ARKIV FÖR MATEMATIK Band 8 nr 13

1.69 06 2 Communicated 9 April 1969 by Einar Hille

A nullstellensatz for ordered fields

By D. W. Dubois

For an ordered field k, a *realzero* of an ideal P in the polynomial ring $k[X]=k[X_1, \ldots, X_n]$ in n variables is a zero in $\bar{k}^{(n)}$, where $\bar{k}$ is the realclosure of k, the *realvariety* $\mathcal{V}_R(P)$ is the set of all realzeros of P, and, as usual, $\mathcal{I}(G)$, for any subset G of $\bar{k}^{(n)}$ is the ideal of all members of $k[X]$ that vanish all over G. Our nullstellensatz asserts:

$$\mathcal{I}\mathcal{V}_R(P)=\sqrt[R]{P}=\textit{realradical of } P,$$

where $\sqrt[R]{P}$ is the set of all $f(X)$ such that for some exponent m, some *rational* functions $u_i(X)$ in $k(X)$, and positive $p_i \in k$

$$f(X)^m(1+\Sigma\, p_i u_i(X)^2) \in P.$$

The proof, which uses Artin's solution of Hilbert's 17th problem, and which grew out of an attempt to find an easier solution to the problem, is straight-forward, inspired in large part by Lang's elegant formulation of various extension theorems, especially Theorem 5, p. 278 [2]. We give a new proof of this theorem, and a generalization to finitely generated formally real rings over k (Theorem 1).

Throughout, k will be an ordered field. For any ordered field K, $\bar{K}$ is its real closure.

A simple consequence of Artin's work (see Theorem 13 and Lemma 1 of Jacobson, Chapter VI [1]) is:

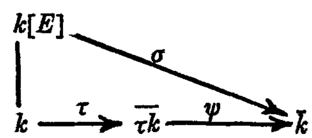
Artin's Theorem. *Let k be an ordered field, let $K=k(T)\equiv k(T_1, \ldots, T_n)$ be a pure transcendental ordered extension of k, with T_i algebraically independent. Let $f(Y) \in k[T][Y]$ have a root in $\bar{K}$, let $u_1, \ldots, u_m$ be a finite set of nonzero elements of $k[T]$. There exists a homomorphism σ over k from $k[T]$ to $\bar{k}$ satisfying*

(i) $\sigma(u_i) \neq 0$, $1 \leqslant i \leqslant m$.

(ii) *$f^\sigma(Y)$ has a root in $\bar{k}$.*

Lang's Theorem (Lang, Theorem 5, p. 278 [2]). *Let k be an ordered field, let $k \xrightarrow{\tau} R$ be an order-embedding of k into a realclosed field R. Let K be a field containing k and admitting an order extending the order of k. Then for every finite subset E of K there exists a homomorphism ψ: $k[E] \to R$ extending τ.*

Proof. Suppose the theorem is known for the case where τ is the inclusion map $k \subset \bar{k}$. For general τ, the algebraic closure $\overline{\tau k}$ in R is a real closure of τk and also of k, so by the uniqueness theorem for real closures there exists ψ: $\overline{\tau k} \cong \bar{k}$ such that ψ is order preserving and $\psi\tau$ is the inclusion $k \subset \bar{k}$. By supposition there exists σ: $k[E] \to \bar{k}$. Then $\psi^{-1}\sigma$: $k[E] \to R$ extends τ.



Hence we consider the case of τ equal to the inclusion of k in $\bar{k}$. It is obviously enough to prove the claim under the hypothesis that $K|k$ is finitely generated. If K is a pure transcendental extension of k then our claim is Artin's Theorem. Suppose $K = k(T)(u)$, where $k(T) = k(T_1, ..., T_n)$, $T_1, ..., T_n$ is a transcendence base and u is algebraic over $k(T)$. Let u be taken as integral over $k[T]$ with monic minimal polynomial $m(X)$ in $k[T][X]$. Let E be a finite subset of K and let D consist of all denominators of coefficients of u^i appearing in expressions for members of E as polynomials in u of degree less than the degree of $m(X)$. Let K be given a fixed order extending the order of k. Then $m(X)$ has a root in the real closure of $k(T)$. By Artin's Theorem there exists a homomorphism σ over k from $k[T]$ to $\bar{k}$ such that

(i) If $d \in D$ then $\sigma(d) \neq 0$.
(ii) $m^{\sigma}(X)$ has a root, say z, in $\bar{k}$.

Suppose $f(x) \in k[T][X]$ vanishes at u. Then $f(X) = m(X)q(X)$, $m(X)$ is primitive, so by Gauss's Theorem, $q(X) \in k[T][X]$. Hence $f(X)$ belongs to the kernel of the homomorphism

$$g(X) \to g^{\sigma}(z), \quad k[T][X] \to \bar{k}.$$

Induced is a homomorphism over k

$$\psi : f(u) \to f^{\sigma}(z), \quad k[T][u] \to \bar{k}.$$

For d in $D \subset k[T]$, $\psi(d) = \sigma(d) \neq 0$. Thus ψ extends to $\psi' : k[T][E] \to \bar{k}$.

Lang's Corollary [2]. *If $u_1 < ... < u_m$ are arbitrary members of $k[E]$ then the ψ of the theorem can be chosen so that $\psi(u_1) < ... < \psi(u_m)$.*

Definitions. Let k be an ordered field, let A be a unitary commutative ring containing k.

$$S(A) \equiv S(A \mid k) = \{1 + \Sigma\, p_i a_i^2;\ a_i \in A,\ 0 < p_i \in k\}.$$

"$A \mid k$ is *formally real*", "*A is formally real over k*" mean that if $\Sigma\, p_i a_i^2 = 0$, $0 < p_i \in k$, $a_i \in A$, then $a_i = 0$ for all i.

Examples of formally real rings over k: If $K \mid k$ is a field extension then $K \mid k$ is formally real if and only if the order of k extends to K. If $A \mid k$ is formally real so is $A[X] \mid k$, where $A[X] = A[X_1, ..., X_n]$ is the polynomial ring.

Proposition 1. *If $A \mid k$ is formally real then $S(A \mid k)$ is a multiplicative set containing no zerodivisors. The total ring of fractions is formally real over k. Thus we have*

$$k \subset A \subset S^{-1}A \subset A_1 = \textit{total ring of fractions},$$

each formally real over k.

The proof is routine and is omitted.

Definition. Let A be formally real over k, let A_1 be the total ring of fractions of A. We set

$$S_1(A) \equiv S_1(A \mid k) = A \cap S(A_1).$$

Clearly $S_1(A)$ *is a multiplicative subset of* A *containing no zero divisors, since* A_1 *is also formally real over* k.

Lemma. *Let* $A \mid k$ *be formally real, let* P *be an ideal of* A *which is maximally disjoint from* $S_1(A)$. *Then* A/P *is a formally real integral domain over* k, *and the order of* k *extends to the field of quotients of* A/P.

Proof. Since $S_1(A)$ is multiplicative, P is prime and A/P is an integral domain. Let P be any ideal disjoint from $S_1(A)$ and suppose A/P is not formally real over k. Then there exist a_i in A, $p_i>0$ in k, a_1 not in P, such that

$$a=\sum_{i=1}^{n} p_i a_i^2 \text{ belongs to } P. \tag{1}$$

Now we shall show that $P+a_1A$ is also disjoint from $S_1(A)$ from which follows the Lemma. Suppose $P+a_1A$ meets $S_1(A)$. Then there exist u in P, d in A, b_i in A_1, $q_i>0$ in k, such that

$$u+dp_1a_1 = 1+\Sigma\, q_i b_i^2 \in S_1(A).$$

Squaring both sides gives ($r_i>0$ in k, c_i in A_1):

$$u(u+2dp_1a_1) = 1+\sum r_i c_i^2 + d^2 p_1\left(-a+\sum_{i=2}^{n} p_i a_i^2\right), \tag{2}$$

where we have substituted from (1) for $p_1a_1^2$. Now a belongs to P, so after transposing d^2p_1a, we have a member of P on the left side of (2) and a member of $S_1(A)$ on the right side, contradicting our hypothesis that P is disjoint from $S_1(A)$.

Theorem 1. *If* $A \mid k$ *is a finitely generated formally real ring then any order-embedding* ψ *of* k *into a real closed field* F *extends to a homomorphism of* $A \mid k$ *into* F.

Proof. Let P be an ideal of A maximally disjoint from $S_1(A)$. Write $A=k[x]=k[x_1, ..., x_n]$ let σ be the canonical map $A\rightarrow A/P$:

$$k[x]\xrightarrow{\sigma} k[\sigma x_1, ..., \sigma x_n] = k[\sigma x].$$

Since A/P is finitely generated, the Lemma allows application of Lang's Theorem to yield a map $\bar{\psi}: k[\sigma x]\rightarrow F$ extending ψ. Then $\bar{\psi}\sigma$ also extends ψ.

Corollary. *Let* A *be formally real over* k, *let* $u_1, ..., u_n$ *be elements of* A *which are not zero-divisors. Then there exists a homomorphism* $\psi: k[u_1, ..., u_n]\rightarrow \bar{k}$ *over* k *with* $\psi(u_i)\neq 0$, $i=1, ..., n$.

Proof. Apply the theorem to the finitely generated formally real subring $k[u_1, ..., u_n, u_1^{-1}, ..., u_n^{-1}] \mid k$ of the total fraction ring of A.

Let $A=k[X]=k[X_1, ..., X_n]$ be the ring of all polynomials in n variables over the ordered field k. Let P be an ideal of A. If $f(X)$ is a polynomial and if there exist $m>0$, $0<p_i\in k$, and polynomials $g_i(X)$, $h_i(X)$ such that $f(X)^m(1+\Sigma p_i g_i(X)^2 h_i(X)^{-2})\in P$, then $f(X)$ clearly vanishes at every *realzero* of the ideal P. Thus

$$\sqrt[R]{P} \subset \mathscr{I}\mathscr{V}_R(P).$$

It is easy to verify that $P \cap S_1(A) = \phi \Leftrightarrow \sqrt[R]{P} \neq A.$

Nullstellensatz. *For an ordered field k, $\mathscr{I}\mathscr{V}_R(P) = \sqrt[R]{P}$ for every P in $k[X_1, ..., X_n]$.*

Proof. Following the argument of Zariski-Samuel vol. II, p. 164 [3], we first show: *If $\sqrt[R]{P}$ is a proper subset of $k[X]$ then $\mathscr{V}_R(P) \neq \phi$.* If $P \subset M$, where M is an ideal, then obviously $\mathscr{V}_R(M) \subset \mathscr{V}_R(P)$, so it is quite enough to verify the claim when P is maximally disjoint from S_1. According to the Lemma, $k[X]/P$ is a finitely generated formally real integral domain which admits a homomorphism ψ over k (by Lang's Theorem) into $\bar{k}$. Denoting the coset of X_i in $k[X]/P$ by x_i, the point $(\psi(x_1), ..., \psi(x_n))$ is a member of $\mathscr{V}_R(P)$, since if $f(X)$ belongs to P then

$$0 = \psi(f(X) + P) = f(\psi(x_1), ..., \psi(x_n)).$$

This proves the italicized assertion.

Now to prove the theorem, let P be any ideal, say $P = (f_1(X), ..., f_q(X))$, and suppose $f(X)$ belongs to $\mathscr{I}\mathscr{V}_R(P)$. The ideal in $k[X][T]$ generated by $\{f_1(X), ..., f_q(X), 1 - Tf(X)\}$ has no realzeros. By the italicized claim there exist polynomials $h(X, T)$, $h_i(X, T)$, and rational functions $g_i(X, T)$ such that

$$1 + \Sigma\, p_i g_i(X, T)^2 = h(X, T)(1 - Tf(X)) + \Sigma\, h_i(X, T) f_i(X),\ 0 < p_i \in k). \quad (1)$$

Suppose $f(X)^{-1}$ can be substituted for T on the left side. The right side has only powers of $f(X)$ in the denominators so for some $m > 0$, we get an expression, with polynomials for $u_i(X)$,

$$f(X)^m(1 + \Sigma\, p_i g_i(X, f(X)^{-1})^2) = \Sigma\, u_i(X) f_i(X),$$

and the right side belongs to P. Hence $f(X) \in \sqrt[R]{P}$. The proof will be completed by showing that $f(X)^{-1}$ can be substituted for T on the left side of (1). Observe that

$$k(X, T) = k(X_1, .., X_n, 1 - Tf(X)).$$

Set $Y = 1 - Tf(X)$. Extend the order of k to $K(X, T)$ so that $1 - Tf(X)$ is infinitesimal relative to $k(X)$. Suppose $f(X)^{-1}$ cannot be substituted for T in (1). Then for at least one $g_i(X)$, the denominator is divisible by $1 - Tf(X) = Y$, hence the left side is infinitely large relative to $k(X_1, ..., X_n)$ while the right side is not, since it is a polynomial in $T = f(X)^{-1}(1 - Y)$ (coefficients in $k(X)$) which has the same order of magnitude as $f(X)^{-1} \in k(X)$. The contradiction completes the proof.

Department of Mathematics and Statistics, University of New Mexico, Albuquerque, NeM. 87106, U.S.A.

REFERENCES

1. JACOBSON, N., Lectures in Abstract Algebra, vol. III, Van Nostrand, 1964.
2. LANG, S., Algebra. Addison-Wesley, 1965.
3. ZARISKI, O., and SAMUEL, P., Commutative Algebra, vol. II. Van Nostrand, 1960.

Tryckt den 18 december 1969

Uppsala 1969. Almqvist & Wiksells Boktryckeri AB