TRANSACTIONS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 264, Number 1, March 1981

WHICH CURVES OVER Z HAVE POINTS WITH COORDINATES IN A DISCRETE ORDERED RING?

BY

LOU VAN DEN DRIES

ABSTRACT. A criterion is given for curves defined over $\mathbf{Z}$ to have an infinite point in a discrete ordered ring.

Using this, one can decide effectively whether a given polynomial in $\mathbf{Z}[X, Y]$ has a zero in a model for the axioms of open induction.

Riemann-Roch for curves over $\mathbf{Q}$ is the main tool used.

Introduction. There is little doubt that most results in (classical) number theory, suitably formulated, can be deduced from a very small subset of the set of 1st order Peano axioms.

Indeed, some experience suggests that the main techniques and theorems can be coded in 1st order terms and deduced from Σ_1-induction, i.e. using only the induction axioms for Σ_1-formulas (G. Kreisel actually carried this out for parts of analytic number theory).

Also the negative solution of Hilbert's 10th problem can be deduced from Σ_1-induction, which implies that there is no algorithm deciding for a given diophantine equation whether Σ_1-induction can prove that it has no zeros, or equivalently:

the set of diophantine equations solvable in a model of Σ_1-induction is not recursive.

So it seems a reasonable guess that (future) decision methods for the solvability of certain types of diophantine equations will actually be derivable from rather weak fragments of Σ_1-induction. (*Question*: Which subset of Σ_1-induction suffices to deduce A. Baker's results?)

Taking this speculation seriously, one is led to the following program:

given a certain fragment of Σ_1-induction, characterize the set of diophantine equations which can be solved in a model of that fragment. Building on previous work of J. C. Shepherdson [**10**], A. Wilkie recently took a first step in this direction by proving [**12**]:

A polynomial $f = f(X) \in \mathbf{Z}[X]$, $X = (X_1, \ldots, X_n)$, has a zero in some model of OPEN *induction* (*see* §1), *iff there is an ideal $I \subset \mathbf{Z}[X]$ containing f such that I has for each prime number p a p-adic integral zero and $\mathbf{Z}[X]/I$ can be discretely ordered.*

However, this does not yet solve Problem 5.1 of [**12**]–first posed by Shepherdson–whether the set of diophantine equations solvable in a model of open induction is recursive. The main result of this paper is an affirmative answer if we restrict the diophantine equations to those in 2 variables.

Received by the editors August 10, 1979.
1980 *Mathematics Subject Classification.* Primary 03C65, 10N05, 10N15.

0002-9947/81/0000-0112/$03.25

Using Wilkie's theorem for $n = 2$, we indicate an algorithm deciding for a given equation

$$f(X, Y) = 0 \qquad (f(X, Y) \in \mathbf{Z}[X, Y])$$

whether it has a solution in a model of open induction.

Let me outline the method I followed:

Shepherdson's problem can be reduced to deciding whether the function field over $\mathbf{Q}$ of the variety defined by an irreducible $f(X) \in \mathbf{Q}[X]$ has a valuation ring of a certain type.

Now for $n = 2$ these valuation rings are discrete and have a simple geometric interpretation: they are the points of the (desingularized, projective) curve defined by f over $\mathbf{Q}$, and so we can apply standard methods in the theory of curves.

However, for $n > 2$, the valuation rings of the function fields do not have such a simple geometric interpretation, and it seems that Shepherdson's problem is still open for $n > 2$.

§1 gives precise definitions, §2 provides the mathematical results needed for the algorithm, the existence of which is finally proved in §3. It may be useful to the reader to consider §3, before reading §2 in detail, to see how the various results of §2 are actually used.

1. Conventions and definitions. All rings are assumed to be commutative with 1.

A discrete ordered ring is a ring endowed with a linear ordering (compatible with the ring operations) in which 1 is the smallest strictly positive element. Clearly such a ring is a domain containing $\mathbf{Z}$ as a discrete ordered subring.

A model of open induction is a discrete ordered ring satisfying all induction axioms

$$[\Delta(\bar{x}, 0) \wedge \forall y \geqslant 0\, (\Delta(\bar{x}, y) \to \Delta(\bar{x}, y + 1))] \to \forall y \geqslant 0\, \Delta(\bar{x}, y)$$

with $\Delta(\bar{x}, y)$ an open formula in the language $\{+, \cdot, -, 0, 1, <\}$ of ordered rings.

Given a domain D, its fraction field is denoted by $Q(D)$, and for the localizations of D with respect to a prime ideal $\underline{p}$ of D and with respect to an element $f \in D \setminus \{0\}$ we use the standard notations:

$$D_{\underline{p}} = \{d/s | d \in D, s \in D \setminus \underline{p}\}, \quad D_f = \{d/f^k | d \in D, k \geqslant 0\}.$$

2. An algebraic characterization of 'discrete-orderable' and its consequences.

LEMMA 1. *Let D be a domain, $\mathbf{Z} \subset D$. Then D has a discrete ordering iff no integer $n > 1$ is a unit in D and the fraction field $Q(D)$ of D has a valuation ring V whose residue field is formally real and which satisfies $V \cap \mathbf{N}^{-1}D = \mathbf{Q}$ ($\mathbf{N}$ is the multiplicative set $\{1, 2, 3, \ldots\} \subset D$).*

PROOF. Let $<$ be a discrete ordering on D, and denote its (unique) extension to an ordering on $Q(D)$ also by $<$. Clearly 1 and -1 are the only units of D. Define $V_< = \{x \in Q(D) | -n < x < n$ for some $n \in \mathbf{N}\}$, the ring of finite elements of $Q(D)$. Clearly $V_<$ is a convex valuation ring of $Q(D)$, so its residue field is real (cf. [7, §7]).

Moreover, if $d/m \in V_<$, $d \in D$, $m \in \mathbf{N}$, then d is a finite element of D, so $d \in \mathbf{Z}$ by the discreteness of the ordering on D; hence $d/m \in \mathbf{Q}$. Conversely, suppose no integer > 1 is a unit of D and V is a valuation ring as described in the lemma.

It is well known, see [7, §7], that then $Q(V) = Q(D)$ has an ordering $<$, with respect to which V is convex. Denote the restriction of $<$ to D also by $<$.

We claim that $<$ discretely orders D. For suppose $0 < d < 1$, $d \in D$. Then $d \in V \cap D \subset \mathbf{Q}$ by assumption, so $d = p/q$ for relatively prime $p, q \in \mathbf{N}$, $q > 1$, implying easily $1/q \in D$, contradicting the noninvertibility of q. □

LEMMA 2. *There is an algorithm which decides, given any deal $I = (f_1, \ldots, f_k) \subset \mathbf{Z}[X]$, $X = (X_1, \ldots, X_n)$, whether there is an integer $n > 1$ whose image in $\mathbf{Z}[X]/I$ is a unit of this ring.*

PROOF. Clearly it suffices to decide whether there is a prime number p whose image in $\mathbf{Z}[X]/I$ is invertible.

Now a prime p becomes invertible in $\mathbf{Z}[X]/I$ iff there are $h, h_1, \ldots, h_k \in \mathbf{Z}[X]$ with $ph + 1 = \sum h_i f_i$, i.e. iff $1 \in (f_1 \bmod p, \ldots, f_k \bmod p) \subset \mathbf{F}_p[X]$ ($f \bmod p$ denoting the image of $f \in \mathbf{Z}[X]$ under the obvious map $\mathbf{Z}[X] \to \mathbf{F}_p[X]$), i.e. iff

$$\bar{\mathbf{F}}_p \vDash \neg \exists x (f_1(x) = \cdots = f_k(x) = 0),$$

$\bar{\mathbf{F}}_p$ being the algebraic closure of $\mathbf{F}_p$.

By (quantifier) elimination theory for algebraically closed fields one can determine an *open* sentence σ (in the language of ring theory) such that

$$F \vDash \sigma \leftrightarrow \neg \exists x (f_1(x) = \cdots = f_k(x) = 0)$$

for each algebraically closed field F.

Combining this with the preceding remarks we obtain:

Some integer > 1 becomes a unit in $\mathbf{Z}[X]/I$ iff for some prime p: $\mathbf{F}_p \vDash \sigma$. A moment's reflection will make it clear to the reader how to determine, given any open σ, whether $\mathbf{F}_p \vDash \sigma$ holds for some prime p. □

REMARK. For a principal ideal $I = (f)$ this reasoning establishes the equivalence between:

(i) no integer > 1 becomes invertible in $\mathbf{Z}[X]/I$, and

(ii) each common prime divisor of the coefficients of f apart from the constant term $f(0)$ divides also the constant term. This case, for $X = (X_1, X_2)$, actually suffices to obtain the decision method for equations in 2 variables mentioned in the introduction. However, if we extend the theory of open induction by requiring the models to be integrally closed in their fraction field, then the full lemma is useful to obtain a similar decision method, cf. [4].

The following proposition is the basic result underlying our decision method.

PROPOSITION 3. *Let K be a field, $K[x, y]$, $y = (y_1, \ldots, y_m)$, a domain such that x is transcendental over K and $y_1, \ldots, y_m$ integral over $K[x]$. Let V be a valuation ring of $K(x, y)$.*

Then the following are equivalent:

(i) $V \cap K[x, y] = K$,

(ii) *K is integrally closed in $K[x, y]$ and V is the only valuation ring of $K(x, y)$ which extends the valuation ring $K[1/x]_{(1/x)}$ of $K(x)$.*

PROOF. Considering $K(x)$ and $K(x, y)$ as algebraic function fields of one variable over K, cf. [2, p. 1], we associate, as usual, to the valuation ring $K[1/x]_{(1/x)}$ the place at infinity P_∞ of $K(x)$, while the finite places of $K(x)$ are associated to the other proper valuation rings of $K(x)$ which contain K. Similarly, the places of $K(x, y)$ are associated to the proper valuation rings of $K(x, y)$ containing K. If the place Q of $K(x, y)$ is associated to the valuation ring A, then Q is said to lie above the place of $K(x)$ which is associated to the valuation ring $A \cap K(x)$ of $K(x)$. The places of $K(x, y)$ lying above P_∞ are called the infinite places of $K(x, y)$–there are at most $[K(x, y): K(x)]$ of them–and the others, naturally, finite places.

A place Q, associated to the valuation ring $A \subset K(x)$, resp. $A \subset K(x, y)$, determines an "evaluation" map:

$$f \mapsto f(Q) \quad \text{from } K(x) \text{ to } A/m(A) \cup \{\infty\},$$
$$\text{resp. from } K(x, y) \text{ to } A/m(A) \cup \{\infty\}$$

which is on A the residue class map, and which maps the elements not in A to ∞; $f(Q)$ is called the value of f at the place Q, and if $f(Q) = \infty$, Q is called a pole of f. So we consider the elements of $K(x)$, resp. of $K(x, y)$, as functions defined on the set of places of $K(x)$, resp. of $K(x, y)$ and in this role they are called (algebraic) functions. Those without poles are so-called constants and they form a subfield, the field of constants, which is for $K(x)$ the field K, and for $K(x, y)$ the algebraic closure of K within $K(x, y)$. For all this, see [2, Chapter I], or [9].

(i) $\Rightarrow$ (ii). From $V \cap K[x, y] = K$, it clearly follows that V is a proper valuation ring of $K(x, y)$ containing K, and that it can only extend the valuation ring $K[1/x]_{(1/x)}$ of $K(x)$ (because $V \cap K[x] = K$), so the place Q_V of $K(x, y)$ associated to V is an infinite place.

That K is integrally closed in $K[x, y]$ is seen as follows: a function $f \in K[x, y]$ integral over K belongs to every valuation ring of $K(x, y)$ containing K, so in particular to V; hence $f \in V \cap K[x, y] = K$.

Suppose now that, apart from Q_V, there is another infinite place Q_∞ of $K(x, y)$. We have only to derive a contradiction from this.

Let B be the integral closure of $K[x]$ in $K(x, y)$, and let $I = \{f \in K[x, y] | f \cdot B \subset K[x, y]\}$, so $K[x, y] \subset B$ and I is the so-called conductor of B in $K[x, y]$; it is important for us that I is a *nonzero* ideal of B as well as of $K[x, y]$.

Because B is a Dedekind domain, we obtain $I = \underline{p}_1^{e_1} \cdots \underline{p}_k^{e_k}$ for distinct maximal ideals $\underline{p}_1, \ldots, \underline{p}_k$ of B and $e_1 > 0, \ldots, e_k > 0$, and these maximal ideals $\underline{p}_1, \ldots, \underline{p}_k$ determine valuation rings $B_{\underline{p}_1}, \ldots, B_{\underline{p}_k}$, hence finite places $\underline{P}_1, \ldots, \underline{P}_k$ of $K(x, y)$.

Riemann's theorem, cf. [2, p. 22], implies that there is an algebraic function $f \in K(x, y)$ which has Q_∞ as its only pole and has a zero of order at least e_i at $\underline{P}_i$ for $i = 1, \ldots, k$.

But f, having no finite poles, belongs to $B = \{q \in K(x, y) | q \text{ has no finite pole}\}$, hence to $B \cap (\underline{p}_1 B_{\underline{p}_1})^{e_1} \cap \cdots \cap (\underline{p}_k B_{\underline{p}_k})^{e_k} = \underline{p}_1^{e_1} \cdots \underline{p}_k^{e_k} = I \subset K[x, y]$, so $f \in V \cap K[x, y] = K$; but f, having Q_∞ as a pole, is not a constant, contradiction!

(ii) $\Rightarrow$ (i). An algebraic function f in $V \cap K[x, y]$ has no finite pole because it is integral over $K[x]$, but also no infinite pole, because Q_V is the only infinite place, by assumption.

So such an f is constant, i.e. integral over K; hence, because K is assumed to be integrally closed in $K[x, y]$ we get $f \in K$, so $V \cap K[x, y] = K$. □

REMARK. The use of Riemann's theorem in this proof can be replaced by using the strong approximation result in Ribenboim's [**9**, p. 76], which is there the main lemma for the proof of Riemann's theorem.

LEMMA 4. *There is an algorithm which decides, given any irreducible* $f \in \mathbf{Q}[X, Y]$, *whether* $\mathbf{Q}$ *is integrally closed in* $\mathbf{Q}[X, Y]/(f)$.

PROOF. Let irreducible $f \in \mathbf{Q}[X, Y]$ be given. By linear transformation of variables we may assume f to be monic in Y, say $\deg_Y f = d > 0$. Put $x = X + (f), y = Y + (f)$, so $\mathbf{Q}[X, Y]/(f) = \mathbf{Q}[x, y]$. Let K be the algebraic closure of $\mathbf{Q}$ in the field $\mathbf{Q}(x, y)$. Then K is the unique finite extension of $\mathbf{Q}$ such that $K \subset \mathbf{Q}(x, y)$ and (x, y) is a zero of an *absolutely* irreducible polynomial $q(X, Y) \in K[X, Y]$, cf. [**6**, p. 71]. Note that each element of $\mathbf{Q}(x, y)$ is of the form $p(x, y)$ for a unique polynomial $p(X, Y) \in \mathbf{Q}(X)[Y]$, $\deg_Y p < d$.

By a systematic search one will eventually find a polynomial $p(X, Y) \in \mathbf{Q}(X)[Y]$, $\deg_Y p < d$, an irreducible polynomial $r(Z) \in \mathbf{Q}[Z]$, and a polynomial $q(X, Y, Z) \in \mathbf{Q}[X, Y, Z]$, such that $r(p(x, y)) = 0$, $q(x, y, p(x, y)) = 0$ and $q(X, Y, p(x, y))$ is absolutely irreducible.

Then $K = \mathbf{Q}[p(x, y)]$ by the description of K given above. Now the integral closure $K \cap \mathbf{Q}[x, y]$ of $\mathbf{Q}$ in $\mathbf{Q}[x, y]$ is a subfield of K. We determine the subfields of K as follows: let $m = \deg r(Z)$ and let $\alpha_1, \ldots, \alpha_m$ be the distinct roofs of $r(Z)$, identifying, say, $p(x, y)$ with α_1.

By [**11**, 56], we can determine the Galois group G of $r(Z)$ over $\mathbf{Q}$ as a permutation group on $\{\alpha_1, \ldots, \alpha_m\}$. Then, by the fundamental theorem of Galois theory, the subfields of K are the fixed fields of the subgroups H of G which contain $\{\sigma \in G | \sigma(\alpha_1) = \alpha_1\}$. Again, by a systematic search, one will find as many subfields of K in the form $\mathbf{Q}[\lambda(\alpha_1)]$, $\lambda(Z) \in \mathbf{Q}[Z]$, as there are such subgroups H of G (to tell these fields apart one may use the algorithms in [**3**, Fact 4]), and then all subfields of K have been found.

For each subfield $\mathbf{Q}[\lambda(p(x, y))]$ we compute a (uniquely determined) polynomial $q \in \mathbf{Q}(X)[Y]$ with $\lambda(p(x, y)) = q(x, y)$ and $\deg_Y q < d$. Then $\mathbf{Q}[\lambda(p(x, y))] \subset \mathbf{Q}[x, y]$ iff $q \in \mathbf{Q}[X, Y]$. By this equivalence we can decide whether $\mathbf{Q}$ is the only subfield of K contained in $\mathbf{Q}[x, y]$, i.e. whether $\mathbf{Q}$ is integrally closed in $\mathbf{Q}[x, y]$. □

REMARKS. (i) If $f \in \mathbf{Q}[X, Y]$ is absolutely irreducible, then $\mathbf{Q}$ is automatically integrally closed in $\mathbf{Q}[X, Y]/(f)$.

This case is the essential one from the diophantine viewpoint: if $f \in \mathbf{Q}[X, Y]$ is irreducible but not absolutely irreducible, then the rational solutions of $f = 0$ lie on the intersection of two distinct affine curves $q(X, Y) = 0$ and $q^\sigma(X, Y) = 0$, where q is an absolutely irreducible factor of f in $K[X, Y]$, K a suitable finite extension of $\mathbf{Q}$, and q^σ is a conjugate of q over $\mathbf{Q}$ different from q; elimination theory then gives a method to determine all rational solutions of $f = 0$ of which, by Bezout, there are at most $(\deg q)^2 \leqslant \frac{1}{4}(\deg f)^2$.

(ii) $f = X^2 - 2Y^2$ is an example of an irreducible but not absolutely irreducible polynomial in $\mathbf{Q}[X, Y]$, such that $\mathbf{Q}$ is integrally closed in $\mathbf{Q}[X, Y]/(f)$.

LEMMA 5. *Let K be a field of characteristic 0, V a discrete valuation ring of K, and i: $K \to \omega$ an indexing such that (K, i) is a computable field (cf. [8]), $i(V)$ is a recursive subset of ω and such that an algorithm exists for deciding, given a polynomial in $V[X]$ by the indices of its coefficients, whether its reduction in $\bar{V}[X]$, $\bar{V} = V/\underline{m}(V)$, has a zero in $\bar{V}$. Then there is an algorithm computing for every irreducible polynomial $f \in K[Y]$ the number $r(f)$ of extensions of V to a valuation ring of $K(y)$, y being a root of f in the algebraic closure of K.*

PROOF. For irreducible $f \in K[y]$, $r(f)$ equals the number r in the decomposition $f = f_1 \times \cdots \times f_r$ of f in irreducible factors $f_1, \ldots, f_r$ in $L[Y]$, where (L, W) is any valued field extension of (K, V) such that:

(a) (L, W) is henselian,

(b) the residue class field of V is algebraically closed in the residue class field of W,

(c) a generator π of $\underline{m}(V)$ also generates $\underline{m}(W)$.

Indeed, for such a valued field extension we have a (K, V)-embedding of (K^h, V^h), the henselization of (K, V), into (L, W), making K^h relatively algebraically closed in its extension L, so the number r of irreducible factors of the (separable) polynomial f is the same in $L[Y]$ as in $K^h[Y]$, and so equals also the number of irreducible factors of f in $\hat{K}[Y]$, $\hat{K}$ being the completion of the valued field (K, V).

But the (monic) irreducible factors of f in $K[Y]$ are in 1-1 correspondence with the extensions of V to a valuation ring of $K(y)$, where $f(y) = 0$, cf. [5, p. 16].

From this description of $r(f)$ we obtain an algorithm based on Gödel's completeness theorem as follows: let Σ be a set of sentences in the language of valued fields augmented by names for the elements of K, such that the models of $\mathrm{Diag}(K, V) \cup \Sigma$ are exactly the valued field extensions (L, W) of (K, V) satisfying (a), (b), (c) above.

By the assumptions on (K, V, i) we may assume that $\mathrm{Diag}(K, V) \cup \Sigma$ is recursive. For an irreducible polynomial $f \in K[Y]$ we can then determine $r(f)$ as the number $r \in \{1, \ldots, \deg f\}$ for which "f decomposes in r irreducible factors" is derivable from $\mathrm{Diag}(K, V) \cup \Sigma$. □

REMARK. Suppose f is monic, $f \in V[Y]$ and the discriminant of f is invertible in V. Then, by Hensel's lemma, a decomposition of its reduction $\bar{f} \in \bar{V}[Y]$, $\bar{V} = V/\underline{m}(V)$, in monic irreducible factors in $\bar{V}[Y]$, can be lifted to a decomposition in

$\hat{V}[Y]$, $\hat{V}$ being the completion of V; so in that case $r(f)$ is simply the number of monic irreducible factors of $\bar{f}$ in $\bar{V}[Y]$.

3. Main results.

THEOREM. *The set P of polynomials $f(X, Y) \in \mathbf{Z}[X, Y]$ with a zero in a model of open induction is recursive.*

PROOF. By Gödel's completeness theorem $\mathbf{Z}[X, Y] \setminus P$ is recursively enumerable. So we have only to show that P is recursively enumerable. Its subset $P_{\text{standard}} = \{f \in \mathbf{Z}[X, Y] | f \text{ has a zero in } \mathbf{Z}\}$ is clearly recursively enumerable, so again it suffices to show that the subset $P_{\text{nonstandard}} = \{f \in \mathbf{Z}[X, Y] | f \text{ has a zero } (x, y) \text{ is a model of open induction with } x \text{ or } y \text{ not in } \mathbf{Z}\}$ is recursively enumerable, because $P = P_{\text{standard}} \cup P_{\text{nonstandard}}$.

In fact, we prove that $P_{\text{nonstandard}}$ is recursive.

Let $f = f(X, Y) \in \mathbf{Z}[X, Y]$ be given, f not a constant.

Using Kronecker's algorithm [**11**, p. 79], we can find a decomposition $f = f_1 \times \cdots \times f_r$ with all $f_i \in \mathbf{Z}[X, Y]$ irreducible. Then $f \in P_{\text{nonstandard}} \Leftrightarrow f_i \in P_{\text{nonstandard}}$ for some $1 \leqslant i \leqslant r$. So to decide whether $f \in P_{\text{nonstandard}}$ we may as well assume that f is irreducible in $\mathbf{Z}[X, Y]$ (and nonconstant).

Under this assumption we claim:

$$f \in P_{\text{nonstandard}} \Leftrightarrow \mathbf{Z}[X, Y]/(f) \text{ can be discretely ordered and } f \text{ has for each prime number } p \text{ a } p\text{-adic integral zero.} \qquad (*)$$

Indeed, if the right-hand side of (*) holds, then Theorem 3.3 of [**12**] (or rather its proof) shows that $\mathbf{Z}[X, Y]/(f)$, endowed with any of its discrete orderings, can be embedded in a model of open induction, so (x, y), with $x = X + (f), y = Y + (f)$, is then a nonstandard point of the curve $f(X, Y) = 0$ in a model of open induction.

Conversely, suppose (x, y) is a nonstandard point on the curve $f(X, Y) = 0$ with coordinates x, y in a model of open induction. Then $|x|$ or $|y|$ is infinite in that model, so x or y is transcendental over $\mathbf{Q}$, so the prime ideal $\{p(X, Y) \in \mathbf{Q}[X, Y]: p(x, y) = 0\}$ of $\mathbf{Q}[X, Y]$ is not maximal, and contains the irreducible polynomial f; hence it equals $f \cdot \mathbf{Q}[X, Y]$. By Gauss's lemma this implies: $\{p \in \mathbf{Z}[X, Y]: p(x, y) = 0\} = (f)$. Again from the proof of Theorem 3.3 of [**12**] we obtain from this the right-hand side of (*). So the proof of (*) is now complete.

The existence of an algorithm for deciding, given any polynomial in $\mathbf{Z}[X, Y]$, whether it has for each prime number p a p-adic integral zero follows immediately from Ax's theorem [**1**, p. 267], which says that the theory of the set of p-adic fields is decidable. So, by the equivalence (*) above, we are reduced to deciding whether $\mathbf{Z}[X, Y]/(f)$ can be discretely ordered. By Lemma 1 of §2, a necessary condition is that no integer > 1 becomes invertible in $\mathbf{Z}[X, Y]/(f)$. Suppose we have found this to be the case by the criterion mentioned in the remark following Lemma 2. Then, by Lemma 1, we have only to decide whether, for $x = X + (f), y = Y + (f)$, the fraction field $\mathbf{Q}(x, y)$ of $\mathbf{Z}[x, y]$ has a valuation ring V with real residue field such that $V \cap \mathbf{Q}[x, y] = \mathbf{Q}$. After a $\mathbf{Q}$-linear transformation of coordinates we reach the situation that $f(X, Y) = f'(X', Y')$ is monic in Y', where X', Y' are the $\mathbf{Q}$-linear

forms in X, Y acting as the new variables. Then

$$\mathbf{Q}[x, y] = \mathbf{Q}[x', y'] \simeq \mathbf{Q}[X', Y']/f'\mathbf{Q}[X', Y'],$$

x' is transcendental over $\mathbf{Q}$ and y' integral over $\mathbf{Q}[x']$. So by Proposition 3 a valuation ring V of $\mathbf{Q}(x, y)$ as described exists if and only if the following two conditions are satisfied:

(i) $\mathbf{Q}$ is integrally closed in $\mathbf{Q}[X, Y]/f\mathbf{Q}[X, Y] \simeq \mathbf{Q}[x, y]$,

(ii) there is only one valuation ring of $\mathbf{Q}(x', y')$ which extends the valuation ring $\mathbf{Q}[1/x']_{(1/x')}$ of $\mathbf{Q}(x')$, and this valuation ring has real residue class field.

Whether (i) holds can be checked by applying the decision method described in Lemma 4. The assumptions of Lemma 5 are fulfilled for $K = \mathbf{Q}(x')$ and $V = \mathbf{Q}[1/x']_{(1/x')}$, so Lemma 5 shows how to decide the first part of (ii). If this first part of (ii) holds, we use the following equivalences to verify the second part of (ii): there exists a valuation ring of $\mathbf{Q}(x', y')$ which extends $\mathbf{Q}[1/x']_{(1/x')}$ and has real residue class field $\Leftrightarrow \mathbf{Q}(x', y')$ has an ordering in which x' is infinite (in absolute value) $\Leftrightarrow \mathbf{R} \models \exists C\{(\forall r \geqslant C\ \exists s f'(r, s) = 0) \vee (\forall r \leqslant C\ \exists s\, f'(r, s) = 0)\}$.

The first equivalence follows from the well-known relation between nonarchimedean orderings and real places, see [7, §7], the second equivalence follows from quantifier elimination for $\mathbf{R}$. □

Let us summarize the purely mathematical content of the preceding proofs in the following proposition, which does not involve notions of recursion theory.

PROPOSITION. *Let $f = f(X, Y) \in \mathbf{Z}[X, Y]$ be absolutely irreducible and assume the coefficients of f have no common divisor and that the leading term of f, considered as a polynomial in Y, is of the form $a \cdot Y^d$, $a \in \mathbf{Z}$. Then f has a nonstandard (i.e. not both coordinates in $\mathbf{Z}$) zero in a discrete ordered ring if and only if the following conditions hold*:

(i) *the coefficients of f apart from the constant term $f(0, 0)$ have no common prime divisor*,

(ii) *f is irreducible as a polynomial in $\mathbf{Q}((1/X))[Y]$*,

(iii) $\mathbf{R} \models \exists C\{(\forall r \geqslant C\ \exists s\, f(r, s) = 0) \vee (\forall r \leqslant C\ \exists s\, f(r, s) = 0)\}$.

PROOF. Let $x = X + (f), y = Y + (f)$ in $\mathbf{Z}[X, Y]/(f)$. Then (i) expresses that no integer 1 is a unit in $\mathbf{Z}[x, y]$ (see remark following Lemma 2). (ii) means that there is only one valuation ring of $\mathbf{Q}(x, y)$ which extends the valuation ring $\mathbf{Q}[1/x]_{(1/x)}$ of $\mathbf{Q}(x)$: simply note that x is transcendental over $\mathbf{Q}$, that $\mathbf{Q}((1/X))$ is the completion of $\mathbf{Q}(X)$ w.r.t. the valuation whose valuation ring is $\mathbf{Q}[1/X]_{(1/X)}$, and apply [5, (2.12)]. (iii), in combination with (ii), says that this unique valuation ring has real residue class field: see the last part of the proof of the theorem.

Combining these observations with Lemma 1, Proposition 3 and the remark following Lemma 4 yields that (i), (ii) and (iii) together say that $\mathbf{Z}[x, y]$ has a discrete ordering; from this the proposition easily follows.

REMARKS. 1. Among the polynomials in $\mathbf{Z}[X, Y]$ the *absolutely irreducible* ones are, from the diophantine viewpoint, the interesting case; see the remark following Lemma 4. Dividing such a polynomial by the g.c.d. of its coefficients and carrying out a transformation of coordinates $X' = X + \lambda Y$, $Y' = Y$, λ a suitable integer,

makes the polynomial satisfy the assumptions of the proposition (w.r.t. the new variables X', Y').

2. To obtain necessary and sufficient conditions for f (satisfying the assumptions of the proposition) to have a nonstandard zero in a model of open induction, one has only to add the following extra clause:

(iv) *f has for each prime number p a p-adic integral zero.*

3. For applications to special cases, extensions of the preceding results and number theoretic interpretations of these, see [4].

ACKNOWLEDGEMENT. I thank Gerard Welters for an inspiring discussion in connection with Proposition 3.

REFERENCES

1. J. Ax, *The elementary theory of finite fields*, Ann. of Math. (2) **88** (1968), 239–271.

2. C. Chevalley, *Algebraic functions of one variable*, Math. Surveys, no. 6, Amer. Math. Soc., Providence, R. I., 1951.

3. L. van den Dries, *New decidable fields of algebraic numbers*, Proc. Amer. Math. Soc. **77** (1979), 251–256.

4. _____, *Some model theory and number theory for models of weak systems of arithmetic*, Proc. Karpacz 1979, Lecture Notes in Math. (to appear).

5. O. Endler, *Valuation theory*, Springer-Verlag, Berlin, Heidelberg, New York, 1972.

6. S. Lang, *Introduction to algebraic geometry*, Interscience, New York, 1958.

7. A. Prestel, *Lectures on formally real fields*, Monografias Mat., IMPA, Rio de Janeiro, 1975.

8. M. Rabin, *Computable algebra: general theory and theory of computable fields*, Trans. Amer. Math. Soc. **95** (1960), 341–360.

9. P. Ribenboim, *The Riemann-Roch theorem for algebraic curves*, Queen's Papers in Pure and Applied Math., no. 2, Kingston, Ont., 1965.

10. J. C. Shepherdson, *A non-standard model for a free variable fragment of number theory*, Bull. Acad. Polon. Sci. Sér. Sci. Math. Astronom. Phys. **12** (1964), 79–86.

11. B. L. van der Waerden, *Modern algebra*. I, Springer-Verlag, Berlin, 1930.

12. A. Wilkie, *Some results and problems on weak systems of arithmetic* (Logic Colloquium 1977), North-Holland, Amsterdam, 1978, pp. 285–296.

DEPARTMENT OF MATHEMATICS, UNIVERSITY OF UTRECHT, UTRECHT, THE NETHERLANDS

Current address: Department of Mathematics, Yale University, New Haven, Connecticut 06520