Zeitschrift: L'Enseignement Mathématique

Herausgeber: Commission Internationale de l'Enseignement Mathématique

Band: 33 (1987)

Heft: 1-2: L'ENSEIGNEMENT MATHÉMATIQUE

Artikel: RADICALS AND HILBERT NULLSTELLENSATZ FOR NOT NECESSARILY ALGEBRAICALLY CLOSED FIELDS

Autor: Laksov, Dan

Kapitel: §5. TWO EXAMPLES

DOI: https://doi.org/10.5169/seals-87902

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

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

$I_R = \{f \in R \mid$ there are positive elements $a_2, a_3, \ldots, a_m$ of k and elements $f_2, f_3, \ldots, f_m$ of R 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.