Pacific Journal of Mathematics

A NULLSTELLENSATZ FOR NASH RINGS

GUSTAVE ADAM EFROYMSON

Vol. 54, No. 1 May 1974

PACIFIC JOURNAL OF MATHEMATICS
Vol. 54, No. 1, 1974

A NULLSTELLENSATZ FOR NASH RINGS

GUSTAVE A. EFROYMSON

Let D be a domain in R^n defined by a finite number of strict polynomial inequalities. Then the Nash ring A_D is the ring of real valued algebraic analytic functions defined on D. In this paper, it is shown that A_D is Noetherian and has a nullstellensatz. For $\mathscr{P}$ a prime ideal of A_D, $A_D/\mathscr{P}$ is said to be rank one orderable if its quotient field can be ordered over R so that it has essentially one infinitesimal. Then $A_D/\mathscr{P}$ is rank one orderable if and only if $\mathscr{P}$ equals the set of functions in A_D which vanish on the zero set of $\mathscr{P}$ in D.

DEFINITION 0.1. Let R denote the real numbers. Let D be a domain in R^n, defined by a finite number of polynomial inequalities $p_i(x) > 0$. A function $f: D \rightarrow R$ is said to be algebraic analytic if there exists a non-trivial polynomial $p_f(z, x_1, \cdots, x_n)$ in $R[z, x_1, \cdots, x_n]$ so that $p_f(f(x), x) = 0$ for all x in D, and if f is analytic (expandable in convergent power series) at every point of D.

DEFINITION 0.2. The ring of all such algebraic analytic functions $f: D \rightarrow R$ is called the Nash ring A_D; see [7] for this notation.

DEFINITION 0.3. (1) An ideal J of A_D is real if $\sum_{i=1}^{m} \lambda_i^2 \in J$ implies all $\lambda_i \in J$.

(2) For $J \subset A_D$, $V_R(J) = \{a \in R^n \mid f(a) = 0 \text{ for all } f \text{ in } J\}$.

(3) For $S \subset D$, $I(S) = \{f \in A_D \mid f(s) = 0 \text{ for all } s \text{ in } S\}$.

In § 1 and § 2 we develop some of the preliminaries for the study of the Nash ring. Most of § 1 comes form Cohen's paper [3]. In § 2 we prove the finiteness of the number of components of an algebraic set using Cohen's theory. In § 3 it is shown that A_D is Noetherian. Mike Artin made several valuable suggestions which were very helpful in proving this theorem.

Finally in § 4 we get to the nullstellensatz. Originally it was intended to prove the following conjecture.

CONJECTURE 0.4.[1] An ideal $J \subset A_D$ is real if and only if $I(V_R(J)) = J$.

Instead of this we are only able to show that: If $\mathscr{P} \subset A_D$ is prime, then $A_D/\mathscr{P}$ is rank one orderable (Definition 4.2) if and only if $I(V_R(\mathscr{P})) = \mathscr{P}$. This is sufficient to prove the conjecture in the case $D \subset R^2$. This is because the only nontrivial case is for $\mathscr{P}$ a prime of dimension 1 in which case $A_D/\mathscr{P}$ real implies $A_D/\mathscr{P}$ rank one orderable.

[1] Added in proof, this conjecture is now a theorem proved by T. Mostowski, preprint 1974.

1. Cohen's effective functions. In his paper, [3], Paul Cohen introduces the concept of an effective function. Since this concept is very useful here and is used in [3] to prove the Tarski principle, which we also find very useful, we will reproduce with some slight modifications the discussion in [3]. The main change here is to drop the term "primitive recursive" which is, I believe, not necessary for our needs.

DEFINITION 1.1. Let k be a field. A polynomial relation $A(x_1, \cdots, x_n)$ is a statement involving a finite number of polynomials in $k[x_1, \cdots, x_n]$ plus the terms: and, or, not, equals, greater than, and also parentheses.

DEFINITION 1.2. Let k be a real closed field. A function f defined on a subset D of k^n is *effective* if for every polynomial relation $A(x, t_1, \cdots, t_s)$, there exists a polynomial relation $B(x_1, \cdots, x_n, t_1, \cdots, t_s)$ so that $A(f(x_1, \cdots, x_n), t_1, \cdots, t_s)$ if and only if $B(x_1, \cdots, x_n, t_1, \cdots, t_s)$.

DEFINITION 1.3. Let $\operatorname{sgn} x = \begin{cases} 0 \text{ if } x = 0 \\ 1 \text{ if } x > 0. \\ -1 \text{ if } x < 0 \end{cases}$

LEMMA 1.4. *The function f is effective if and only if there exists for each positite integer d a polynomial relation $A_d(c_0, \cdots, c_d, x_1, \cdots, x_n, \lambda)$ so that $A_d(c, x, \lambda)$ if and only if*

$$\lambda = \operatorname{sgn}(c_0 f(x)^d + \cdots + c_d) .$$

Proof. All polynomial relations can be constructed from inequalities $p(x) > 0$.

DEFINITION 1.5. Let $p(x) = a_0 x^m + \cdots + a_m$ be a polynomial. By a *graph* for $p(x)$ we mean a k-tuple $t_1 < t_2 < \cdots < t_k$ so that in each interval $(-\infty, t_1), (t_1, t_2), \cdots, (t_k, \infty)$, $p(x)$ is monotonic. By the *data* for the graph we mean $\operatorname{sgn}(a_i)$, all i; $\langle t_1, \cdots, t_n \rangle$, and, $\operatorname{sgn} p(t_i)$ all i.

It is clear that from the data for its graph we can determine in which (t_{i-1}, t_i) the polynomial has roots.

THEOREM A_m. *There are effective functions of $a_0, \cdots, a_m$ which give the data for the graph of $p(x) = a_0 x^m + \cdots + a_m$. Namely, we have effective functions: $t_i(a)$, $\operatorname{sgn}(p(t_i(a))$ and of course $\operatorname{sgn}(a_i)$ so that $t_1(a) < \cdots < t_{m-1}(a)$ forms a graph for $p(x)$.*

THEOREM B_m. *Let $p(x) = a_0 x^m + \cdots + a_m$. There are $m + 1$ effective functions: $k(a)$ and $\xi_1(a) < \xi_2(a) < \cdots < \xi_m(a)$* (possibly not everywhere defined) *so that* $\xi_1(a), \cdots, \xi_{k(a)}(a)$ *are the roots of* $p(x)$.

Proof. The proof is by induction. The theorems are trivial for $m = 0$. We now assume that we have proven both A_r and B_r for all integers $r < m$. First we prove A_m. The polynomial $p'(x)$ has lower degree r than m and so by the corresponding B_r, its roots are effective functions of the coefficients of $p'(x)$ and the coefficients of $p(x)$.

Next we prove B_m. First choose a graph $t_1(a) < \cdots < t_{m-1}(a)$ for $p(x)$ using A_m. From the data we can determine the number of roots $k(a)$ effectively. We have to show that roots are effective. In each interval $(-\infty, t_1), \cdots, (t_i, t_{i+1}), \cdots, (t_{m-1}, \infty)$, there is at most one root of $p(x)$. Some of the t_i could be roots, but since we know sgn t_i, this is no problem. Moreover, we can tell from (sgn t_i, sgn t_{i+1}) whether or not $p(x)$ has a root in (t_i, t_{i+1}). Suppose ξ is such a root. Then, by Lemma 1.4, we have to show that if $q(x) = c_0x^s + \cdots + c_s$ is another polynomial, sgn $q(\xi)$ is an effective function of the c_i's and a_i's. First divide $q(x)$ by $p(x)$ and if $r(x)$ is the remainder we can replace $q(x)$ by $r(x)$ since the coefficients of $r(x)$ are effective functions of the c_i's and a_i's, and $q(\xi) = p(\xi)b(\xi) + r(\xi) = r(\xi)$. So we can assume $s < m$. By induction, we know the roots $u_1 < \cdots < u_s$ of $q(x)$ effectively in terms of the c_i's. Thus sgn $(u_i - t_j)$ is effective for all i and j, meaning that we know effectively which of the u_j are between t_i and t_{i+1}. By checking sgn $(p(u_j))$ for all j, we can determine effectively where ξ is relative to the u_j's. Then from the data for $q(x)$ we know sgn $q(\xi)$ also.

THEOREM 1.6. (Tarski and [3]). *Let k be a real closed field and let $A(x_1, \cdots, x_n)$ be a polynomial relation in $k[x_1, \cdots, x_n]$ with $n > 1$. Then there exists a polynomial relation $B(x_2, \cdots, x_n)$ so that $\{\exists x_1 \in k$ so that $A(x_1, \cdots, x_n)$ if and only if $B(x_2, \cdots, x_n)\}$.*

Proof. Regard the polynomials $p_1(x), \cdots, p_s(x)$ which appear in $A(x_1, \cdots, x_n)$ as polynomials in x_1 with their coefficients in $k[x_2, \cdots, x_n]$. Then one notes that the truth of $\exists x_1 A(x_1, \cdots, x_n)$ depends only on the relative positions of the roots of the $p_i(x)$ and the sign of the $p_i(x)$ in between these roots. By Theorems A_m and B_m this data is effectively determined from the coefficients of the p_i which are just polynomials in $k[x_2, \cdots, x_n]$.

THEOREM 1.7. *The function $f(x_1, \cdots, x_n)$ is effective if and only if there exists a polynomial relation $A_f(z, x_1, \cdots, x_n)$ so that $\{z = f(x_1, \cdots, x_n)$ if and only if $A_f(z, x_1, \cdots, x_n)\}$.*

Proof. If f is effective, consider the polynomial relation $t = z$. By the definition of effective function, there exists a polynomial relation $A_f(t, x_1, \cdots, x_n)$ so that $A_f(t, x_1, \cdots, x_n)$ if and only if $f(x_1, \cdots, x_n) = t$.

Now suppose $A_f(t, x_1, \cdots, x_n)$ exists so that $\{z = f(x_1, \cdots, x_n)$ iff $A_f(z, x_1, \cdots, x_n)\}$. Given any polynomial relation $A(z, t_1, \cdots, t_s)$, consider the relation (A_f and A). Then by Theorem 1.6, there exists $B(x_1, \cdots, x_n, t_1, \cdots, t_s)$ so that ($\exists z$: A_f and A) iff $B(x_1, \cdots, x_n, t_1, \cdots, t_s)$.

Theorem 1.7 is the only result in this section which does not appear in [3]. The reason for adding it is to give a possibly simpler description of the concept "effective function".

THEOREM 1.8. (Tarski's principle as proved by Cohen [3]). *Let k be a real field with only one ordering and let $A(x_1, \cdots, x_n)$ be a polynomial relation $k[x_1, \cdots, x_n]$. Then if Q_i is either $\forall$ or $\exists$, the statement* (∗) $\{Q_1x_1 \in L, Q_2x_2 \in L, \cdots, Q_nx_n \in L, A(x_1, \cdots, x_n)\}$ *is true for one real closed field $L \supset k$ iff it is true for every real closed $L \supset K$.*

Proof. First note that $\forall x$ is just $\sim \exists x \sim$. Then use induction and Theorem 1.6 to find a polynomial relation B involving only the coefficients of the polynomials in $A(x_1, \cdots, x_n)$ so that(*) iff B. Since any real closed field induces the unique ordering on k, B is true or false independent of L.

2. Algebraic analytic functions.

THEOREM 2.1. *Let $A(x_1, \cdots, x_n)$ be a polynomial relation. Let $D = \{(a_1, \cdots, a_n)$ in R^n such that $A(a_1, \cdots, a_n)\}$. Then each connected component of D is also defined by a polynomial relation. Moreover, there is a finite number of such components.*

Proof. We use induction on n. For $n = 1$, since D is a union of points and intervals, the result is obvious. For $n > 1$, $A(x_1, \cdots, x_n)$ involves a finite number of polynomials $p_i(x_1, \cdots, x_n)$ for $i = 1, \cdots, s$. Consider each p_i as a polynomial in x_n with coefficients in $k[x_1, \cdots, x_{n-1}]$. Then there exist functions $\varphi_{ij}(x_1, \cdots, x_{n-1})$ as in Theorem B_n giving the roots of $p_i(x)$. So our region D will be a union of intersections of sets of the form $\varphi_{ij}(x_1, \cdots, x_{n-1}) < x_n < \varphi_{i'j'}(x_1, \cdots, x_{n-1})$ (where $<$ could be $\leqq$), where $(x_1, \cdots, x_{n-1})$ is such that (1) both $\varphi_{ij}(x_1, \cdots, x_{n-1})$ and $\varphi_{i'j'}(x_1, \cdots, x_{n-1})$ are defined, (2) $(x_1, \cdots, x_{n-1}, \varphi_{ij}(x_1, \cdots, x_{n-1})) \in D$, (3) $(x_1, \cdots, x_{n-1}, \varphi_{i'j'}(x_1, \cdots, x_{n-1})) \in D$, and (4) $\varphi_{ij}(x_1, \cdots, x_{n-1}) < \varphi_{i'j'}(x_1, \cdots, x_{n-1})$.

It will be enough to show that the domain $E \subset D$ of $\varphi_{ij} = \varphi$

can be split up as a union of E_i where each E_i is connected and defined by a polynomial relation and φ is continuous on E_i. This is because we can further divide the E_i into connected components where other $\varphi_{i'j'}$ are defined, continuous and $> \varphi_{ij}$ by the same process. Let $p_\varphi(x_1, \cdots, x_{n-1}, z) =$ the irreducible polynomial for φ and let $g(x_1, \cdots, x_{n-1}) =$ the discriminant of p_φ with respect to z. By further subdividing and using Theorem B_m we can also assume $\varphi =$ i^{th} root of p_φ. So the subset of E where $g(x_1, \cdots, x_{n-1}) \neq 0$ can be written as $E_1 \cup \cdots \cup E_t$ where each E_i is connected and by our induction hypothesis each E_i can be defined by a polynomial relation. So fix E_1 say. Then let $\alpha_1(x_1, \cdots, x_{n-1}), \cdots, \alpha_d(x_1, \cdots, x_{n-1})$ be the roots (real and complex) of $p_\varphi(x_1, \cdots, x_{n-1}, z)$. The α_i are continuous functions and if some $\alpha_i(P)$ is not real, then there exists $j \neq i$ with $\alpha_i(P) = \overline{\alpha_j(P)}$. Since the α_i are continuous, no complex root can become real without p_φ getting a double root so this cannot happen in E_1 since $g \neq 0$ there. So let $\alpha_1, \alpha_2, \cdots, \alpha_u$ be the real roots of p_φ and suppose $P \in E_1$ that $\alpha_1(P) < \cdots < \alpha_u(P)$ and $\alpha_i(P) = \varphi(P)$. For Q near enough to P, $\alpha_1(Q) < \cdots < \alpha_u(Q)$ and so $\varphi(Q) = \alpha_i(Q)$ which shows that φ is continuous at P (since α_i is) and so φ is continuous on E_1. The other E_i are handled just the same way.

On the rest of E, we have $g(x_1, \cdots, x_{n-1}) = 0$ and so we can solve for $x_{n-1} = \psi(x_1, \cdots, x_{n-2})$, for possibly more than one ψ but only a finite number. Now let

$$h(x_1, \cdots, x_{n-2}) = \varphi(x_1, \cdots, x_{n-2}, \psi(x_1, \cdots, x_{n-2})) .$$

Then, by induction, we can split up the domain F of ψ into sets F_j which are connected and on which both φ and ψ are continuous. Then $E_{t+j} = \{(x_1, \cdots, x_{n-2}, \psi(x_1, \cdots, x_{n-2})) \mid (x_1, \cdots, x_{n-1}) \in F_j\}$ is connected and φ is continuous on E_{t+j}.

THEOREM 2.2. *Let D be a domain of R^n defined by a finite number of polynomial inequalities. Then, if $f: D \to R$ is algebraic analytic, f is effective.*

Proof. There is a polynomial $p_f(z, x_1, \cdots, x_n)$ so that $p_f(f(x), x) =$ 0 for all x in D. Let $g(x_1, \cdots, x_n)$ be the discriminant of p_f considered as a polynomial in z. Then in any connected subset of D where $g(x) \neq 0$, f will equal a fixed root of $p_f(z, x)$. So $f(x)$ is effective there. When $g(x) = 0$, we can solve for x_n in terms of the other variables and in polynomially defined regions D_i of R^{n-1}, x_n will be an algebraic analytic function of $x_1, \cdots, x_{n-1}$. There is a finite number s of the D_i so that $D = D_1 \cup \cdots \cup D_s$. On each D_i, f also will be an algebraic analytic function and so by induction on n we are done.

DEFINITION 2.3. Let D be the subset of R^n defined by $D = \{a \in R^n$ such that $p_1(a) > 0, \cdots, p_s(a) > 0\}$, where all $p_i(a)$ are in $R[x_1, \cdots, x_n]$. Let $f\colon D \to R$ be an algebraic analytic function. By Theorem 2.1, there is a polynomial relation $A_f(z, x_1, \cdots, x_n)$ in $R[z, x_1, \cdots, x_n]$ so that $A_f(z, x)$ iff $z = f(x)$. Finally let L be a real closed field containing R. Now $A_f(z, x)$ makes sense for $z, x_1, \cdots$ and x_n in L. If we let $D_L = \{a \in L^n$ such that all $p_i(a) > 0\}$, we can define $f_L\colon D_L \to L$ by setting $z = f_L(x_1, \cdots, x_n)$ iff $A_f(z, x_1, \cdots, x_n)$.

LEMMA 2.4. *For f_L defined as above, we have $(f+g)_L = f_L + g_L$ and $(fg)_L = f_L g_L$.*

Proof. We have $f(x) = z$ iff $A_f(z, x)$; $g(x) = w$ iff $A_g(w, x)$ and $(f+g)(x) = u$ iff $A_{f+g}(u, x)$. But $\forall x, z, w, u$ in R we have: $p_i(x) > 0$, $A_f(z, x)$, $A_g(w, x)$ and $A_{f+g}(u, x)$ implies $u = z + w$. So by Theorem 1.8, the same holds for L.

One handles $(fg)_L$ similarly.

3. The Nash ring is Noetherian. We retain the notation of § 2 so that D is a domain in R^n defined by a finite number of polynomial inequalities and A_D is the ring of algebraic analytic functions $f\colon D \to R$.

LEMMA 3.1. *Every maximal ideal of A_D corresponds to a point of D and vice versa.*

Proof. Let $\mathscr{M}$ be a maximal ideal of A_D and suppose that for every $P \in D$ there exists $f_P \in \mathscr{M}$ with $f_P(P) \neq 0$. Then choose $f \neq 0$, $f \in \mathscr{M}$. Let $V_R(f)$ denote the zero set of f in D. There exists a polynomial $p_f(z, x)$ so that $p_f(f(x), x) = 0$ for all x in D. Then if $p_f(z, x) = a_d(x)z^d + \cdots + a_0(x)$, we have $a_d(x)(f(x))^d + \cdots + a_0(x) = 0$ for all x in D. Then it follows that a_0 vanishes on $V_R(f)$, and so $V_R(f) \subset V_R(a_0)$. The singular points of $V(a_0)$ will have dimension $\leqq n-2$ and if we let W be the singular set of $V_R(a_0)$, then $V_R(a_0) - W$ will be a union of a finite number of topological components; $C_1, \cdots, C_s$ by Theorem 2.1 or ([8], p. 547). For each C_i choose $P_i \in C_i$ and $f_i \in \mathscr{M}$ so that $f_i(P_i) \neq 0$. Then f_i will vanish only on $W_i \subset C_i$ which is of dimension $\leqq n-2$. Then replacing $V_R(a_0)$ by $W \cup W_1 \cup \cdots \cup W_s$, we go through the same process of removing the singular points and finding new f_i which vanish only on a lower dimensional piece of $W \cup W_1 \cup \cdots \cup W_s$. Eventually we obtain $f_1, \cdots, f_t \in \mathscr{M}$ so that for all P in D, there exist some f_i with $f_i(P) \neq 0$. Let $f = \sum f_i^2$. Then f is in $\mathscr{M}$ and also a unit in A_D, which is a contradiction.

LEMMA 3.2. *For every maximal ideal $\mathscr{M} \subset A_D = A$, the local ring $A_{\mathscr{M}}$ is Noetherian.*

Proof. (As in [1], p. 87). Every maximal ideal $\mathscr{M}$ corresponds to a point of D, so we may as well assume that this point is $0 = (0, 0, \cdots, 0)$. The completion of A at $\mathscr{M}$ is then isomorphic to $R[[x_1, \cdots, x_n]]$ and thus Noetherian. We have $R[x_1, \cdots, x_n] \subset A_{(0)} \subset R[[x_1, \cdots, x_n]] = \hat{A}_{(0)}$.

Let $I_1 \subset I_2 \subset \cdots$ be an increasing sequence of finitely generated ideals of $A_{(0)}$. We will show that this sequence is eventually constant. Since $\{I_j\hat{A}_{(0)}\}$ is eventually constant, it is sufficient to show that I finitely generated implies $I\hat{A}_{(0)} \cap A_{(0)} = I$. So let $I = (a_1, \cdots, a_s)$ and let $b \in I\hat{A}_{(0)} \cap A_{(0)}$. Then there exists a finite etale extension B of $R[x_1, \cdots, x_n]$ which contains $a_1, \cdots, a_s$, and b. This follows from the definition of A. Now $\hat{B} = \hat{A}_{(0)}$. So $(a_1, \cdots, a_s)\hat{B} \cap B = (a_1, \cdots, a_s)B$ (by [9], p. 269, Theorem 12). Thus $b \in (a_1, \cdots, a_s)A_{(0)}$, since $B \subset A_{(0)}$.

LEMMA 3.3. *Let $\mathfrak{q}$ be a prime ideal of $R[x_1, \cdots, x_n] \subset A_D = A$. Then $\mathfrak{q}A_D = \mathscr{P}_1 \cap \cdots \cap \mathscr{P}_s$ where the $\mathscr{P}_i$ are prime in A.*

Proof. Let C = the complex numbers. Let V = the variety of $\mathfrak{q}$ in C^n. Let W be a normalization of V. Then we can consider $W \subset C^{n+m}$ so that $\pi: C^{n+m} \to C^n$ induces $\pi: W \to V$. If $(z_1, \cdots, z_n)$ are coordinates for C^n, letting $z_j = x_j + iy_j$, we get $C^n \cong R^{2n}$ and similarly we get $C^{n+m} \cong R^{2(n+m)}$. If

$$D = \{(x_1, \cdots, x_n, y_1, \cdots, y_n) \in R^{2n} \mid p_i(x, \cdots, x_n) > 0,\ i = 1, \cdots, t\}\ ,$$

then $\pi^{-1}(D) = \{(x_1, \cdots, x_{n+m}, y_1, \cdots, y_{n+m}) \in R^{2(n+m)} \mid p_i(x_1, \cdots, x_n) > 0,\ i = 1, \cdots, t$ and $y_j = 0$ for $j = 1, \cdots, n\}$. As usual $p_i(x) \in R[x_1, \cdots, x_n]$. So $\pi^{-1}(D)$ is defined by a polynomial relation. Also since W is the zero set of some polynomials $g_1(z_1, \cdots, z_{n+m}), \cdots, g_s(z_1, \cdots, z_{n+m})$ in $C[z_1, \cdots, z_{n+m}]$, W considered in $R^{2(n+m)}$ is the zero set of

$$\mathrm{Re}\,(g_1(x_1, \cdots, x_{n+m}, y_1, \cdots, y_{n+m}))\ ,$$
$$\mathrm{Im}\,(g_1(x_1, \cdots, x_{n+m}, y_1, \cdots, y_{n+m})), \cdots .$$

Then, by Theorem 2.1, $\pi^{-1}(D) \cap W$ has a finite number of components $E_1, \cdots, E_s$.

For each E_i, we define a prime $\mathscr{P}_i$ in A_D by letting $\mathscr{P}_i = \{f \in A_D \mid f \circ \pi$ vanishes on an open neighborhood of E_i in $W\}$. Since any f in A_D can be extended to an open neighborhood U of D in C^n, f will be defined on $\pi^{-1}(U)$ and so on $\pi^{-1}(U) \cap W$.

Since W is normal, about every point $R \in W$, there exists a neighborhood $U_R \subset W$ so that $U_R - (U_R \cap W_{sing})$ is connected. Here W_{sing} = singular points in W. The above statement follows from Zariski's Main Theorem [9], p. 320, Theorem 32, and [5] p. 115, Theorem 16. So if $f \circ \pi$ vanishes over some neighborhood $U \subset W$ of some $Q \in E_i$, it follows that $f \circ \pi$ vanishes over some neighborhood of E_i. So if $(fg) \circ \pi$ vanishes on a neighborhood of E_i, then either $f \circ \pi$ or $g \circ \pi$ will vanish on a neighborhood of some point of E_i and so over a neighborhood of E_i. Thus $\mathscr{P}_i$ is prime.

It also follows that $\mathfrak{q} A_D = \mathscr{P}_1 \cap \cdots \cap \mathscr{P}_s$. If $f \in \mathfrak{q}$, then f vanishes on W and so $(f \circ \pi)$ will vanish on a neighborhood of each E_i and so $f \in \mathscr{P}_1 \cap \cdots \cap \mathscr{P}_s$.

If $f \in \mathscr{P}_1 \cap \cdots \cap \mathscr{P}_s$, then $f \circ \pi$ vanishes on a neighborhood in W of E_i, for all i. So, if $P \in D$, $f \circ \pi$ vanishes on a neighborhood of $\pi^{-1}(P)$ on W so f vanishes on V near P. By the local nullstellensatz [5], p. 92, Theorem 20, $\mathscr{P}_1 \cap \cdots \cap \mathscr{P}_s \hat{A}_P = \mathfrak{q} \hat{A}_P$ where $\hat{A}_P$ = the completion of the local ring A_P. But, as in the proof of Lemma 3.2, this implies that $\mathscr{P}_1 \cap \cdots \cap \mathscr{P}_s A_P = \mathfrak{q} A_P$. By Theorem 3.1, all maximal ideals of A come from some P in D and so $\mathfrak{q} A = \mathscr{P}_1 \cap \cdots \cap \mathscr{P}_s$.

THEOREM 3.4. *A_D is Noetherian.*[2]

Proof. It is enough to show that $\mathscr{P}$ prime in A_D implies $\mathscr{P}$ is finitely generated, [6], p. 8, Theorem 3.4. Let $A = A_D = \lim A_j$ where $A_0 = R[x_1, \cdots, x_n]$ and A_j is finitely generated over A_0 and A_j is etale over A_0 in a neighborhood of D. Let $\mathscr{P} \cap A_j = \mathfrak{q}_j$. Then $\mathfrak{q}_0 A = \mathscr{P}_1 \cap \cdots \cap \mathscr{P}_s$, all $\mathscr{P}_i$ prime, by Lemma 3.3. If $A_k \supset A_j$, then $\mathfrak{q}_j A_k = \mathfrak{q}_k \cap \mathfrak{q}_{jk2} \cap \cdots \cap \mathfrak{q}_{jkt}$ where t depends on j and k, and all $\mathfrak{q}_{jkl}$ are prime and of the same dimension. Also $\mathfrak{q}_j A = \mathfrak{q}_k A \cap \cdots \cap \mathfrak{q}_{jkt} A$. But $\mathfrak{q}_j A \supset \mathfrak{q}_0 A$ and so is the intersection of a finite number of the $\mathscr{P}_i$. Since $\lim \mathfrak{q}_j A = \mathscr{P}$, $\mathfrak{q}_j$ eventually stops splitting and $\mathfrak{q}_j A = \mathscr{P}$, for j large.

4. The Nullstellensatz.

We retain the notation of the previous sections so that D is defined by a finite number of polynomial inequalities. A_D is still the Nash ring.

LEMMA 4.1. *If $f \in A_D$ and $f(a) > 0$ for all $a \in D$, then, there exists $h \in A_D$ so that $f = h^2$. Moreover, f and h are units in $A = A_D$.*

Proof. Define $h(a) = f(a)^{1/2}$ for all a in D. Then note that h is in A. The fact that f and h are units is clear.

[2] This theorem has been proved independently by different methods by J. J. Risler, [10].

DEFINITION 4.2. Consider L an ordered field containing R, the reals. Then ε in L is infinitesmal if $0 < |\varepsilon| < \lambda$ for all λ in R.

We say L is *rank one ordered* if there exists ε infinitesmal in L and if for any other infinitesmal α in L there exist positive integers m and n so that $|\varepsilon|^m < |\alpha|$ and $|\alpha|^n < |\varepsilon|$.

THEOREM 4.3. *Let $\mathscr{P}$ be a prime ideal in A_D. Then the quotient field of $A_D/\mathscr{P}$ is rank one orderable if and only if $I(V_R(\mathscr{P})) = \mathscr{P}$.*

Proof. The proof will occupy the rest of the section. We first assume $A_D/\mathscr{P}$ rank one orderable and note that there are two cases which will be handled separately. Let $p_1(x) > 0$, $p_2(x) > 0, \cdots, p_s(x) > 0$ be the polynomial inequalities defining D and let $p(x) = \prod p_i/(1 + \sum x_j^2)^l$ where $l > \sum \deg p_i$. Then there exists a real number $M > 0$ so that $|p(x)| < M$ for all x in R^n and so by Tarski's principle (Theorem 1.8) $|p(x)| < M$ for all x in L^n for L any real closed field containing R.

Now let L be a real closure of the quotient field of $A_D/\mathscr{P}$ which by hypothesis will be rank one ordered. We let φ be the total map $A_D \to A_D/\mathscr{P} \to L$. Then since $R[x_1, \cdots, x_n] \subset A_D$, we have $x = (x_1, \cdots, x_n) \in L^n$. So $p(\varphi x)$ makes sense and (considering $R \subset L$) we have two cases (1) $p(\varphi x)$ is infinitesmal and (2) $p(\varphi x) - \alpha$ is infinitesmal for some $\alpha \in R$, $\alpha \neq 0$. By Theorem 3.4, A_D is Noetherian and so $\mathscr{P} = (f_1, \cdots, f_u)$ for some $f_1, \cdots, f_u \in \mathscr{P}$. We let $X = V(\mathscr{P}) = \{(x_1, \cdots, x_n) \in C^n \mid f_i(x_1, \cdots, x_n) \quad i = 1, \cdots, u\}$ and let $\mathfrak{q} = \mathscr{P} \cap R[x_1, \cdots, x_n]$ and $W = V(\mathfrak{q})$.

LEMMA 4.4. *In Case (1), $p(\varphi x) = \varepsilon$ infinitesmal in L, $X = V(\mathscr{P})$ contains a real nonsingular point of $W = V(\mathfrak{q})$ and so $I(V_R(\mathscr{P})) = \mathscr{P}$.*

Proof. If X_R, the set of real points of X, is such that X_R is contained in the singular set of W, then there exists $q(x) \in R[x_1, \cdots, x_n]$ so that $q(X_R) = 0$ but $\varphi q \neq 0$. This is because $R[x_1, \cdots, x_n]/\mathfrak{q}$ is orderable and so $\mathfrak{q} = I(V_R(\mathfrak{q}))$ by the Dubois-Risler Nullstellensatz ([4], Theorem 2.1). Let $f = \sum f_i^2$, (recall $\mathscr{P} = (f_1, \cdots, f_u)$). Then for any $a \in R^n$, $f(a) = 0$ if and only if $a \in X_R$.

Now let $h(x) = \prod_{i=1}^{u} p_i^2 q^2/(1 + \sum_{i=1}^{n} x_i^2)^m$ where $m \geqq \sum \deg p_i + \deg q$. Then $h(x)$ is bounded on R^n and so in particular on D. We now define a new function $g(r) = \inf\{f(x) \mid x \text{ in } D \text{ and } h(x) = r\}$. For r small and positive, $\{x \mid h(x) = r\}$ is a compact set in D and so $g(r)$ is defined and positive. Also $g(0) = 0$. By Theorem 1.8, Tarski's principle, $g(r)$ is defined by a polynomial relation. This means that $g(r)$ is "piecewise algebraic" and each of the pieces can be expanded in Puisseaux series. Then it follows easily that there exists an integer λ so that $g(r) \geqq r^\lambda$ for all r in the domain of g. Then $f(x) \geqq h(x)^\lambda$ for all x in D. Since $p(x) > 0$ on D, we have $f(x) - h(x) + p(x)^m > 0$ for all x in D, and for any positive integer m. Applying Lemma 4.1, we see $\varphi f - h(\varphi x) + \varepsilon^m > 0$ for all positive integers m. But since ε is infinitesimal in L and L is rank one ordered, we see $\varphi f \geqq h(\varphi x) > 0$. But this contradicts $f \in \mathscr{P} = \ker \varphi$. So X contains a nonsingular real point P of W.

That $I(V_R(\mathscr{P})) = \mathscr{P}$ will now be shown. First, by the implicit function theorem, we know that there exists a neighborhood U of P in R^n so that $U \cap W_R = U \cap X_R$ is isomorphic to a ball in R^d, $d =$ dimension of W. That is we have an analytic algebraic map of a ball $B \subset R^d$, $B \xrightarrow{j} X_R$ which induces a homomorphism $A_D/\mathscr{P} \to A_B$, $g \to g \circ j$. Now if g vanishes on X_R, $g \circ j$ vanishes on B and since $g \circ j$ is analytic, it is zero. But then g itself will vanish on a complex neighborhood of P in X and so $g = 0$ on X and is in $\mathscr{P}$.

LEMMA 4.5. *In Case* (2), $p(\varphi x) - \alpha$ *infinitesimal,* $\alpha \neq 0$ *and* $\alpha \in R$, *we have* $f(\varphi x)$ *makes sense and* $= \varphi f$.

Proof. For each p_i we have $p_i(a) > 0$ for all a in D so by Lemma 4.1, $p_i = h^2$ for some unit h in A_D. But then $\varphi p_i = (\varphi h)^2 > 0$. But $\varphi p_i = p_i(\varphi x)$ and so $p_i(\varphi x) > 0$ for all i which implies $\varphi x \in D_L$. This shows $f(\varphi x)$ is defined by Definition 2.3.

If any φx_i were infinite (larger in absolute value than all real numbers), then we would be in Case (1), so we can assume that for each i there exists $a_i \in R$ with $a_i - \varphi x_i$ infinitesimal or 0. Now $P = (a_1, \cdots, a_n)$ is not on the boundary of D for if it were then $p(a_1, \cdots, a_n)$ would $= 0$. This would imply $p(\varphi x_1, \cdots, \varphi x_n)$ infinitesimal and put us in Case (1).

For notational simplicity, we assume $P = (0, \cdots, 0)$ and by the above, we can assume that P is in the interior of D. For any $f \in A_D$, we can expand f in finite Taylor series about P so $f(x) = \sum_{|i| \leqq m} \partial f/\partial x^i(P)x^i + \sum_{|i|=m} x^i g_i(x)$ where $i = (i_1, \cdots, i_n)$ is an n-tuple of nonnegative integers, $|i| = i_1 + \cdots + i_n$, and $g_i \in A_D$. We abbreviate by writing $f = p_m(x) + \sum x^i g_i(x)$. By assumption each φx_i is infinitesimal or 0.

We claim that $\exists M_i \in R$ so that $|\varphi g_i| < M_i$. This is because g_i being analytic at P is bounded near P so there exists M_i a positive real number and $\delta > 0$ so that $||x|| < \delta$ implies $|g_i(x)| < M_i$. But then there exists an integer $j_0 > 0$ so that $M_i^2 - g^2(x) + \sum_{i=1}^n (x_i/\delta)^{2j} > 0$ for all x in D, and all $j \geqq j_0$. But then $M_i \geqq |\varphi g|$ as in the argument of Lemma 4.4. So we see that $|\varphi f - \varphi p_m| < \varepsilon^m M_m < \varepsilon^{m/2}$, ε infinitesimal and > 0 in L. So $\lim_{m \to \infty} \varphi p_m = \varphi f$ in L.

Next note that $f(\varphi x) = p_m(\varphi x) + \sum_{|i|=m} (\varphi x)^i g_i(\varphi x)$ so $|f(\varphi x) - p_m(\varphi x)| < \varepsilon^{m/2}$ also and $\lim_{m\to\infty} p_m(\varphi x) = f(\varphi x)$. But $p_m(\varphi x) = \varphi p_m$ and so our result follows.

LEMMA 4.6. *If $f(\varphi x) = \varphi f$, for all $f \in A_D$, then $I(V_R(\mathscr{P})) = \mathscr{P}$.*

Proof. Note that $g \in I(V_R(\mathscr{P}))$ if and only if (*): For all a in D, $f_i(a) = 0$, $i = 1, \cdots, u$ implies $g(a) = 0$. By Theorem 2.2, there are polynomial relations A_{f_i} and A_g so that (*) is equivalent to (**): For all a in D, $A_{f_i}(0, a_1, \cdots, a_n)$, $i = 1, \cdots, u$ implies $A_g(0, a_1, \cdots, a_n)$. Now apply Theorem 1.8 and we have (***): For all a in D_L, $A_{f_i}(0, a_1, \cdots, a_n)$ $i = 1, \cdots, u$ implies $A_g(0, a_1, \cdots, a_n)$. But by hypothesis $\varphi f_i = f_i(\varphi x) = 0$ so by (***) $g(\varphi x) = 0$. But $\varphi g = g(\varphi x)$ and so $g \in \mathscr{P}$.

LEMMA 4.7. *If $\mathscr{P}$ has the zeros property, $I(V_R(\mathscr{P})) = \mathscr{P}$, then $A_D/\mathscr{P}$ is rank one orderable.*

Proof. As in the proof of Lemma 4.6, it follows that if $\mathscr{P}$ has the zeros property, then $X = V(\mathscr{P})$ contains a real nonsingular point P. Then the completion of the local ring of X at P is isomorphic to $R[[t_1, \cdots, t_d]]$, $d =$ dimension X. Thus $A_D/\mathscr{P} \subsetneq R[[t, \cdots, t_d]]$ and so we are reduced to the following lemma.

LEMMA 4.8. *$R[[t_1, \cdots, t_d]]$ can be rank one ordered.*

Proof. Choose $\alpha_1, \cdots, \alpha_d$ positive real numbers linearly independent over Q the rational numbers. Then order d-tuples $\langle m_1, \cdots, m_d\rangle$ of nonnegative integers by $\langle m_1, \cdots, m_d\rangle > \langle m_1', \cdots, m_d'\rangle$ if and only if $\sum_{i=1}^d m_1\alpha_i > \sum_{i=1}^d m_i'\alpha_i$. This is clearly a well ordering. Now order power series $\sum a_i t^i$ for $i = \langle i_1, \cdots, i_d\rangle$ by taking $\sum a_i t^i >$ 0 if the least i (with the described well ordering) with $a_i \neq 0$ has $a_i > 0$. This gives the required ordering.

THEOREM 4.9. *Let $D \subset R^2$ be defined by strict polynomial inequalities. Then an ideal $J \subset A_D$ is real* (Definition 0.3) *if and only if $I(V_R(J)) = J$.*

Proof. First note that if $J = \mathscr{P}$ is prime, then $A_D/\mathscr{P}$ will have transcendence degree $\leqq 2$ over R. If the transcendence degree is 0, then $\mathscr{P}$ is a maximal ideal in A_D and by Lemma 3.1 corresponds to a point of D. So $\mathscr{P}$ has the zeros property trivially.

If the transcendence degree is 2, then clearly $\mathscr{P} = (0)$ and $V_R(\mathscr{P}) = D$ and again no problem.

If the transcendence degree is 1, then the quotient field of $A_D/\mathscr{P}$ if real can only be rank one orderable and so Theorem 4.3 applies and $\mathscr{P}$ is real if and only if $I(V_R(\mathscr{P})) = \mathscr{P}$.

To finish, note that for any radical ideal $J \subset A_D$; $J = \mathscr{P}_1 \cap \cdots \cap \mathscr{P}_s$ an intersection of prime ideals, since A_D is Noetherian. But as in [4] Lemma 2.2, J is real if and only if each $\mathscr{P}_i$ is real. So J real implies $I(V_R(J)) \subset I(V_R(\mathscr{P}_1)) \cap \cdots \cap I(V_R(\mathscr{P}_s)) = \mathscr{P}_1 \cap \cdots \cap \mathscr{P}_s = J$. Since $I(V_R(J)) \supset J$ always, $J = I(V_R(J))$.

The converse is easy.

References

1. M. Artin, *Grothendieck Topologies*, Seminar notes, Harvard University, 1962.

2. N. Bourbaki, *Commutative Algebra*, Chapter 6, Valuations, Hermann, Paris, 1964.

3. P. Cohen, *Decision procedures for real and p-adic fields*, Comm. on Pure and Appl. Math. **22** (1969), 131-151.

4. G. Efroymson, *Local Reality on Algebraic Varieties*, J. Algebra, **29** (1974), 133-142.

5. R. Gunning and H. Rossi, *Analytic Functions of Several Complex Variables*, Prentice Hall, Englewood Cliffs, N. J., 1965.

6. M. Nagata, *Local Rings*, Interscience, John Wiley and Sons, New York, 1962.

7. R. Palais, *Equivariant Real Algebraic Differential Topology, Part I. Smoothness Categories and Nash Manifolds*, Notes Brandies University, 1972.

8. H. Whitney, *Elementary structures of real algebraic varieties*, Annals of Math., **66** (1957), 545-556.

9. O. Zariski and P. Samuel, *Commutative Algebra*, Volume II, Van Nostrand, Princeton, 1960.

10. J. J. Risler, *Sur L'anneau des fonctions de Nash globales*, C. R. Acad. Sci., Paris, **276** (1973), A1513-1516.

Received April 16, 1973 and in revised form September 18, 1973.

THE UNIVERSITY OF NEW MEXICO

Printed in Japan by International Academic Printing Co., Ltd., Tokyo, Japan

Pacific Journal of Mathematics

Vol. 54, No. 1 May, 1974