f_m(0, x_2)) = x_2^{de} p(g_1(x_2), g_2(x_2), \ldots, g_m(x_2))$$

is identically zero in $k[x_2]$, where e is the degree of p. Hence

$$p(g_1(x_2), g_2(x_2), \ldots, g_m(x_2))$$

is identically zero. In particular we have that $(g_1(0), g_2(0), \ldots g_m(0))$ is a zero of p in $\mathbf{A}_K^m$ with $g_j(0) \neq 0$. This contradicts the assumption that $p \in P_K^0(m)$.

Example 2. Let $k = K = \mathbf{Q}$ and let $R = k[x_1, x_2, x_3]$. Moreover, let

$$f(y_1, y_2, y_3) = y_1^3 + y_2^3 + 3y_3^3$$

and $I = (f(y_1, y_2, y_3))$ the ideal in R generated by f.

The following three assertions hold:

(i) We have that $Z_K(I) = \{(a, -a, 0) \mid a \in K\} \subseteq \mathbf{A}_K^3$ and

$$\{f \in R \mid f \text{ vanishes on } Z_K(I)\} = (x_1 + x_2, x_3).$$

(ii) $\sqrt[K]{I} = (x_1 + x_2, x_3)$.

(iii) The ideal I_T does not contain a (non-zero) linear form.

In particular we have a strict inequality $I_T \subset \sqrt[K]{I}$.

The first assertion of (i) is a well known result in number theory (see e.g. Hardy and Wright [3], Theorem 232 page 196) and the second assertion of (i) is an immediate consequence of the first. Assertion (ii) follows from (i) and the Hilbert K-Nullstellensatz.

To prove assertion (iii) we let $l = ax_1 + bx_2 + cx_3$ be a non-zero linear form and $p = p(y_1, y_2, ..., y_m) \in P_K^0(m)$ an element of degree d. Assume that there are polynomials $f_i = f_i(x_1, x_2, x_3)$ of R for $i = 1, 2, ..., m-1$ such that

$$p(f_1, f_2, ..., f_{m-1}, l) = f(x_1, x_2, x_3)\, g(x_1, x_2, x_3)$$

for some polynomial $g = g(x_1, x_2, x_3)$. Then the following six assertions hold:

(a) *The polynomials* $f_1, f_2, ..., f_{m-1}$ *have zero constant term.*

Indeed, specialize x_1, x_2, x_3 to 0, 0, 0 respectively. We obtain that

$$p(f_1(0,0,0), f_2(0,0,0), ..., f_{m-1}(0,0,0), 0) = f(0,0,0)\, g(0,0,0) = 0\,.$$

Hence the existence of a non-zero constant term would contradict the assumption that $p \in P_K^0(m)$.

Denote by $l_i = l_i(x_1, x_2, x_3)$ the linear term of f_i.

(b) *The homogenous polynomial* $p(l_1, l_2, ..., l_{m-1}, l)$ *is not (identically) zero and it is the lowest non-zero homogeneous term of*

$$p(f_1, f_2, ..., f_{m-1}, l)\,.$$

Indeed, if $p(l_1, l_2, ..., l_{m-1}, l)$ were zero, we can specialize (x_1, x_2, x_3) to a point (a_1, b_1, c_1) of K^3 which is not a zero of l. We then obtain $p(l_1(a_1, b_1, c_1), l_2(a_1, b_1, c_1), ..., l_{m-1}(a_1, b_1, c_1), l(a_1, b_1, c_1)) = 0$ which again contradicts the assumption that $p \in P_K^0(m)$. The second assertion of (b) follows from (a).

Denote by $h(x_1, x_2, x_3)$ the non-zero homogenous term of $g(x_1, x_2, x_3)$ which has lowest degree.

(c) *We have that* $h(x_1, x_2, x_3)$ *is of degree* $d-3$ *and that*

$$p(l_1, l_2, ..., l_{m-1}, l) = f(x_1, x_2, x_3)\, h(x_1, x_2, x_3)\,.$$

Indeed, since f is homogeneous of degree 3, assertion (c) follows from assertion (b).

We write $l_i = a_i x_1 + b_i x_2 + c_i x_3$ for $i = 1, 2, ..., m-1$.

(d) *We have that* $a = b$ *and that* $a_i = b_i$ *for* $i = 1, 2, ..., m-1$.

Indeed, specialize x_1, x_2, x_3 to $1, -1, 0$ respectively. From assertion (c) we obtain that

$$p(a_1-b_1, a_2-b_2, ..., a_{m-1}-b_{m-1}, a-b) = f(1, -1, 0)\, h(1, -1, 0) = 0 .$$

Hence assertion (d) follows from the assumption that $p \in P_K^0(m)$.

(e) *We have that* $a = b = a_i = b_i = 0$ *for* $i = 1, 2, ..., m-1$.

Indeed, specializing x_1, x_2, x_3 to $x_1, x_2, 0$ respectively, we obtain from the equation of assertion (c) and from assertion (d) that

$$p\big(a_1(x_1+x_2), a_2(x_1+x_2), ..., a_{m-1}(x_1+x_2), a(x_1+x_2)\big)$$
$$= (x_1^3+x_2^3)\, h(x_1, x_2, 0) .$$

The left hand side of the latter equation is equal to

$$(x_1+x_2)^d p(a_1, a_2, ..., a_{m-1}, a)$$

which is not divisible by $x_1^3 + x_2^3$ unless $p(a_1, a_2, ..., a_{m-1}, a) = 0$. Assertion (e) therefore follows from assertion (d) and the assumption that $p \in P_K^0(m)$.

(f) *We have that* $c \neq 0$ *and* $p(c_1, c_2, ..., c_{m-1}, c) = 0$.

Indeed, since $l = ax_1 + bx_2 + cx_3$ is non-zero it follows from assertion (e) that $c \neq 0$. Moreover it follows from assertion (e) that the equation of assertion (c) can be written as

$$p(c_1x_3, c_2x_3, ..., c_{m-1}x_3, cx_3) = f(x_1, x_2, x_3)\, h(x_1, x_2, x_3) .$$

The left hand side of the latter equation is equal to $x_3^d p(c_1, c_2, ..., c_{m-1}, c)$ which is not divisible by $f(x_1, x_2, x_3)$ unless $p(c_1, c_2, ..., c_{m-1}, c) = 0$.

We have thus proved that, if we assume that polynomials $f_1, f_2, ..., f_{m-1}$ such that $p(f_1, f_2, ..., f_{m-1}, l) \in I$ exist, we arrive at the contradiction (f) to the assumption that $p \in P_K^0(m)$. Hence we must have that $l \notin I_T$ as asserted.

REFERENCES

[1] ADKINS, W. A., P. GIANNI and A. TOGNOLI, A. Nullstellensatz for an algebraically non-closed field. *Bollettino U.M.I. 15* (1978), 338-343.

[2] DUBOIS, D. W. A Nullstellensatz for ordered fields. *Ark. Mat. 8* (1969), 111-114.

[3] HARDY, G. H. and E. M. WRIGHT. *An introduction to the Theory of numbers.* Clarendon Press, Oxford 1954 (third edition).

[4] LAKSOV, D. Generalized radicals of ideals in algebras. *Rend. del Sem. Mat. Università e Politecnico Torino.* Fascicolo speciale (1986), 77-89.

[5] —— Radicals defined by universal polynomials. *TRITA-MAT 27* (1986). (Preprint KTH-Stockholm).

[6] LANG, S. *Algebra.* Addison-Wesley 1965.

[7] RISLER, J. J. Une caractérisation des idéaux des variétés algébriques réelles. *C. R. Acad. Sci. Paris Sér. A-B, 271* (1970), 1171-1173.

(Reçu le 22 janvier 1986)

Dan Laksov

Department of Mathematics
Royal Institute of Technology
S-100 44 Stockholm (Sweden)