INFORMATION TO USERS

This manuscript has been reproduced from the microfilm master. UMI films the text directly from the original or copy submitted. Thus, some thesis and dissertation copies are in typewriter face, while others may be from any type of computer printer.

The quality of this reproduction is dependent upon the quality of the copy submitted. Broken or indistinct print, colored or poor quality illustrations and photographs, print bleedthrough, substandard margins, and improper alignment can adversely affect reproduction.

In the unlikely event that the author did not send UMI a complete manuscript and there are missing pages, these will be noted. Also, if unauthorized copyright material had to be removed, a note will indicate the deletion.

Oversize materials (e.g., maps, drawings, charts) are reproduced by sectioning the original, beginning at the upper left-hand corner and continuing from left to right in equal sections with small overlaps.

Photographs included in the original manuscript have been reproduced xerographically in this copy. Higher quality 6" x 9" black and white photographic prints are available for any photographs or illustrations appearing in this copy for an additional charge. Contact UMI directly to order.

Bell & Howell Information and Learning
300 North Zeeb Road, Ann Arbor, MI 48106-1346 USA
800-521-0600

Some Diophantine Properties of Ordered Polynomial Rings

by

Sidney Raffer

A dissertation submitted to the Graduate Faculty in Mathematics in partial fulfillment of the requirements for the degree of Doctor of Philosophy, The City University of New York

2000

This manuscript has been read and accepted for the Graduate Faculty in Mathematics in satisfaction of the dissertation requirement for the degree of Doctor of Philosophy.

4/19/2000 _____

Date

_____

Chair of Examining Committee

4/19/00 _____

Date

_____

Executive Officer

Joel Hamkins _____

Roman Kossak _____

Attila Mate _____

Supervisory Committee

THE CITY UNIVERSITY OF NEW YORK

Contents

1. Introduction

1.1. The Subject

This essay concerns *open induction domains*. These are ordered rings satisfying a limited form of the principle of mathematical induction. In an open induction domain A, the principle of induction is required to hold for finite unions of sets defined by systems of equations and inequalities made from polynomials with coefficients in A.

The study of this class of rings begins with Shepherdson [SHEP], where it is shown that a discretely ordered ring A is an open induction domain if and only if for every element r of the real closure of A, there is an element a of A such that $a \leq r < a + 1$. The latter condition means that an analogue of the integer part operator, with A in place of the standard integers, can be defined on the real closure of A.

There are natural open induction domains identified in [SHEP]. The ring S of Puiseux polynomials with integer constant terms and real algebraic coefficients is one example. (See Section 2.3 for the definition of Puiseux polynomial.) An important difference between open induction and more powerful theories, such as Peano arithmetic, is that the axioms of open induction are not the only source of information about open induction domains. Much can learned about open induction by studying specific open induction domains and their subrings.

We shall be concerned with two main problems.

(i) Which polynomials have a zero in at least one open induction domain? Does the set of all such polynomials have an algebraic or number-theroretic description? Is this set effectively enumerable? The latter question seems to have been raised for the first time by Wilke in [W]. Van den Dries [VD1] gave an effective procedure for determining if a polynomial in two variables has a zero in a model of open induction. His result does not seem to generalize to *inequalities* in two variables. The problem for equations in three variables remains open.

(ii) How strong a set of axioms for arithmetic can an open induction domain satisfy and still be given so that the ring operations are effectively computable? A sharp question along these lines was posed in [AML]: Are there effectively presentable open induction domains $A \neq \mathbb{Z}$ such that every system of polynomial equations and inequalities unsolvable in $\mathbb{Z}$ is unsolvable in A?

We shall consider problem **(i)** in a more general form: Which systems of equations and *inequalities* have a solution in an open induction domain? We have found a number-theoretic description of these systems, given in Theorem 3.7. We do not know if this description is effective. Our description is a consequence of an $\forall_1$ axiomatization of the class of discretely ordered rings that *extend* to a model of open induction. This is given in Theorem 3.4.

In an effort to approach problem **(ii)** we study the theory consisting of the axioms for open induction, together with all universal sentences in the language of $\{+, -, \cdot, <, 0, 1\}$

that are true in the ring of integers. Following [AML], we call this theory *Diophantine correct* open induction. We give an axiomatization that eliminates induction entirely. Specifically, we show that Diophantine correct open induction is axiomatized by all sentences σ of the form

$$\forall x_1 \ldots \forall x_n \exists y \phi(\bar{x}, y)$$

such that ϕ is a quantifier free formula and σ is true in $\mathbb{Z}$. This is Theorem 5.6.

Finally, we consider the class of ordered rings A with the property that every universal sentence in the language of $\{+, \cdot, 0, 1, <\}$ holding in $\mathbb{Z}$ holds in A. These are the *Diophantine correct* ordered rings. We would like to build Diophantine correct models of open induction as unions of chains of very simple Diophantine correct ordered rings. In order to do so, we have to be able to recognize these rings. In Theorems 6.4, 6.5 and the subsequent examples, we connect the problem of determining whether an ordered ring is Diophantine correct with a class of problems in Diophantine approximation.

1.2. Some Details.

In this section we give a more detailed summary of our problems and results. The reader who is on unfamiliar ground can proceed directly to Section 2 without loss of continuity.

Each linear combination over the reals of finitely many rational powers of a single variable t determines a function from $(0, \infty)$ into $\mathbb{R}$. Let $\wp$ be the set of all such functions.

$\wp$ forms a ring under pointwise addition and multiplication. We introduce an ordering on $\wp$ by defining a function to be *positive* if it takes on positive values for all sufficiently large t. (See Section 2.3.)

We are going to study subrings of $\wp$, especially finitely generated subrings, of two special types: Discretely ordered rings, and Diophantine correct rings. In order to build open induction domains with various properties, we would like to know how to recognize these types of rings. Typically, they will be generated by finitely many functions whose defining coefficients are given as algebraic functions of an algebraically independent tuple $\bar{r}$. We will want to know how the properties of the ring depend on $\bar{r}$.

If $f_1, f_2 \ldots \in \wp$, then $\mathbb{Z}[\bar{f}]$ will denote the ordered subring of $\wp$ generated by the f_i. The symbol $\theta(\bar{x})$ will denote a system of finitely many equations $p(\bar{x}) = 0$ and inequalities $q(\bar{x}) > 0$, where $p(\bar{x})$ and $q(\bar{x})$ are polynomials with integer coefficients, and $\bar{x}$ is a finite tuple of variables. Elements $\bar{a} \in \mathbb{Z}[\bar{f}]$ will satisfy θ iff each of the equations $p(\bar{a}(t)) = 0$ and inequalities $q(\bar{a}(t)) > 0$ hold for all sufficiently large t.

For some choices of $\bar{f}$, the ring $\mathbb{Z}[\bar{f}]$ will solve systems of equations and inequations ($p \neq 0$) with no integer solutions. In $\mathbb{Z}[t, \sqrt{2}t]$ for example, the generators satisfy $x \neq 0$ and $2x^2 = y^2$. We can avoid this situation, if we wish, by requiring that the functions f_i be algebraically independent over $\mathbb{Q}$. The ring $\mathbb{Z}[\bar{f}]$ will then be a polynomial ring over $\mathbb{Z}$. In any such ring, a system of equations and inequations is solvable iff it has solutions in integers.

Even if $\mathbb{Z}[\bar{f}]$ does not disagree with $\mathbb{Z}$ with respect to the solvability of equations, it can do so with respect to the solvability of inequalities. For example, $\mathbb{Z}[\bar{f}]$ can be densely ordered. This will be the case if $\mathbb{Z}[\bar{f}]$ contains elements x and y such that $x < y < x+1$. Rings in which these inequalities are unsolvable are said to be *discretely ordered.* It is perhaps surprising that a discretely ordered ring which solves only those systems of equations and inequations with integer solutions can still solve systems of inequalities with no integer solutions. But this is so. For example, the ring $A = \mathbb{Z}[t, \alpha t - \frac{r}{t^2}]$, where $\alpha \in \mathbb{R}$ is the real cube root of 2 and $r \in \mathbb{R}$ is transcendental, is a discretely ordered polynomial ring in two variables. Any system of equations and inequations with a solution in A has an integer solution. In Example 4 following Theorem 6.5, we prove that there are systems of inequalities solvable in A but not in $\mathbb{Z}$. Specifically, A violates Roth's theorem.

Diophantine correct rings can differ from $\mathbb{Z}$ in very simple ways. For example, $\mathbb{Z}[t]$ is Diophantine correct, but $t \in \mathbb{Z}[t]$ is neither even nor odd. This does not cause any system θ to conflict with $\mathbb{Z}$. The reason that t is neither even or odd is that a certian element, that behaves like "$\lfloor \frac{t}{2} \rfloor$", is missing from the ring. We can add such an element: The ring $\mathbb{Z}[\frac{t}{2}]$ is a Diophantine correct extension of $\mathbb{Z}[t]$ in which t is even.

In fact all of the differences between $\mathbb{Z}[t]$ and $\mathbb{Z}$ expressible in the first order language $\{+, -, \cdot, 0, 1, <\}$ of ordered rings are correctable in the sense that they can be removed by adjoining more elements to the ring. $\mathbb{Z}[\bar{f}]$, in other words, extends to an ordered

ring that satisfies all first order sentences true in the ordered ring $\mathbb{Z}$.

This extension cannot take place inside $\wp$ since, e.g., the elements of $\wp$ are polynomially related. This leads to the question: Which first-order discrepancies between $\mathbb{Z}[t]$ and $\mathbb{Z}$ can be removed by extending $\mathbb{Z}[t]$ to a larger Diophantine correct subring of $\wp$? More generally, what subtheories of true arithmetic can a subring of $\wp$ satisfy?

In [*BO*], *normal* open induction domains were found as subrings of $\wp$. An integral domain A is "normal" if every element the quotient field of A satisfying a monic polynomial with coefficients in A is an element of A. For example, $\mathbb{Z}$ is a normal open induction domain. Normal open induction can be axiomatized by adding an infinite set of $\forall_1$ sentences in the language of rings to the axioms of open induction. Normality implies, for example, that A cannot have two elements whose ratio is $\sqrt{2}$.

We do not know whether $\wp$ includes a Diophantine correct model of open induction other than $\mathbb{Z}$. Nor do we know whether the models given in [BO] are Diophantine correct. The idea that they might be was suggested to the author by M. Otero, who attributed the suggestion to Wilkie.

As we mentioned, the problem with $\mathbb{Z}[t]$, that t is neither even nor odd, can be fixed by extending it to $\mathbb{Z}[\frac{t}{2}]$, which is also Diophantine correct. Observe that the element $\frac{t}{2}$ of $\wp$ is not a finite distance from any element of $\mathbb{Z}[t]$. For every element of $\wp$ algebraic over $\mathbb{Z}[t]$ but not a finite distance from $\mathbb{Z}[t]$, one can construct a statement true in $\mathbb{Z}$ but not in $\mathbb{Z}[t]$. For example, $\sqrt{2}t$ is such an element of $\wp$. We can write the inequalities

$y \leq \sqrt{2}x < y + 1$ as a system $\theta(x, y)$ using polynomials with integer coefficients. The sentence $\forall x \exists y \theta(x, y)$ is true in $\mathbb{Z}$ but false in $\mathbb{Z}[t]$.

In this case, we know of a Diophantine correct extension of $\mathbb{Z}[t]$ contained in $\wp$ in which $\forall x \exists y \theta(x, y)$ becomes true, namely $\mathbb{Z}[t, \sqrt{2}t - r]$, for any r transcendental over $\mathbb{Q}$. (See Example 1 following Theorem 6.5.) In [BO] open induction domains are constructed by carrying out this kind of extension repeatedly. We would like to know when such extensions preserve Diophantine correctness.

We shall give a method for translating each question "Is $\mathbb{Z}[f]$ Diophantine correct?" into a problem in number theory. Here are some sample translations. (The assertions made here are proved in Section 6.)

(i) Let S be the set of all values of the quadratic form

$$x(2^{\frac{1}{3}}x - y)$$

as x and y range over $\mathbb{Z}$. Then $\mathbb{Z}[t, 2^{\frac{1}{3}}t - \frac{r}{t}]$, with r transcendental, is Diophantine correct iff r is a limit point of S.

Little is known about the distribution of the elements of S. In particular, S is not known to have positive elements in every neighborhood of 0. See [LDA II.2, page 25].

(ii) Let S be the closure, in $\mathbb{R}$, of the set of all real numbers of the form $\left|\frac{n^3 - m^2}{\sqrt{n}}\right|$, as n and m range over the positive integers. The ring $\mathbb{Z}[t^2, t^3 - \frac{r}{2t^2}]$, where r is a real

transcendental, is Diophantine correct iff $r \in S$.

Hall's conjecture [RI, Section C2, page 249] asserts that the nonzero values of $\left|\frac{n^3-m^2}{\sqrt{n}}\right|$, where n and m range over the positive integers, are all greater than some fixed positive constant c.

2. Preliminaries.

In this section we give a number of definitions and theorems that will be used in subsequent sections. All of the definitions given here are standard. All of the theorems are known, and none are due to the author.

2.1. Logic.

We shall be concerned exclusively with first-order languages in which equality is a logical symbol. Lower-case Greek letters will denote formulas. We shall use over-bars, as in $\bar{x}$, to denote finite tuples of objects $x_1, x_2 \ldots$. When the intention is clear, we shall say $\bar{x} \in S$ when we mean that $\bar{x}$ is a tuple of elements of the set S.

If ϕ is a formula and $\bar{x}$ is a tuple of variables, we shall use the notation $\phi(\bar{x})$ to indicate that the free variables of ϕ appear among the x_i. If A is a structure and $\phi(\bar{x})$ is a formula in the language of A, then

$$A \models \phi(\bar{a})$$

means that ϕ, with $a_1, a_2 \ldots$ assigned to $x_1, x_2 \ldots$ respectively, is true in A.

A formula is *open* if it has no quantifiers. A formula is of type $\forall_1$ if it consists of a

string of universal quantifiers followed by an open formula. A formula is of type $\exists_1$ if it consists of a string of existential quantifiers followed by an open formula. A formula is of type $\forall_2$ if it consists of a string of universal quantifiers followed by an $\exists_1$ formula.

A *theory* is a set of sentences. If T' is another theory in the same language as T and if every model of T is a model of T', we shall write $T \Rightarrow T'$. If ϕ is a sentence in the language of T and ϕ is provable from T, we write $T \vdash \phi$. We will not define provability here, since, in view of the Godel's Completeness Theorem [SH, Section 4.2], one can restate the meaning of this symbol in terms of models: $T \vdash \phi$ if and only if every model of T is also a model of ϕ.

If T is a theory, then $\forall_1(T)$ denotes the set of $\forall_1$ sentences ϕ in the language of T such that $T \vdash \phi$; similarly for $\exists_1$ and $\forall_2$.

We shall say that T is an $\forall_1$ theory if $\forall_1(T) \Rightarrow T$; similarly for $\exists_1$, etc.

A theory T *admits elimination of quantifiers* if for every formula $\phi(\bar{x})$ there is an open formula $\psi(\bar{x})$ such that $T \vdash \forall\bar{x}(\phi(\bar{x}) \leftrightarrow \psi(\bar{x}))$.

If A is a structure and f is a function symbol in the language of A then f^A will denote the corresponding function of A; similarly for relation and constant symbols. If $\phi(x_1 \ldots x_n)$ is a formula in the language of A, we will use ϕ^A to denote the subset of A^n defined by ϕ. Note that ϕ^A depends on the specification of $\bar{x}$.

When the meaning is clear, we will use the same symbol for a structure and its domain.

If A is a structure, and if the structure A' is obtained from A by adding new functions, relations, or distinguished elements, we shall say that A' is an *expansion* of A, and that A is a *reduct* of A'.

If A is a structure, $f : A^n \to A$ is a function, and $\bar{r} \in A$, then f is *definable in A from parameters $\bar{r}$* if there is a formula $\phi(\bar{u}, x_1 \ldots x_n, y)$ in the language of A such that for all $a_1 \ldots a_n, b \in A$,

$$A \models \phi(\bar{r}, \bar{a}, b) \text{ ifft } f(\bar{a}) = b.$$

If A is a structure and $\bar{r} \in A$, then a subset S of A^n is *definable in A from $\bar{r}$* if there is a formula $\phi(\bar{u}, x_1 \ldots x_n)$ in the language of A, such that for all $a_1 \ldots a_n \in A$,

$$A \models \phi(\bar{r}, \bar{a}) \text{ iff } \bar{a} \in S.$$

If A is a structure for a language L, then $Th(A)$ will denote the set of all sentences of L true in A. $\forall_1(A)$ will denote the set of all $\forall_1$ sentences of L true in A, and similarly for $\exists_1$, etc.

A theory is *satisfiable* if it has a model. A theory T is *finitely satisfiable* if every finite subset of T has a model. A theory is *consistent* if no contradiction ($\phi \wedge \neg\phi$ for a sentence ϕ, say) can be proved from it. As mentioned above, we will not discuss the concept of provability here. However, as satisfiability and consistency are equivalent in view of Godel's Completeness Theorem [SH Section 4.2], the two terms will be used

interchangeably.

The *Compactness Theorem* asserts that a finitely satisfiable theory is satisfiable. This was first proved by Gödel. See e.g. [HO, Theorem 6.1.1].

If A is a structure, we define a set of formulas $D(A)$, the *diagram* of A, as follows: Add to the language of A a new constant symbol c_a for every element a of A. Expand A to a structure A' for the new language by putting $c_a^{A'} = a$. Let $D(A)$ be all open sentences of $Th(A')$.

The method of diagrams in model theory goes back at least to Abraham Robinson's 1949 Ph.D. thesis. Hodges [HO, chapter 1, page 22] traces it to Wittgenstein's *Tractatus logico-philosophicus*. The proofs of following three propositions are well known examples of this method.

Proposition 2.1. *Let A be a structure, and T a theory in the language of A. Then the following are equivalent:*

(1) $A \models \forall_1(T)$.

(2) $T \cup D(A)$ *is consistent.*

(3) A *is a substructure of a model of* T.

Sketch of Proof. For (1) $\Rightarrow$ (2), assume (2) is false. Use the fact that an inconsistency in $T \cup D(A)$ would mean the existence of a sentence $\neg\psi$, where ψ is a conjunction of

sentences from $D(A)$, such that $\neg\psi$ is satisfied by the expansion of every model of T to the language of $D(A)$. Think of the diagram constants in ψ as variables and take the universal closure, to obtain a sentence of $\forall_1(T)$ inconsistent with $D(A)$. This contradicts (1).

For (2) $\Rightarrow$ (3), let $B \models T \cup D(A)$. Then A is embedded in B via the map $c^A \mapsto c^B$, where c is an arbitrary diagram constant of A. ■

Proposition 2.2. *T is an $\forall_1$ theory iff every substructure of a model of T is a model of T.*

Sketch of Proof. For the *if* direction, suppose T is not $\forall_1$. Choose $\psi \in T$ such that $\forall_1(T) + \neg\psi$ has a model A. By the last Proposition, A extends to a model of T. Contradiction. ■

For complete proofs, see [CHK Theorem 3.2.2, page 124], and [HO Lemma 8.5.1, page 391].

If A is a structure and S is a subset of the domain of A, then $\langle S \rangle_A$ will denote the intersection of all substructures of A including S. A is *finitely generated* if for some finite subset S of A, we have $\langle S \rangle_A = A$. We shall need:

Proposition 2.3. *Let T be an $\forall_1$ theory, and A a structure for the language of T. Then A satisfies T iff every finitely generated substructure of A satisfies T.* ■

2.2. The p-adic Integers

The definition of p-adic integers and all results about them in this section are due to K. Hensel.

Let p be a prime number. There are unique ring homomorphisms $h_n : \mathbb{Z}/p^n\mathbb{Z} \to \mathbb{Z}/p^{n-1}\mathbb{Z}$, for each $n > 1$. The *ring of p-adic integers*, $\mathbb{Z}_p$, is defined to be the subring of the product ring $\prod_{n\geq 1} \mathbb{Z}/p^n\mathbb{Z}$ consisting of all sequences a such that for $n > 1$,

$$h_n(a_n) = a_{n-1}.$$

The fraction field of $\mathbb{Z}_p$, called the *field of p-adic numbers*, is denoted by $\mathbb{Q}_p$.

Each ring $\mathbb{Z}_p$ contains an isomorphic copy of $\mathbb{Z}$, namely, the subring of eventually constant sequences.

Proposition 2.4. *The ring $\mathbb{Z}_p$ has exactly one maximal ideal. It is generated by p, and consists precisely of all non-units of $\mathbb{Z}_p$.*

Sketch of Proof. The ideal of multiples of p in $\mathbb{Z}_p$ consists of all elements a such that $a_1 = 0$ in $\mathbb{Z}/p\mathbb{Z}$. To prove that all non-units have this property, we choose $a \in \mathbb{Z}_p$ such that $a_1 \neq 0$, and show that a is a unit. To prove the latter, choose $b_1 \in \mathbb{Z}/p\mathbb{Z}$ such that $a_1 b_1 = 1$. Prove inductively the existence of $b_n \in \mathbb{Z}/p^n\mathbb{Z}$ such that $a_n b_n = 1$ and $h_n(b_n) = b_{n-1}$, using the fact that $h_n(a_n) = a_{n-1}$. Then b will be the required inverse of a. ■

For a proof, see [SE Section 1.2 Proposition 2].

Give each ring $\mathbb{Z}/p^n\mathbb{Z}$ the discrete topology, and give $\prod_{n\geq 1} \mathbb{Z}/p^n\mathbb{Z}$ the product topology. $\mathbb{Z}_p$ then acquires the subspace topology. One easily checks that $\mathbb{Z}_p$ is closed in $\prod_{n\geq 1} \mathbb{Z}/p^n\mathbb{Z}$. Since the latter is compact, so is $\mathbb{Z}_p$.

To decode this: Two elements of $\mathbb{Z}_p$ are close if they agree, as sequences, on a long initial segment. A basic open subset of $\mathbb{Z}_p$ consists of all elements that have a given initial segment. $\mathbb{Z}_p$ is closed in $\prod_{n\geq 1} \mathbb{Z}/p^n\mathbb{Z}$ because $a \in \prod_{n\geq 1} \mathbb{Z}/p^n\mathbb{Z}$ satisfies the condition $h_n(a_n) = a_{n-1}$ iff every initial segment of a satisfies that condition.

Note that addition and multiplication are continuous in $\mathbb{Z}_p$. This merely says that if a and a' agree on a long initial segment, and if b and b' agree on a long initial segment, then so do $a + b$ and $a' + b'$, and so do ab and $a'b'$.

We shall need

Proposition 2.5. *$\mathbb{Z}$ is dense in $\mathbb{Z}_p$.*

Proof. The statement of the proposition means that every open subset of $\mathbb{Z}_p$ contains an element of $\mathbb{Z}$. It suffices to prove this for basic open subsets, each of which consists of all elements of $\mathbb{Z}_p$ with some given initial segment $\alpha_1 \ldots \alpha_n$. But the element a of $\mathbb{Z}_p$ such that $a_i = \alpha_i$ for $i = 1 \ldots n$, and such that $a_i = \alpha_n$ for $i > n$, represents an element of $\mathbb{Z}$. ■

Finally, we mention the p-adic metric. Define the function $\phi_p : \mathbb{Z}_p \to \mathbb{R}$ as follows: $\phi_p(0) = 0$, and for non-zero $a \in \mathbb{Z}_p$, $\phi_p(a) = p^{-m}$, where m is the least positive integer

such that $a_m \neq 0$. The function ϕ_p measures the number of zeros a p-adic number a "begins with", which is the same as the power of p that divides a. The function $\phi_p(x-y)$ gives a metric on $\mathbb{Q}_p$ that defines the p-adic topology described above. For a discussion of this see [SE Section 1.2 Proposition 3].

2.3. Ordered Rings

Rings are structures of type $\{+, -, \cdot, 0, 1\}$ satisfying the usual axioms [LA]. Note that our rings have unit elements. A ring is an *integral domain* if it satisfies

$$\forall x, y(xy = 0 \rightarrow x = 0 \vee y = 0).$$

An *Ordered Ring* A is a structure of type $\{+, -, \cdot, 0, 1, <\}$ satisfying the axioms for a commutative ring, and additional axioms for $<$ that we describe, after [PF], as follows: Let

$$P = \{a \in A : a >^A 0\},$$

and let

$$-P = \{-a : a \in P\}.$$

For A to be an ordered ring, we require that P be closed under $+^A$ and $\cdot^A$, that $P \cap -P = \emptyset$, and that $P \cup -P \cup \{0^A\} = A$.

The above conditions imply that $<^A$ is a total ordering of the domain of A that is

compatible with the ring operations in the usual way.

It is straightforward to write down $\forall_1$ sentences that formulate each of the above conditions. We shall refer to this set of $\forall_1$ sentences as OR, the theory of ordered rings.

The significance of our definition of ordered ring is given by the following, first proved by Artin and Schreier [AS].

Proposition 2.6. *Let A be an integral domain. Then A has an expansion to an ordered ring iff 0^A is not a sum of non-zero squares of elements of A.*

Sketch of Proof. Let S be the set of all $P \subseteq A$ such that P is closed under $+^A$ and $\cdot^A$ and $-1 \notin P$. Then S is not empty since the set of sums of squares is an element of S. By Zorn's Lemma, take a maximal element P of S. Show that for P maximal, the remaining properties hold: $P \cap -P = \emptyset$, and $P \cup -P \cup \{0^A\} = A$. ■

For a complete proof, see [PF, Chapter 6, Corollary 1.6].

We shall often make reference to ordered ring $\wp$ defined as follows: The domain of $\wp$ is the set of all functions from $(0, \infty)$ into $\mathbb{R}$ of the form $t \mapsto \sum_{i=1}^{l} c_i t^{q_i}$, where $c_i \in \mathbb{R}$, and $q_1, \ldots, q_l$ are rational numbers. Addition and multiplication of elements of $\wp$ is defined pointwise. The positive elements of $\wp$ are those functions f such that $f(t)$ is positive for all sufficiently large t.

It is simple to check that $\wp$ is a ring. As for the ordering, we shall verify that for every function $f \in \wp$ different from 0, either f or $-f$ is positive.

Since $f \neq 0$, we can write $f(t)$ in the form $\sum_{i=1}^{l} c_i t^{q_i}$, with $q_1 < q_2 < \ldots < q_l$, and $c_l \neq 0$. Then $\sum_{i=1}^{l} c_i t^{q_i - q_l}$ tends to c_l as t tends to infinity. Since

$$f(t) = t^{q_l} \sum_{i=1}^{l} c_i t^{q_i - q_l},$$

it follows that $f(t)$ is either positive for large t, or negative for large t, depending on the sign of c_l. Therefore either f or $-f$ is positive.

If $\bar{f} \in \wp$, then $\mathbb{Z}[\bar{f}]$ will denote the substructure of $\wp$ generated by the f_i. This is again an ordered ring, consisting of all functions $g(\bar{f}(t))$ such that g is a polynomial with integer coefficients.

A *Puiseux polynomial* is an element of $\wp$ of the form $t \mapsto \sum_{i=1}^{l} c_i t^{q_i}$, where the q_i ar non-negative. It is more customary to think of Puiseux polynomials as formal objects rather than functions. For our purposes it will be harmless to blur this distinction, and we shall do so. The Puiseux polynomials form a subring of $\wp$.

A *discretely ordered ring* is an ordered ring satisfying the additional axiom

$$\forall x(\neg 0 < x < 1).$$

This is the same as requiring that an ordered ring satisfy

$$\forall x, y(\neg x < y < x + 1).$$

We shall refer to the theory of discretely ordered rings as *DOR*. Note that *DOR* is an $\forall_1$ theory.

A discretely ordered ring A is *p-adically correct* if for every prime p there is a homomorphism from A into $\mathbb{Z}_p$. Theorem 3.1 and proposition 2.1 immediately imply that this class is $\forall_1$ axiomatizable.

An ordered ring is *Diophantine correct* if it satisfies the theory $\forall_1(\mathbb{Z})$, where we regard $\mathbb{Z}$ here as an ordered ring.

2.4. Real Closed Fields.

An *Ordered Field* is an ordered ring whose reduct to $\{+, -, \cdot, 0, 1\}$ is a field.

A field is *formally real*, if zero is not a sum of non-zero squares.

A *Real Closed Field* is a formally real field F such that no formally real field E properly including F is algebraic over F. The definition of real closed field and the following three theorems are from Artin and Schreier [AS].

Theorem 2.7. *Let F be a formally real field. Then F is real closed iff*

(1) *Every element of F or its negative is a square in F, and*

(2) *Every one-variable polynomial of odd degree with coefficients in F has a root in F.* ■

It follows that the class of real closed fields is first-order axiomatizable.

For a proof of the theorem, see [LA, Chapter XI, Section 2, Proposition 2.1, and Theorem 2.2].

Every real closed field F has one and only one expansion $(F, <)$ to an ordered field, obtained by taking P (in the definition of ordered ring) to be the set of squares of all non-zero elements. When F is a real closed field, and there is no danger of confusion, we shall not distinguish between F and $(F, <)$.

If A is an ordered ring, then a *real closure* of A is an ordered field F extending A such that F is real closed, and every element of F is algebraic over A. The existence of a real closure of an ordered ring follows easily from Zorn's Lemma. The following uniqueness result is deeper.

Theorem 2.8. *Let A be an ordered ring. Let F and F' be real closures of A. Then there is an isomorphism of ordered rings $h : F \to F'$ fixing every element of A.* ■

In light of the last Theorem, we shall speak of "the" real closure F of an ordered ring A when we care only about the isomorphism type of the pair (A, F).

We shall use the abbreviation *RCF* for the theory of real closed fields.

Theorem 2.9. *RCF is complete and admits elimination of quantifiers.* ■

The first assertion follows from the second, by showing that all quantifier-free sentences are decidable in *RCF*. The theorem is due to Tarski. For a proof, see [MMP, Chapter 1, Section 2, Theorem 2.3 and Corollary 2.4].

We shall make repeated use of

Theorem 2.10. *(Thom's Lemma.) Let F be a real closed field. Let $f_i(t)$ $(i = 1 \ldots n)$ be polynomials in the variable t with coefficients in F. Suppose that for all i there is some j such that f_j is the formal derivative of f_i with respect to t. Let $\square_i$ denote any one of the symbols $>$, $=$, or $<$. Then the set of $t \in F$ such that*

$$\bigwedge_i f_i(t) \square_i 0$$

is either empty or a singleton or an open interval with endpoints in $F \cup \{\pm\infty\}$.

The formal derivative of a polynomial $\sum_{i=0}^{n} c_i t^i$ in the variable t with coefficients c_i in an arbitrary ring is the polynomial $\sum_{i=1}^{n} i c_i t^{i-1}$.

Sketch of Proof. By the completeness of RCF it suffices to prove the theorem for $\mathbb{R}$. The proof is by induction on n. If $n = 1$ then f_1 is the zero polynomial, and the Lemma follows. Suppose $n > 1$. We can assume f_n has maximal degree. If f_n has degree 1 then each formula $f_i(t) \square_i 0$ defines either the empty set, a singleton or a half-line, and the intersection of such sets satisfies the requirements of the lemma. Assume f_n has degree greater than 1. By induction the polynomials $f_1 \ldots f_{n-1}$ satisfy the conclusion of the Lemma. If the set S defined by $\bigwedge_{i<n} f_i(t) \square_i 0$ is either empty or a singleton, then so will be $\bigwedge_{i \leq n} f_i(t) \square_i 0$. Suppose S is neither empty nor a singleton. Since f_n' is one of the f_i and f_n has degree greater than 1, it follows that f_n' has no root in S. f_n is therefore

strictly increasing or strictly decreasing on S. If f_n does not change sign on S, then the set defined by $\bigwedge_{i\leq n} f_i(t)\square_i 0$ will either be empty, or the same as the set defined by $\bigwedge_{i<n} f_i(t)\square_i 0$. If f_n does change sign on S, then it will have a single root $r \in S$. In this case, $\bigwedge_{i\leq n} f_i(t)\square_i 0$ will define either $\{r\}$, or an interval with one endpoint r and the other an endpoint of S. ■

For details see [VD3, Chapter 2, Lemma 1.2].

From Thom's Lemma we shall derive the following well-known fact:

Proposition 2.11. *Let F be a real closed field. Let $\bar{a} \in F$. Suppose $r \in F$ is algebraic over the field $\mathbb{Q}(\bar{a})$. Then there is an open formula $\phi(\bar{x}, y)$ such that $\phi(\bar{a}, y)$ defines r in F.*

Proof. Since r is algebraic over $\mathbb{Q}(\bar{a})$, we can choose a polynomial $f(\bar{x}, y)$ with integer coefficients such that $f(\bar{a}, r) = 0$, but $f(\bar{a}, y)$ is not the zero polynomial. Let $f'(\bar{x}, y)$ be the formal derivative of $f(\bar{x}, y)$ with respect to the variable y. Let ϕ_1 be the formula $f(\bar{x}, y) = 0$. Consider the disjuction $\delta(\bar{x}, y)$ defined as follows:

$$(\phi_1(\bar{x}, y) \wedge f'(\bar{x}, y) = 0) \vee (\phi_1(\bar{x}, y) \wedge f'(\bar{x}, y) > 0) \vee (\phi_1(\bar{x}, y) \wedge f'(\bar{x}, y) < 0). \quad (2.1)$$

In F, $\delta(\bar{a}, y)$ defines the same subset as $\phi_1(\bar{a}, y)$. Let $\phi_2(\bar{x}, y)$ be any one of the three disjuncts of $\delta(\bar{x}, y)$, chosen so that $\phi_2(\bar{a}, r)$ holds in F. Define ϕ_3 from ϕ_2, ϕ_4 from ϕ_3, etc, in a similar way, differentiating f i times for the definition of ϕ_{i+1}. Then the conjuncts

of $\phi_n(\bar{a}, y)$, where n is the y-degree of f, give a sequence of polynomial equations and inequalities that is closed under formal derivatives, in the sense of the hypotheses of Thom's Lemma. It follows from Thom's Lemma that the set S defined by $\phi_n(\bar{a}, y)$ in $\mathbb{R}$ is either empty, a singleton, or an open interval. Our construction puts $r \in S$. Since the conjuncts of ϕ contain at least one non-trivial equation, it follows that $S = \{r\}$. Therefore ϕ_n is the required formula ϕ. ■

2.5. Open Induction.

An Open Induction Domain is a discretely ordered ring satisfying all sentences

$$\forall \bar{y}\ ((\phi(0, \bar{y}) \wedge \forall x \geq 0\ (\phi(x, \bar{y}) \rightarrow \phi(x+1, \bar{y}))) \rightarrow \forall z \geq 0\ \phi(z, \bar{y})) \tag{2.2}$$

such that $\phi(x, \bar{y})$ is an open formula. We shall use the abbreviation OI for the theory, in the language of ordered rings, consisting of DOR plus the above sentences.

Theorem 2.12. *(Division Theorem) If A is an Open Induction Domain, then the following sentence is true in A :*

$$\forall y > 0\ \forall x\ \exists! q, r\ (x = yq + r \wedge 0 \leq r < y).$$

Proof. Let $y \in A$ be positive. We prove first that for every $x \geq 0$ there is some $q \in A$ such that

$$yq \leq x < y(q+1). \tag{2.3}$$

Otherwise, assume $x \geq 0$ and there is no such q. Let S be the subset of A defined by the following formula $\sigma(q)$:

$$q \geq 0 \wedge yq \leq x.$$

Clearly $0 \in S$. If $q \in S$ then by assumption

$$A \models \neg\, yq \leq x < y(q+1).$$

Therefore $y(q+1) \leq x$. Hence $q+1 \in S$.

We have shown that the open formula $\sigma(q)$ satisfies the hypotheses of a sentence of the form (2.2). Since A is an open induction domain, S contains all non-negative elements of A. But, from our choice of S, $x+1 \notin A$. Contradiction. This proves (2.3).

Next, we define q and r and prove they are unique.

Given $y > 0$ and $x \geq 0$, choose q such that

$$yq \leq x < y(q+1)). \tag{2.4}$$

Put $r = x - yq$. Then $x = yq + r \wedge 0 \leq r < y$. Suppose also $x = yq' + r' \wedge 0 \leq r' < y$. Then

$$yq' \leq x < y(q' + 1). \tag{2.5}$$

Since A is an integral domain, (2.4) and (2.5) imply that

$$q < q' + 1 \wedge q' < q + 1.$$

Thus

$$q < q' + 1 < q + 2.$$

Since A is discretely ordered, $q' + 1 = q + 1$. Hence $q' = q$ and $r' = r$.

Finally, if $x < 0$, carry out the same argument with $-x$. Then write $-x = yq + r$ in the form $x = y(-q - 1) + (y - r)$. ■

Theorem 2.13. *If A is an open induction domain, and $n \in \mathbb{Z}$ is a positive integer, then the quotient ring A/nA is isomorphic to $\mathbb{Z}/n\mathbb{Z}$.*

Proof. One need only show that A/nA has n elements. The last theorem implies that every $x \in A$ has the form $nq + r$ for exactly one $r \in [0, n)$. ■

We shall need the following theorem due to Shepherdson.

Theorem 2.14. *Suppose A is a discretely ordered ring, with real closure F. Then $A \models OI$ iff every element of F is a finite distance from some element of A.*

Sketch of proof. Suppose $A \models OI$. Suppose, e.g., $r \in F$ is positive. For some $\bar{a} \in A$, r is definable in F by a an open formula $\theta(\bar{a}, x)$. Eliminate over RCF the quantifier in $\exists z(\theta(\bar{a}, z) \wedge x \leq z)$, to obtain an open formula $\psi(\bar{a}, x)$. Argue that if $\psi(\bar{a}, x)$ has no greatest element in A, then the set of non-negative elements of A satisfying $\psi(\bar{a}, x)$ is inductive. Then argue that there are non-negative elements of A that do not satisfy $\psi(\bar{a}, x)$. Conclude that there is a largest element in A satisfying $\psi(\bar{a}, x)$. This element will be a finite distance from r.

For the other direction, one shows that every subset of A definable by an open formula is a finite union of sets $(r, r') \cap A$, where (r, r') is an interval in F. For sets of this form the induction axioms can be directly verified. ■

For a proof, see [VD2, Section 3, Theorem 3.1].

2.6. Valuation Rings

Let F be a field. A subring V of F is a *valuation ring* if for every nonzero element $x \in F$, either x or x^{-1} is in V. A valuation ring has a unique maximal ideal I, consisting of all the non-units of V. V is said to be *real* if the field V/I is formally real. V/I is called the *residue field* of V.

If F is an ordered ring and $S \subseteq F$ is a valuation ring, then S is *convex in* F if any element of F between two elements of S is in S.

The following theorem was proved by Baer 1927, and Krull 1932.

Theorem 2.15. *Suppose F is a field and $V \subseteq F$ is a real valuation ring. Then F has an expansion to an ordered field such that V is convex in F.*

Sketch of proof. The field V/I can be ordered, since it is formally real. Fix one such ordering. Since F is the fraction field of V, any ordering on V extends uniquely to an ordering on F. We construct an ordering on V whose extension to F makes V convex.

First, show that an ordering of V that makes I a convex subset of V extends to an ordering on F making V convex. (Use the definition of valuation ring.)

Next, find an ordering on V so that I is convex: Start with the set P_0 of all linear combinations

$$\sum v_i^2 a_i$$

such that $0 \neq v_i \in V$, and such that $a \in V$ has a positive image in V/I. P_0 will have all the properties required of an ordering on V, except perhaps that $V \neq P_0 \cup -P_0 \cup \{0\}$. Such a subset is called a *precone*. Extend P_0 to a maximal precone P included in V via Zorn's Lemma, and argue that maximal precones have the missing property. P will then give an ordering of V.

If $x \in P$ then the image of x in V/I cannot be negative. Otherwise, by our choice of P_0, $-x \in P_0$. This is impossible since P is an ordering and $P_0 \subseteq P$.

Thus the projection homomorphism $h : V \to V/I$ preserves the relation $\leq$. It follows (using only that V and V/I are ordered rings and the projection map h preserves $\leq$)

that I is a convex subset of V. ■

For a complete proof see [PS, III.2, Satz 10].

3. An Axiomatization of $\forall_1(OI)$.

Following Shepherdson's discovery of recursively presentable non-standard models of Open Induction, Wilkie, Van den Dries and others [W], [VD1], [VD2], [MM], [SM], studied techniques for constructing such models. They considered the following situation: One is given a finitely generated commutative ring extension $A = \mathbb{Z}[a_1 \ldots a_n]$ of $\mathbb{Z}$. Let I be the ideal of all polynomials in $\mathbb{Z}[x_1 \ldots x_n]$ that vanish at $\bar{a}$. Then $\mathbb{Z}[\bar{a}]$ is isomorphic to the quotient ring $\mathbb{Z}[\bar{x}]/I$. By the Hilbert Basis Theorem [LA, Chapter IV, Section 4, Theorem 4.1] I is finitely generated. Thus A can be specified by giving a finite number of polynomials $f_1 \ldots f_m$ that generate I. One would like to know, given $\bar{f}$, whether there is an ordering on A that makes A into an ordered subring of some open induction domain. Can this be determined effectively? At issue is how to determine whether the sentence

$$\exists \bar{x} \bigwedge_i f_i(\bar{x}) = 0$$

is consistent with OI. We can make this determination if we know which sentences

$$\forall \bar{x} \bigwedge_i f_i(\bar{x}) \neq 0$$

belong to the theory $\forall_1(OI)$. This leads to the more general question,

$$\text{"Is } \forall_1(OI) \text{ a recursive theory?"} \tag{3.1}$$

This can be considered a variation on Hilbert's Tenth Problem: The latter asks, in effect, whether $\forall_1(T)$ is a recursive theory, where T is the theory of the ordered ring $\mathbb{Z}$.

The most important thing we know about $\forall_1(OI)$ was discovered by Wilkie [W]. Let us say that a "$\mathbb{Z}-$Ring" is a Discretely Ordered Ring satisfying all sentences

$$\forall x \exists y \, (ny \leq x < n(y+1)),$$

such that n is a positive integer. Wilkie [W] proposed this definition, and he proved

Theorem 3.1. *A Discretely Ordered Ring A extends to a model of Open Induction if and only if any one of the following conditions hold:*

(1) *A extends to a $\mathbb{Z}-$Ring.*

(2) *For each positive integer n, and each prime $p \in \mathbb{Z}$, there is a ring homomorphism from A onto the ring $\mathbb{Z}/p^n\mathbb{Z}$.*

(3) *For each prime p, there is a ring homomorphism from A into the p-adic integers $\mathbb{Z}_p$.*

Sketch of Proof. Suppose A extends to a model B of OI. Then Theorem 2.12 implies that B is itself a $\mathbb{Z}$-Ring. This proves (1). (1) $\Rightarrow$(2) follows from the axioms for $\mathbb{Z}-$Rings, with p^n replacing n. For (2)$\Rightarrow$(3), let

$$h_n : A \rightarrow \mathbb{Z}/p^n\mathbb{Z}$$

be onto ring homomorphisms. Let k_n be the cannonical map from $\mathbb{Z}/p^n\mathbb{Z}$ onto $\mathbb{Z}/p^{n-1}\mathbb{Z}$. As is explained in Section 2.2, $\mathbb{Z}_p$ is the subring of $\prod_n \mathbb{Z}_{p^n}$ consisting of all sequences a such that $k_n(a_n) = a_{n-1}$. Note that the maps h_n are unique: Each is determined by the image of $1 \in A$. From this, deduce that $k_n \circ h_n = h_{n-1}$. Now define $h : A \rightarrow \mathbb{Z}_p$ as follows: $h(a)_n = h_n(a)$. It follows from $k_n \circ h_n = h_{n-1}$ that $h(a) \in \mathbb{Z}_p$. It remains only to check that h is a homomorphism. This completes the case (2)$\Rightarrow$(3).

Finally, we assume (3) and prove that A extends to a model of OI. This is the point of what Wilke did. It happens in two stages. First, one shows how to use the maps h_p from A into $\mathbb{Z}_p$ to extend A to a $\mathbb{Z}-$Ring A' included in $\{\frac{a}{n} : a \in A \wedge n \in \mathbb{Z}^+\}$. The construction is as follows: Put $\frac{a}{n}$ in A' iff for all p, n divides $h_p(a)$ in $\mathbb{Z}_p$. This gives us A'. We extend A' to a model of OI by transfinite induction. At each stage we have a $\mathbb{Z}-$Ring and we add an "integer part" of some element of its real closure, and extend to another $\mathbb{Z}-$Ring. Eventually, we obtain a $\mathbb{Z}-$Ring B such that every element in the real closure of B is a finite distance from B. This means B is a model of OI. (cf.

Theorem 2.14.) ■

In this section, we shall use Wilke's result to give an axiomatization of $\forall_1(OI)$. We shall need the following

Definition 3.2. *A polynomial $f \in \mathbb{Q}[\bar{x}]$ is said to be integer valued if $f(\bar{n}) \in \mathbb{Z}$ for every tuple $\bar{n} \in \mathbb{Z}$. If F is an integral domain of characteristic zero, and S is a subset of F, we shall use $\mathbb{Z}\langle S\rangle$ to denote the subring of the fraction field of F consisting of all $f(\bar{s})$ such that $\bar{s} \in S$ and f is an integer valued polynomial. We shall often take S to be subset $\{x_1 \ldots x_n\}$ of the polynomial ring $\mathbb{Z}[\bar{x}]$. In this case, we shall write simply $\mathbb{Z}\langle x_1 \ldots x_n\rangle$ instead of $\mathbb{Z}\langle\{x_1 \ldots x_n\}\rangle$.*

The integer-valued polynomials were characterized by Polya and Nagel. Their main result is summarized by

Theorem 3.3. *For i a positive integer, let*

$$h_i(x) = \frac{x(x-1)\cdots(x-i+1)}{i!}.$$

Let $h_0(x) = 1$. A polynomial in $\mathbb{Q}[x_1 \ldots x_n]$ is integer valued iff it is an integer linear combination of products of the form

$$h_{i_1}(x_1)\cdots h_{i_n}(x_n),$$

where $i_1, i_2 \ldots$ are non-negative integers.

A proof can be found in [NAR1, Chapter II, Theorem 2.1]. ■

We shall prove

Theorem 3.4. *$\forall_1(OI)$ is axiomatized by the set of sentences T consisting of OR (the axioms for Ordered Rings) together with all sentences*

$$\forall \bar{x}\,(\neg 0 < f(\bar{x}) < n),$$

such that f is a polynomial with integer coefficients, n is a positive integer, and $\frac{f(\bar{x})}{n}$ is an integer-valued polynomial.

Proof. We consider first the direction $\forall_1(OI) \Rightarrow T$. Since T is an $\forall_1$ theory, it suffices to show that $OI \Rightarrow T$.

Suppose $A \models OI$. Clearly $A \models OR$. Let $\bar{a} \in A$, and suppose $\frac{f(\bar{x})}{n}$ is integer valued. We have to show that

$$A \models \neg 0 < f(\bar{a}) < n. \tag{3.2}$$

We will prove that the element $\frac{f(\bar{a})}{n}$ of the quotient field of A is in fact an element of A. Since A is a Discretely Ordered Ring, $\frac{f(\bar{a})}{n}$ cannot be between 0 and 1. Thus (3.2) will follow.

Since $A \models OI$, there is a ring homomorphism $\pi : A \rightarrow \mathbb{Z}/n\mathbb{Z}$ with kernel nA. (See Theorem 2.13.) The polynomial $f(\bar{x})$ vanishes at all tuples from $\mathbb{Z}/n\mathbb{Z}$, since $\frac{f(\bar{x})}{n}$ is integer valued. Thus $f(\pi(\bar{a})) = 0$. Since π is a homomorphism, $\pi(f(\bar{a})) = 0$. This means $f(\bar{a}) \in nA$, the kernel of π. Hence $\frac{f(\bar{a})}{n} \in A$. This proves $OI \Rightarrow T$.

Next, we show that $T \Longrightarrow \forall_1(OI)$. Suppose $A \models T$. In order to prove that A satisfies $\forall_1(OI)$, it suffices to show that every finitely generated subring of A satisfies $\forall_1(OI)$. Let $\bar{a} = a_1 \ldots a_m$ be a tuple from A, and let $B = \mathbb{Z}[\bar{a}]$. Since T is an $\forall_1$ theory, $B \models T$. We shall prove that B satisfies $\forall_1(OI)$.

It follows from the definition of T that B is a Discretely Ordered Ring. By Theorem 3.1, B will satisfy $\forall_1(OI)$ if for all primes p and all positive integers n there is a ring homomorphism from B onto $\mathbb{Z}/p^n\mathbb{Z}$.

Let I be the ideal in $\mathbb{Z}[x_1 \ldots x_m]$ consisting of all polynomials f such that $f(\bar{a}) = 0$, so that B is ring-isomorphic to $\mathbb{Z}[x_1 \ldots x_m]/I$. By the Hilbert Basis Theorem, I is generated by a finite set of polynomials $g_1 \ldots g_l$. If we knew that there was a tuple of integers $\bar{\mu}$ such that for all i,

$$g_i(\bar{\mu}) \equiv 0 \bmod p^n, \tag{3.3}$$

then we could construct a homomorphism $h : B \rightarrow \mathbb{Z}/p^n\mathbb{Z}$ as follows:

$$h(k(\bar{a})) = k(\bar{\mu}) + p^n\mathbb{Z},$$

for all $k \in \mathbb{Z}[x_1 \dots x_m]$. This definition of h makes sense because if $k_i \in \mathbb{Z}[x_1 \dots x_m]$ and $k_1(\bar{a}) = k_2(\bar{a})$, then $k_1(\bar{x}) - k_2(\bar{x}) \in I$. From this, and (3.3), it follows that

$$k_1(\bar{\mu}) + p^n\mathbb{Z} = k_2(\bar{\mu}) + p^n\mathbb{Z}.$$

It is immediate that h is a homomorphism. Since $h(1) = 1 + p^n\mathbb{Z}$, it follows that h maps B *onto* $\mathbb{Z}/p^n\mathbb{Z}$.

Thus we are reduced to showing that there are integers $\bar{\mu}$ such that (3.3) holds.

Assume, by way of contradiction, that there is a positive integer n and a prime p such that the polynomials g_i have no common integral zero mod p^n. Under these conditions, we shall construct a polynomial $f \in \mathbb{Z}[\bar{x}]$ such that $\frac{f(x)}{p^n}$ is integer valued, and

$$B \models 0 < f(\bar{a}) < p^n,$$

contrary to our assumption that $B \models T$.

Let $r_1 \dots r_k$ be all the integers between 0 and p^n that are not divisible by p. Define the polynomial $f(\bar{x})$ by

$$f(\bar{x}) = Mp^n + \prod_{u=1}^{k} \prod_{v=1}^{l} \prod_{w=0}^{n-1} (h_{p^w}(g_v(\bar{x})) - r_u), \tag{3.4}$$

where the h_i are defined in the statement of Theorem 3.3, and

$$M = -\left\lfloor \frac{\prod_{u=1}^{k}\prod_{v=1}^{l}\prod_{w=0}^{n-1}(-r_u)}{p^n} \right\rfloor.$$

Since for all v, $g_v(\bar{a}) = 0$, and since, for all w, $h_{p^w}(0) = 0$, it follows that

$$f(\bar{a}) = Mp^n + \prod_{u=1}^{k}\prod_{v=1}^{l}\prod_{w=0}^{n-1}(-r_u).$$

It follows from our choice of M that $f(\bar{a})$ is the unique integer in the interval $[0, p^n)$ congruent to $\prod_{u=1}^{k}\prod_{v=1}^{l}\prod_{w=0}^{n-1}(-r_u) \bmod p^n$. Since the r_i are not divisible by p, it follows that $0 < f(\bar{a}) < p^n$. If we show that $\frac{f(\bar{x})}{p^n}$ is an integer-valued polynomial then the proof of Theorem 3.4 will be complete. To this end, we shall need

Lemma 3.5. *If $w \in \mathbb{Z}$ is non-negative, and if $y \in \mathbb{Z}$, and if p does not divide y, then p does not divide $h_{p^w}(yp^w)$.*

Assuming this Lemma, let us show that $\frac{f(\bar{x})}{p^n}$ is integer valued. Let $\bar{x} \in \mathbb{Z}$. We have to show that $\frac{f(\bar{x})}{p^n} \in \mathbb{Z}$. Since the polynomials g_v have no common zero mod p^n, it follows that for some v, $g_v(\bar{x})$ has the form $p^w y$, with $0 \leq w \leq n-1$ and y not divisible by p. Lemma 3.5 implies that $h_{p^w}(g_j(\bar{x}))$ is not divisible by p. Thus for some u,

$$h_{p^w}(g_v(\bar{x})) \equiv r_u \bmod p^n.$$

But then the factor $h_{p^w}(g_v(\bar{x})) - r_u$ in (3.4) is divisible by p^n. Thus $\frac{f(\bar{x})}{p^n} \in \mathbb{Z}$. This completes the proof of Theorem 3.4.

Proof of Lemma 3.5. Let $v_p(n)$ be the exact power of p in the non-zero integer n. We have

$$h_{p^w}(yp^w) = \frac{yp^w(yp^w-1)\dots(yp^w-p^w+1)}{p^w!}.$$

Using the multiplicativity of v_p, we find that

$$v_p(h_{p^w}(yp^w)) = v_p(\frac{yp^w}{p^w}) + \sum_{k=1}^{p^w-1} (v_p(yp^w-k) - v_p(k)).$$

Since p does not divide y, the first summand is 0. We claim that each term

$$v_p(yp^w-k) - v_p(k)$$

of the second summand is also 0. We make use of the following easily verified fact: If x and y are integers different from 0, and if $v_p(x) < v_p(y)$, then $v_p(y-x) = v_p(x)$.

Since for each term of the above sum, $k < p^w$, it follows that $v_p(k) < v_p(yp^w)$. Thus $v_p(yp^w-k) = v_p(k)$, and the Lemma is proved. ■

Remark 1. *The technique for constructing f in the last theorem is taken from the*

proof of Skolem's Theorem that every function from $\mathbb{Z}/p^n\mathbb{Z}$ to $\mathbb{Z}/p^n\mathbb{Z}$ has the form

$$z + p^n\mathbb{Z} \mapsto g(z) + p^n\mathbb{Z}$$

for some integer-valued polynomial g. A proof of this Theorem can be found in [NAR1, Chapter 1, Section 4].

Example.

Let $A = \mathbb{Z}[t, \frac{t^2+1}{3}]$, where t is an indeterminate. We regard A as an ordered ring by embedding it in $\wp$. (The ordered ring $\wp$ is defined in Section 2.3.) Thus the positive elements of A are those polynomials in t whose leading coefficients are positive. The ring A is discretely ordered, but does not satisfy $\forall_1(OI)$.

To see that A is discretely ordered, we use the fact that the ideal I in the polynomial ring $\mathbb{Z}[x, y]$ consisting of all f such that $f(t, \frac{t^2+1}{3}) = 0$ is generated by the single polynomial $g(x, y) = 3y - x^2 - 1$. (Think of g as a polynomial in y with coefficients in $\mathbb{Q}(x)$. It has $\frac{x^2+1}{3}$ as a root, and is irreducible, hence every polynomial in $\mathbb{Q}(x)[y]$ that has $\frac{x^2+1}{3}$ as a root is divisible by g in $\mathbb{Q}(x)[y]$. Gauss's Lemma [LA Chapter 4, Section 2, Theorem 2.1] implies that this divisibility holds in $\mathbb{Q}[x][y]$, hence in $\mathbb{Z}[x][y]$.)

Now g has a zero in the nine-element field F, namely $x = \sqrt{-1}$, $y = 0$. We define a

homomorphism $h : A \to F$ as follows:

$$h(f(t, \frac{t^2+1}{3})) = f(\sqrt{-1}, 0),$$

for every $f \in \mathbb{Z}[x, y]$. This makes sense because if $f_1(t, \frac{t^2+1}{3}) = f_2(t, \frac{t^2+1}{3})$, then $f_1(x, y) - f_2(x, y) \in I$. Therefore $f_1(\sqrt{-1}, 0) - f_2(\sqrt{-1}, 0) = 0$, from which it follows that

$$h(f_1(t, \frac{t^2+1}{3})) = h(f_2(t, \frac{t^2+1}{3})).$$

It is easy to check that h is a homomorphism.

If A is not discretely ordered, then some element α of A has the form $\frac{a}{3^n}$, with a an integer not divisible by 3 in $\mathbb{Z}$, and $n > 0$. Since 3 does not divide a in $\mathbb{Z}$, we can choose integers u and v such that $au + 3v = 1$. Applying h to this equation, and using $a = 3^n\alpha$, we obtain $0 = 1$ in F.

To see that A does not satisfy $\forall_1(OI)$, we shall (in order to illustrate the last theorem) use the fact that the congruence

$$g(x, y) \equiv 0 \bmod 3$$

(where g is defined above) has no integer solutions. Given this data, the theorem con-

structs the following integer valued polynomial $H(x, y)$

$$\frac{h_1(g(x,y)-1)h_1(g(x,y)-2)}{3}.$$

This works out to be

$$\frac{(3y-x^2-2)(3y-x^2-3)}{3}.$$

Substituting t for x, and $\frac{t^2+1}{3}$ for y, we obtain $\frac{2}{3}$, which confirms, according to Theorem 3.4, that $A \not\models \forall_1(OI)$.

Theorem 3.6. *If A is an Ordered Ring then $A \models \forall_1(OI)$ iff $\mathbb{Z}\langle A\rangle$ is discretely ordered.*

Proof. Suppose $A \models \forall_1(OI)$. Let h be an integer-valued polynomial, and let $\bar{a} \in A$. Choose $n \in \mathbb{Z}$ such that $h_1 = nh$ has integer coefficients. By Theorem 3.4

$$A \models \neg 0 < h_1(\bar{a}) < n.$$

Thus

$$\mathbb{Z}\langle A\rangle \models \neg 0 < h(\bar{a}) < 1.$$

Since the elements of $\mathbb{Z}\langle A\rangle$ are all of the form $h(\bar{a})$ for some integer-valued polynomial h and some tuple $\bar{a} \in A$, it follows that $\mathbb{Z}\langle A\rangle$ is discretely ordered.

Conversely, suppose $\mathbb{Z}\langle A\rangle$ is discretely ordered. Suppose h_1 is a polynomial with

integer coefficients and n is an integer such that $h = \frac{h_1}{n}$ is integer valued. If $\bar{a} \in A$, then

$$\mathbb{Z}\langle A\rangle \models \neg 0 < h(\bar{a}) < n.$$

Hence

$$A \models \neg 0 < h_1(\bar{a}) < n.$$

Thus, Theorem 3.4 implies that $A \models \forall_1(OI)$. ■

Remark 2. *Keeping the notation of the last theorem, note that* $\mathbb{Z}\langle\mathbb{Z}\langle A\rangle\rangle = \mathbb{Z}\langle A\rangle$. *This is true because the integer valued polynomials are closed under composition. Therefore, by the last theorem, if* A *is an ordered ring, then* $\mathbb{Z}\langle A\rangle \models \forall_1(OI)$ *iff* $\mathbb{Z}\langle A\rangle$ *is discretely ordered.*

Theorem 3.7. *Let* ϕ *be an open formula. Then*

$$OI \vdash \forall \bar{x}\, \neg\phi(\bar{x})$$

iff there are polynomials $f_1 \ldots f_l$ *with integer coefficients and positive integers* $n_1 \ldots n_l$, *such that* $\frac{f_i}{n_i}$ *is an integer valued polynomial and*

$$RCF \vdash \forall \bar{x}\, (\phi(\bar{x}) \rightarrow \bigvee_{i=1}^{l} 0 < f_i(\bar{x}) < n_i). \tag{3.5}$$

Proof. Suppose $OI \vdash \forall \bar{x} \neg \phi(\bar{x})$, and just suppose RCF does not prove any such sentence (3.5). If $\bar{x} = x_1 \ldots x_l$, let $\bar{c} = c_1 \ldots c_l$ be new constants. Let T be the theory consisting of RCF plus $\phi(\bar{c})$ plus all sentences $\neg 0 < f(\bar{c}) < n$ such that f is a polynomial with integer coefficients and $\frac{f}{n}$ is integer valued. Then T is consistent.

Let F be a model of T. Suppose $\bar{a} = \bar{c}^F$. It follows from the choice of T that $\mathbb{Z}\langle \bar{a} \rangle$ is discretely ordered. Thus, by the remark following Theorem 3.6,

$$\mathbb{Z}\langle \bar{a} \rangle \models \forall_1(OI).$$

This means $\mathbb{Z}\langle \bar{a} \rangle$ extends to a model A of OI. But $\phi(\bar{a})$ holds in $\mathbb{Z}\langle \bar{a} \rangle$, hence also in A. This is impossible, since $OI \vdash \forall \bar{x}\, \neg \phi(\bar{x})$.

Conversely, suppose there are integer-valued polynomials f_i such that (3.5) holds. Since every model of OI extends to a real closed field, $OI \vdash \forall_1(RCF)$. Thus OI proves the sentence of (3.5). By Theorem 3.4, for every polynomial f with integer coefficients, and for every integer n such that $\frac{f}{n}$ is integer valued,

$$OI \vdash \forall \bar{x}\, (\neg 0 < f(\bar{x}) < n).$$

Thus $OI \vdash \forall \bar{x}\, \neg \phi(\bar{x})$. ■

Since RCF is a complete Theory, condition (3.5) holds iff the sentence

$$\forall \bar{x}\,(\phi(\bar{x}) \rightarrow \bigvee_i 0 < f_i(\bar{x}) < n_i) \tag{3.6}$$

is true in $\mathbb{R}$. Now the formula $\phi(\bar{x}) \rightarrow \bigvee_i 0 < f_i(\bar{x}) < n_i$ defines a subset of $\mathbb{R}^n$. It follows from the MRDP theorem ([MAT, Chapter 5 Section 6] that there is no algorithm for determining, for arbitrary open ϕ, whether or not $\phi^{\mathbb{R}^n}$ has an integer point. But it may well be decidable whether the complements of subsets of this form have integer points. If so, then $\forall_1(OI)$ is recursive.

In Lemma 2 of [VD1], Van den Dries gives a purely ring-theoretic condition for a ring to have an expansion to a discretely ordered ring. We shall use Theorem 3.6 to give a similar result for models of $\forall_1(OI)$.

Proposition 3.8. *Let A be an integral domain extending $\mathbb{Z}$, with fraction field F. Then A has an expansion $(A, <)$ satisfying $\forall_1(OI)$ iff there is a real valuation ring $V \subsetneq F$ such that $V \cap \mathbb{Z}\langle A\rangle = \mathbb{Z}$.*

Proof. All notions about valuation rings used here are explained in Section 2.

Suppose, first, that A has an expansion $(A, <)$ satisfying $\forall_1(OI)$. The ordering on A extends uniquely to an ordering on F. Regarding F in this way as an ordered field, let V be the subring of F consisting of all elements with absolute value less than some standard integer. Clearly V is convex. It follows that V is a real valuation ring. (If

$x \in F$, and $x \neq 0$, then either $|x| \leq 1$, or $|x^{-1}| \leq 1$. Hence either $|x|$ or $|x^{-1}|$ is in V. But $x = \pm |x|$.) By Theorem 3.6, $\mathbb{Z}\langle A \rangle$ is discretely ordered by $<$. It follows from this, and the definition of V, that $V \cap \mathbb{Z}\langle A \rangle = \mathbb{Z}$. This proves the left-to-right direction.

Conversely, assume that there is a real valuation ring $V \subseteq F$ such that $V \cap \mathbb{Z}\langle A \rangle = \mathbb{Z}$. By Theorem 2.15, there is an order relation on F making V convex. We *arbitrarily* select one such relation $<$. If we prove that $\mathbb{Z}\langle A \rangle$ is discretely ordered by $<$, it will follow from Theorem 3.6 that $(A, <) \models \forall_1(OI)$.

Suppose, on the contrary, that $h \in \mathbb{Z}\langle A \rangle$, and $0 < h < 1$. Since V is a subring of F, the ring V contains 0 and 1. But V is convex. Therefore $h \in V$. Since $V \cap \mathbb{Z}\langle A \rangle = \mathbb{Z}$, it follows that $h \in \mathbb{Z}$. But $(\mathbb{Z}, <)$ is an ordered ring, since it is a substructure of $(F, <)$. The ordering $<$ on $\mathbb{Z}$ must coincide with the usual one, since there is only one ordering making $\mathbb{Z}$ into an ordered ring. Hence $0 < h < 1$ is impossible. Thus $\mathbb{Z}\langle A \rangle$ is discretely ordered by $<$. ■

The proof of the last Proposition actually shows that if there is a real valuation ring $V \subseteq F$ such that $V \cap \mathbb{Z}\langle A \rangle = \mathbb{Z}$, then not only does A have *some* expansion $(A, <)$ satisfying $\forall_1(OI)$, but in fact if $<$ is *any* order on F making V convex then $(A, <) \models \forall_1(OI)$.

4. Rings of Polynomials with Algebraic Coefficients

Let $\bar{f} \in \wp$ be polynomials whose defining coefficients are algebraic. (See Section 2.3 for the definition of the ordered ring $\wp$.) In this section we consider the question: When is true that $\mathbb{Z}[\bar{f}] \models \forall_1(OI)$? We shall prove

Theorem 4.1. *Let $\bar{f} = f_1 \dots f_n \in \wp$ be polynomials with algebraic coefficients. Let $I \subseteq \mathbb{Z}[x_1 \dots x_n]$ be the ideal of all polynomials g such that $g(\bar{f}) = 0$. Then $\mathbb{Z}[\bar{f}] \models \forall_1(OI)$ iff for all primes p, I has a zero in the p-adic integers $\mathbb{Z}_p$.*

Proof. 4.1Let $A = \mathbb{Z}[\bar{f}]$. Suppose $A \models \forall_1(OI)$. By Theorem 3.1, for each prime p and each integer $n > 1$, there is a homomorphism $\pi : A \to \mathbb{Z}_p$. If $g \in I$ then the equation $g(\bar{f}) = 0$ holds in A, hence $g(\pi\bar{f}) = 0$ holds in $\mathbb{Z}_p$. Thus I has the zero $\pi\bar{f}$ in $\mathbb{Z}_p$.

Conversely, suppose for all primes $p \in \mathbb{Z}$, I has a zero in $\mathbb{Z}_p$. By Theorem 3.6, in order to prove that $A \models \forall_1(OI)$, it suffices to show that $\mathbb{Z}\langle A\rangle$ is discretely ordered. Suppose $h(\bar{x})$ is an integer-valued polynomial and $h(\bar{f})$ is finite. Since $h(\bar{f})$ is a polynomial, it follows that $h(\bar{f})$ is a real algebraic number. It will be sufficient to show that

$$h(\bar{f}) \in \mathbb{Z}.$$

To this end, let $p \in \mathbb{Z}$ be a prime, and let $\bar{\gamma}$ be a zero of I in $\mathbb{Z}_p$. There is a unique homomorphism λ from $\mathbb{Z}[\bar{x}]$ into $\mathbb{Z}_p$ taking $\bar{x}$ to $\bar{\gamma}$. If $g_1(\bar{x})$ and $g_2(\bar{x})$ are in $\mathbb{Z}[\bar{x}]$, and $g_1(\bar{f}) = g_2(\bar{f})$, then $g_1(\bar{x}) - g_2(\bar{x}) \in I$. Therefore $g_1(\bar{\gamma}) - g_2(\bar{\gamma}) = 0$, i.e., $g_1(\bar{\gamma}) = g_2(\bar{\gamma})$. It follows that the map π from A to $\mathbb{Z}_p$, defined by

$$\pi(g(\bar{f})) = g(\bar{\gamma})$$

is well defined. One easily checks that π is a homomorphism.

One can extend π to a homomorphism from the subring $A[\mathbb{Q}]$ of the fraction field of A into $\mathbb{Q}_p$. This extension is possible because $\mathbb{Z}_p$ has characteristic zero, hence π restricted to $\mathbb{Z}$ is one-to-one. We shall call the extended map π as well. Since $h(\bar{f})$ is algebraic over $\mathbb{Q}$, there is an irreducible polynomial $g(x) \in \mathbb{Z}[x]$ such that $g(h(\bar{f})) = 0$. Applying π, we obtain in $\mathbb{Q}_p$ the equation

$$g(h(\bar{\gamma})) = 0.$$

We claim that in fact $h(\bar{\gamma}) \in \mathbb{Z}_p$, hence g has a zero in $\mathbb{Z}_p$.

Suppose $h(\bar{x})$ has the form

$$\frac{h_1(\bar{x})}{rp^s},$$

with h_1 a polynomial with integer coefficients, r an integer not divisible by p, and s a non-negative integer.

Choose a tuple of integers $\bar{m}$ so close to $\bar{\gamma}$, in the sense of the p-adic metric, that $h_1(\bar{\gamma}) - h_1(\bar{m})$ is divisible by p^s in $\mathbb{Z}_p$. (See Section 2.2 for a definition of the p-adic metric.) Since h is integer-valued, $h_1(\bar{m})$ is divisible by p^s in $\mathbb{Z}$, hence also in $\mathbb{Z}_p$. It follows that $h_1(\bar{\gamma})$ is divisible by p^s in $\mathbb{Z}_p$. Since r is a unit in $\mathbb{Z}_p$, it follows that $h_1(\bar{\gamma})$ is divisible by rp^s in $\mathbb{Z}_p$. Thus $h(\bar{\gamma}) \in \mathbb{Z}_p$.

We have shown that g has a zero in $\mathbb{Z}_p$. Since p was arbitrary, this is true for every prime p. Since $\mathbb{Z}_p/p\mathbb{Z}_p$ is isomorphic to $\mathbb{Z}/p\mathbb{Z}$, it follows that g has a zero in $\mathbb{Z}/p\mathbb{Z}$ for every prime p.We shall now prove that this is possible (for g irreducible over $\mathbb{Z}[x]$) iff $g(x)$ has the form

$$\pm x + c$$

for some integer c.

If g is linear, let us say $g(x) = bx + c$, and if $p \in \mathbb{Z}$ is a prime dividing b, then p must also divide c, else g has no zeros mod p. But then g is divisible by p, contrary to the irreducibility of g over $\mathbb{Z}[x]$. Thus if g is linear, then $b = \pm 1$, and g has the form $\pm x + c$.

It remains to show that g must be linear. For this, we make use of the following theorem due to Hasse.

Theorem 4.2. *Suppose $f \in \mathbb{Z}[x]$ is an irreducible polynomial of degree greater than 1. Then there are infinitely many primes $p \in \mathbb{Z}$ such that f has no zero* mod p. ■

A useful sketch of the proof can be found in [CF, page 362].

The polynomial g constructed above has a zero mod p for every prime p. Thus, by Hasse's Theorem, g is linear. We have shown that g must have the form $\pm x + c$ for some $c \in \mathbb{Z}$. Since $g(h(\bar{f})) = 0$, we conclude that $h(\bar{f}) \in \mathbb{Z}$. ■

Example.

Let $A = \mathbb{Z}[\bar{f}]$, where the coefficients of the f_i are algebraic. Let $I \subseteq \mathbb{Z}[\bar{x}]$ be the vanishing ideal of $\bar{f}$. If I has a zero in $\mathbb{Z}$, then $A \models \forall_1(OI)$. This is true because if I has an integer zero, then I has a zero in $\mathbb{Z}_p$ for every prime p.

Example.

We show that the ring

$$A = \mathbb{Z}[t, \sqrt{2}(t^2 - 13)(t^2 - 17)(t^2 - 221)]$$

satisfies $\forall_1(OI)$.

Note that the polynomial

$$y^2 - 2(x^2 - 13)^2(x^2 - 17)^2(x^2 - 221)^2 \tag{4.1}$$

has a zero in A, but not in $\mathbb{Z}$.

We sketch the proof. A computation using the law of quadratic reciprocity shows that the polynomial

$$f(t) = (t^2 - 13)(t^2 - 17)(t^2 - 221)$$

has zeros mod p for every prime p. See [BS, page 3].

If p is an odd prime, then at least one of the three factors of f does not have a multiple root mod p. That factor will have a p-adic zero. (This can be deduced from Hensel's Lemma, which is a p-adic analogue of Newton's Method. From a simple zero mod p one obtains successively zeros mod p^2, p^3, etc., thus constructing a p-adic zero.) Thus if p is an odd prime then $f(t)$ has a zero in the p-adic integers. As for $p = 2$, it is shown in [BS, Chapter 1, Section 6], Theorem 2, that any number $8n + 1$, in particular 17, is a square in $\mathbb{Z}_2$. It follows that the polynomial (4.1) has a zero in $\mathbb{Z}_p$ for every prime p.

Finally, to apply Theorem 4.1, we have to identify the vanishing ideal $I \subseteq \mathbb{Z}[\bar{x}]$ of the tuple

$$t, \sqrt{2}(t^2 - 13)(t^2 - 17)(t^2 - 221).$$

One easily checks that I is the ideal generated by (4.1). Our argument shows that I has zero's in $\mathbb{Z}_p$ for all p. Thus $A \models \forall_1(OI)$.

5. Diophantine Correct Open Induction

Let A be a discretely ordered ring, and r an element in some ordered field including the real closure of A. One would like to find conditions on r for the extension $A[r]$ to be discretely ordered. Very little is known about this, even in the case where A is a finitely generated ring of polynomials. But if one requires that $A \models \forall_1(OI)$, and that r be transcendental over A, then there are sufficient conditions, found by Wilkie [W, Lemma 3.1] for $A[r]$ to satisfy $\forall_1(OI)$, namely, that r not be a finite distance from the subring $A[\mathbb{Q}]$ of the quotient field of A, and that r not be infinitely close to any element of the real closure of A.

Suppose now that the ordered ring A is Diophantine correct, and suppose r is chosen to satisfy Wilkie's conditions. Must $A[r]$ be Diophantine correct? We do not know the answer to this question. In an effort to approach it, we have made the following study of $\forall_1(\mathbb{Z}) + OI$. (Here $\mathbb{Z}$ refers to an *ordered ring.*)

We shall use the abbreviation DOI (Diophantine correct Open Induction) to mean $\forall_1(\mathbb{Z}) + OI$.

In this section we shall prove that DOI is equivalent to the set of all sentences of $Th(\mathbb{Z})$ of the form

$$\forall x_1 \forall x_2 \ldots \forall x_n \exists y \phi,$$

with ϕ an open formula. As preparation for the proof, we begin with a Lemma on the structure of the definable subsets of a real closed field.

Suppose that F is a real closed field, and $\phi(x, \bar{y})$ is a formula in the language of ordered rings. It is well known (see, for example, [VD3, page 2]) that for each $\bar{r} \in F$, the subset of F defined by $\phi(x, \bar{r})$ can be expressed as a finite union $I_1 \cup \ldots \cup I_n$, where the I_i are either singletons or open intervals with endpoints in $F \cup \{\pm\infty\}$.

We shall need to know that the intervals I_i can be defined in terms of $\bar{r}$ in a uniform manner.

Lemma 5.1. *Let $\phi(x, \bar{y})$ be a formula in the language of ordered rings. Then there is a finite list of open formulas $\gamma_i(x, \overline{y})$ such that RCF proves the following sentences:*

(1) $\forall x, \overline{y}\,(\phi(x, \bar{y}) \leftrightarrow \bigvee_i \gamma_i(x, \overline{y}))$

(2) $\bigwedge_i \forall \overline{y}\ ($

$(\neg \exists x\, \gamma_i(x, \overline{y})) \vee$

$(\exists! x\, \gamma_i(x, \overline{y})) \vee$

$(\exists z \forall x (\gamma_i(x, \overline{y}) \leftrightarrow x < z)) \vee$

$(\exists z \forall x (\gamma_i(x, \overline{y}) \leftrightarrow x > z)) \vee$

$(\exists z, w \forall x\, (\gamma_i(x, \overline{y}) \leftrightarrow z < x < w)))$

Proof. To explain these sentences: Think of $\bar{y}$ as a tuple from some real closed field F. Let $S_{\bar{y}}$ denote the set of x in F such that $\phi(x, \bar{y})$ holds, and let $G^i_{\bar{y}}$ denote the set of

x in F such that $\gamma_i(x, \bar{y})$ holds. Then the first sentence says that $S_{\bar{y}}$ is the union, over i, of the $G^i_{\bar{y}}$. The second sentence says that $G^i_{\bar{y}}$ is either empty, a singleton, or an open interval. The point is that the intervals $G^i_{\bar{y}}$ are described, in terms of $\bar{y}$, by a fixed set of formulas.

To prepare for the proof, let us say a conjunction of formulas $f_i(x, \bar{y})\square_i 0$, where $\square_i$ is one of the symbols $>$, $<$, $=$, is a *Thom formula* if for every i there is some j such that f_j is the formal derivative of f_i with respect to x. (Thom's Lemma is Theorem 2.10.)

Every formula $f(x, \bar{y})\square 0$ is equivalent in RCF to a disjunction of Thom formulas. We prove this by induction on the x-degree of f.

If f is the zero polynomial then $f(x, \bar{y})\square 0$ is a Thom formula. Otherwise, RCF proves

$$f(x, \bar{y})\square 0 \quad \leftrightarrow \quad ((f(x, \bar{y})\square 0 \wedge f'(x, \bar{y}) > 0) \vee$$

$$(f(x, \bar{y})\square 0 \wedge f'(x, \bar{y}) \quad = \quad 0) \vee (f(x, \bar{y})\square 0 \wedge -f'(x, \bar{y}) > 0)).$$

By induction, write each of $f'(x, y) > 0$, $f'(x, \bar{y}) = 0$, and $-f'(x, \bar{y}) > 0$ as a disjunction of Thom formulas, and rearrange to get $f(x, \bar{y})\square 0$ as a disjunction of Thom formula.

Note that the set of disjunctions of Thom formulas is closed (up to logical equivalence) under conjunction.

Since every open formula is equivalent in RCF to a disjunction of conjunctions

of formulas $f(x,\bar{y})\square 0$, where $\square$ is $=$ or $>$ or $<$, it follows that every open formula is equivalent in RCF to a disjunction of Thom formulas.

To prove Lemma 5.1, we can assume that the formula ϕ is open, since RFC admits elimination of quantifiers. Therefore we can assume that $\phi(x,\bar{y})$ is a disjunction Thom formulas $\gamma_i(x,\bar{y})$. Statement (1) of the Lemma is now immediate. If F is any real closed field, and if $\bar{s} \in F$, then statement (2) of the Lemma, with the quantifiers $\forall\bar{y}$ instantiated by $\bar{s}$, must be true in F according to Thom's Lemma. ■

Lemma 5.2. *Let A be an ordered ring. Let F be its real closure. For every $r \in F$, there are $a, b \in A$ such that $a < r < b$.*

Proof. If $r \in F$, then there is a polynomial $f(x,\bar{y})$ with integer coefficients and a tuple $\bar{c} \in A$ such that $f(x,\bar{c})$ is not the zero polynomial, and $f(r,\bar{c}) = 0$. In [BRU Chapter 6, Section 3, Proposition 6.3.1], an explicit construction is given of polynomials $\alpha(\bar{y})$, $\beta(\bar{y})$ with integer coefficients depending only on f such that $\alpha(\bar{c}) < r < \beta(\bar{c})$. ■

Finally, we shall need the following fundamental fact about Open Induction due to Shepherdson [Shep].

Lemma 5.3. *Open induction proves the least number principle for open formulas. Specifically, for every open formula $\phi(x,y)$, Open Induction proves*

$$\forall\bar{y}((\exists x \geq 0\ \phi(x,\bar{y})) \rightarrow \exists z \geq 0\ (\phi(z,\bar{y}) \wedge \forall w\ (0 \leq w < z \rightarrow \neg\phi(w,\bar{y}))).$$

Proof. (Sketch.) Suppose A is an ordered ring and F is its real closure. Then A satisfies open induction iff every element of F is a finite distance from some element of A. (See Theorem 2.14.)

Suppose $\phi(x, \bar{y})$ is an open formula, A is a model of OI, $\bar{a}, b \in A$, and

$$A \models \phi(b, \bar{a}) \wedge b \geq 0. \tag{5.1}$$

We have to show that there is a least element b of A satisfying (5.1).

The formula

$$\phi(x, \bar{a}) \wedge x \geq 0$$

defines a finite union of pairwise disjoint intervals I_i in F, with endpoints in $F \cup \{\pm\infty\}$. (This is a consequence of Lemma 5.1. For a direct proof, see [VD3].) By the definition of b, one of the intervals I_i meets A. Choose the interval I_i meeting A with the smallest left-hand endpoint, and call it I. Choose $b' \in A$ to be a finite distance from $\inf I$. Choose $n \in \mathbb{Z}$ such that $b' + n \leq \inf I \leq b' + n + 1$. Since I contains an element of A, and A is discretely ordered, one of $b' + n$, $b' + n + 1$ must be in I. The smaller of the two that is in I will be the least non-negative element of A satisfying $\phi(x, \bar{a})$. ■

For the remainder of this section, all formulas will be assumed to belong to the language of ordered rings.

Lemma 5.4. *For every formula $\forall x\, \phi(x, \bar{y})$ with ϕ open, there are open formulas $\psi_i(x_i, \bar{y})$*

such that

$$OI \vdash \forall \overline{y}\,((\forall x \phi(x,\overline{y})) \leftrightarrow \bigwedge_i \exists x_i \psi_i(x_i,\overline{y})).$$

Proof. *By Lemma 5.1, there is a finite list of open formulas* $\gamma_i(x,\bar{y})$ *such that* RCF *proves*

(1) $\forall x, \overline{y}\,(\neg\phi(x,\bar{y}) \leftrightarrow \bigvee_i \gamma_i(x,\overline{y}))$, and

(2) $\bigwedge_i \forall \overline{y}$ (

$(\neg\exists x\, \gamma_i(x,\overline{y})) \vee$

$(\exists! x\, \gamma_i(x,\overline{y})) \vee$

$(\exists z \forall x(\gamma_i(x,\overline{y}) \leftrightarrow x < z)) \vee$

$(\exists z \forall x(\gamma_i(x,\overline{y}) \leftrightarrow x > z)) \vee$

$(\exists z\,, w \forall x\,(\gamma_i(x,\overline{y}) \leftrightarrow z < x < w))).$

Note the negation symbol in the first sentence.

For each i, choose quantifier free formulas $\alpha_i(z,\overline{y})$ and $\beta_i(z,\overline{y})$ such that RCF proves

$$\forall z, \overline{y}\,(\alpha_i(z,\overline{y}) \leftrightarrow \forall w\,(\gamma_i(w,\overline{y}) \rightarrow z < w)) \tag{5.2}$$

and

$$\forall z, \overline{y}\,(\beta_i(z,\overline{y}) \leftrightarrow \forall w\,(\gamma_i(w,\overline{y}) \rightarrow w < z)). \tag{5.3}$$

This is possible because RCF admits elimination of quantifiers.

Take $\psi_i(x_i, \overline{y})$ to be the formula

$$\alpha_i(x_i, \overline{y}) \wedge \beta_i(x_i + 1, \overline{y}).$$

If F is a real closed field, and $\bar{r} \in F$, then $\psi_i(x_i, \bar{r})$ defines all elements x_i of F such that x_i is less than any element of the set defined by $\gamma_i(x, \bar{r})$, and $x_i + 1$ is greater than any element of that set.

We shall prove that the sentence

$$\forall \overline{y}\,((\forall x \phi(x, \overline{y})) \leftrightarrow \bigwedge_i \exists x_i \psi_i(x_i, \overline{y}))$$

holds in every Open Induction Domain A.

For the left-to-right direction of the equivalence, let $\overline{a}$ be a tuple from an Open Induction Domain A, and suppose that $A \models \forall x\, \phi(x, \overline{a})$. For each i, we have to find some g in A such that

$$A \models \alpha_i(g, \overline{a}) \wedge \beta_i(g + 1, \overline{a}). \tag{5.4}$$

Let F be a real closure of A. Let S_i be the subset of F defined by the formula $\gamma_i(x, \overline{a})$. By definition of γ_i, S_i is either empty, or an interval with endpoints in F. If S_i is empty, then the definition of α_i and β_i implies that any $g \in A$ will make (5.4) true.

Suppose S_i is not empty. We claim that S_i is a bounded interval. Otherwise, S_i

would have the form (r, ∞) or $(-\infty, r)$, for some $r \in F$. By Lemma 5.2, S_i would then meet A. But Sentence (1) holds in A, since it is universal and holds in F. Sentence (1), together with our assumption that $A \models \forall x\, \phi(x, \overline{a})$, implies that S_i is disjoint from A. It follows that S_i is a bounded interval.

By Lemma 5.2, and the fact that S_i is bounded, there is an element g_1 of A greater than any element of S_i. By (5.2), the open formula $\alpha_i(z, \overline{a})$ defines in F the set of elements less than every element of S_i. Thus, for some $z \in A$,

$$A \models \alpha_i(z, \overline{a}) \wedge z < g_1. \tag{5.5}$$

By Lemma 5.3, there is a greatest element z of A satisfying (5.5). Call it g. Since A is discretely ordered, $g + 1 \leq g_1$. From the maximality of g, it follows that

$$A \models \neg\alpha_i(g + 1, \overline{a}).$$

This means $g + 1$ is at least as large as some element of S_i. But S_i is an interval disjoint from A. Hence $g + 1$ is greater than every element of S_i. We conclude from (5.3) that the formula $\beta_i(g + 1, \overline{a})$ is true in F, and therefore in A.

We have shown that $A \models \alpha_i(g, \overline{a}) \wedge \beta_i(g+1, \overline{a})$. This proves the left-to-right direction of our equivalence.

For the other direction, assume that for every i, we have some b_i in A such that

$$A \models \alpha_i(b_i, \overline{a}) \wedge \beta_i(b_i + 1, \overline{a}).$$

Then this formula also holds in F. Thus, for each i,

$$F \models \forall w\,(\gamma_i(w, \overline{a}) \rightarrow b_i < w) \wedge\ \forall w\,(\gamma_i(w, \overline{a}) \rightarrow w < b_i + 1).$$

Thus every element b of F satisfying $\gamma_i(b, \overline{a})$ lies between b_i and $b_i + 1$. Since A is discretely ordered, there can be no such element b in A. Thus, for every $b \in A$, we have

$$A \models \neg \bigvee_i \gamma_i\,(b, \overline{a})\,.$$

It follows from (1) that $A \models \forall x\,\phi(x, \overline{a})$, as required. ■

Corollary 5.5. *Let A and B be Open Induction Domains. Suppose A is a substructure of B. Let ϕ be an open formula. Let $\overline{a}$ be a tuple from A. Then $A \models \forall x \phi(x, \overline{a})$ iff $B \models \forall x \phi(x, \overline{a})$.* ■

We come now to the point of this section.

Theorem 5.6. *DOI is equivalent to the theory T consisting of all sentences of $Th(\mathbb{Z})$ of the form*

$$\forall x_1 \forall x_2 \ldots \forall x_n \exists y \phi,$$

with ϕ an open formula.

Proof. Consider first the implication $T \Rightarrow DOI$. By hypothesis, $T \Rightarrow DOR+ \forall_1(\mathbb{Z})$. So we have only to verify that T proves all instances of the induction scheme for open formulas. But for each open formula ϕ, the induction axiom

$$\forall \overline{x}\,((\phi(\overline{x},0) \wedge \forall y \geq 0\,(\phi(\overline{x},y) \rightarrow \phi(\overline{x},y+1))) \rightarrow \forall z \geq 0\,\phi(\overline{x},z))$$

is logically equivalent to

$$\forall \overline{x}\,\forall z\,\exists y\,(z \geq 0 \rightarrow$$

$$(y \geq 0 \wedge \phi(\overline{x},0) \wedge ((\phi(\overline{x},y) \rightarrow \phi(\overline{x},y+1)) \rightarrow \phi(\overline{x},z))))$$

The latter belongs to T.

Conversely, we show that $DOI \Longrightarrow T$. Suppose that $A \models DOI$. Let $\phi(\overline{x},y)$ be an open formula such that $\mathbb{Z} \models \forall \overline{x}\,\exists y\,\phi(\overline{x},y)$. We have to show that

$$A \models \forall \overline{x}\,\exists y\,\phi(\overline{x},y).$$

By Lemma 5.4, there are open formulas ψ_i such that OI proves the equivalence

$$\forall \overline{x}\,((\exists y\,\phi(\overline{x},y)) \longleftrightarrow \bigvee_i \forall z_i \psi(\overline{x},z_i)). \tag{5.6}$$

This equivalence is therefore true in $\mathbb{Z}$. Hence $\mathbb{Z}$ satisfies

$$\forall \overline{x} \bigvee_i \forall z_i \psi(\overline{x}, z_i)).$$

But this sentence is universal, so it holds in A. Since A is an Open Induction Domain, it satisfies (5.6). Therefore $A \models \forall \overline{x}\, \exists y\, \phi(\overline{x}, y)$, as required. ■

6. A Criterion for Diophantine Correctness.

In this section we give a number-theoretic description of the finitely generated Diophantine correct rings $\mathbb{Z}[\bar{f}]$, where $\bar{f} \in \wp$. Here $\wp$ (see Section 2.3) is the ordered ring of functions from $(0, \infty)$ to $\mathbb{R}$ defined by finite real linear combinations of rational powers of a variable t. The ring $\mathbb{Z}[\bar{f}]$ has the ordering it acquires as a subring of $\wp$

We shall regard $\mathbb{Z}[\bar{f}]$ as "given" if we are given a transcendence basis $\bar{r}$ for the field generated by the coefficients of the f_i, and if for each coefficient c of each of the f_i, we are given a formula $\psi(\bar{u}, v)$ in the language of ordered rings such that $\psi(\bar{r}, v)$ defines c in $\mathbb{R}$. From this data, we shall translate each question "Is $\mathbb{Z}[\bar{f}]$ Diophantine correct?" into a problem in number theory. We shall need:

Lemma 6.1. *Let $f_1, f_2 \ldots f_n \in \wp$. Let $\theta(\bar{x})$ be an open formula. Then $\mathbb{Z}[\bar{f}] \models \theta(\bar{f})$ iff for all sufficiently large $u \in \mathbb{R}$, $\mathbb{R} \models \theta(\bar{f}(u))$.*

Proof. If θ is atomic, then we can assume it has one of the forms $G(\bar{f}) = 0$, or $G(\bar{f}) > 0$, where G is a polynomial with integer coefficients. Suppose θ has the form $G(\bar{f}) = 0$. Assume $\mathbb{Z}[\bar{f}] \models \theta(\bar{f})$. Then the value of the term $G(\bar{f})$ in the structure $\mathbb{Z}[\bar{f}]$ is the zero-function. The left-to-right direction of the statement of the Lemma follows. For the right-to-left direction, we appeal to the fact that a non-zero polynomial can

have only finitely many roots. This implies that $G(\bar{f}(t))$ is the zero function. Hence $\mathbb{Z}[\bar{f}] \models G(\bar{f}) = 0$.

If θ has the form $G(\bar{f}) > 0$, the Lemma follows from the fact that the value of the term $G(f)$ interpreted in the structure $\mathbb{Z}[\bar{f}]$, namely the ring element $G(f(t))$, is by definition positive iff $G(f(u))$ is positive for large u.

If θ is not atomic, the Lemma is proved by induction on the complexity of θ. The case where θ is $\theta_1 \wedge \theta_2$ is immediate. Suppose θ is $\neg\theta_1$. For the left-to-right direction of the Lemma, suppose $\mathbb{Z}[\bar{f}]$ satisfies $\neg\theta_1(\bar{f})$. Then by induction we deduce that for infinitely many positive $u \in \mathbb{R}$, $\mathbb{R} \models \neg\theta_1(\bar{f}(u))$. The set of positive $u \in \mathbb{R}$ such that $\mathbb{R} \models \neg\theta_1(\bar{f}(u))$ is a union of finitely many intervals. (This is true of any subset of $\mathbb{R}$ definable in the language of ordered rings.) It follows that for all sufficiently large $u \in \mathbb{R}$, $\mathbb{R} \models \neg\theta_1(\bar{f}(u))$. The right-to-left direction is immediate. ■

Lemma 6.2. *Let $f_1 \ldots f \in \wp$. The ordered ring $A = \mathbb{Z}[\bar{f}]$ is Diophantine correct iff for every open formula ϕ such that $\mathbb{A} \models \phi(\bar{f})$, there is a tuple $\bar{m} \in \mathbb{Z}$ such that $\mathbb{Z} \models \phi(\bar{m})$.*

Proof. Suppose A is not Diophantine correct. Choose $\psi(\bar{x})$ open and $\bar{a} \in A$ such that $A \models \psi(\bar{a})$ and $\mathbb{Z} \models \forall\bar{x}\neg\psi(\bar{x})$. Let g_i be polynomials with integer coefficients such that $a_i = g_i(\bar{f})$. Let $\phi(\bar{x})$ be the open formula

$$\psi(g_1(\bar{x}), g_2(\bar{x}) \ldots).$$

Then A satisfies $\phi(\bar{f})$, yet there are no integers $\bar{m}$ such that $\mathbb{Z} \models \phi(\bar{m})$, a contradiction. Conversely, suppose A is diophantine correct. Suppose ϕ is open, and $\mathbb{A} \models \phi(\bar{f})$. Then it cannot be true that $\mathbb{Z} \models \forall \bar{x} \neg \phi(\bar{x})$. So for some integers $\bar{m}$, $\mathbb{Z} \models \phi(\bar{m})$. ■

Lemma 6.3. *Suppose $\phi(\bar{x})$ is a formula in the language of ordered rings, and $\bar{r} \in \mathbb{R}^n$ is a tuple of reals algebraically independent over $\mathbb{Q}$. If $\mathbb{R} \models \phi(\bar{r})$, then there is a neighborhood U of $\bar{r}$ in $\mathbb{R}^n$ such that $U \subseteq \phi^{\mathbb{R}}$.*

Proof. Since RCF admits elimination of quantifiers, we can assume $\phi(\bar{x})$ is open. We can write ϕ as an equivalent (in RCF) disjunction of formulas of the form

$$\bigwedge f_i(\bar{x}) = 0 \wedge \bigwedge_i g_i(\bar{x}) > 0,$$

where the f_i and g_i are polynomials with integer coefficients. One of the above disjuncts will hold at $\bar{x} = \bar{r}$. For that disjunct, each f_i must be the zero polynomial, else $\bar{r}$ would not be algebraically independent over $\mathbb{Q}$. Thus $\bar{r}$ belongs to the open subset U of $\mathbb{R}^n$ defined by

$$\bigwedge_i g_i(\bar{x}) > 0.$$

Clearly $U \subseteq \phi^{\mathbb{R}}$. ■

We are now ready to give our characterization of the Diophantine correct rings $\mathbb{Z}[\bar{f}]$. First we consider the case where not all the coefficients of the f_i are algebraic.

Theorem 6.4. *Let $f_1 \dots f_n \in \wp$. Assume that for every i, $|f_i|$ tends to infinity as t tends to infinity. Let F be the field generated by the coefficients of the f_i. Assume F has transcendence degree at least 1 over $\mathbb{Q}$. Let*

$$\bar{r} = r_1 \dots r_l$$

be a transcendence basis for F over $\mathbb{Q}$. Then

(1) *There is an open formula $\theta(x_1 \dots x_l, y_1 \dots y_n)$ in the Language of Ordered Rings such that for all $\bar{y} \in \mathbb{R}$, $\mathbb{R} \models \theta(\bar{r}, \bar{y})$ iff for some $t \geq 1$, $\bigwedge_i y_i = f_i(t)$.*

(2) *If θ is as in (1), then $\mathbb{Z}[\bar{f}]$ is diophantine correct iff for every open set $U \subseteq \mathbb{R}^l$ containing $\bar{r}$, and for every $M > 0$, there are points $\bar{s} \in U$, $\bar{m} \in \mathbb{Z}^n$ such that*

$$\mathbb{R} \models (\bigwedge_i |m_i| > M) \wedge \theta(\bar{s}, \bar{m}).$$

Proof. To prove (1), let $\bar{c}$ be all the coefficients of the f_i. Evidently there is a formula θ_1 in the language of ordered rings such that for all $\bar{y} \in \mathbb{R}$, $\theta_1(\bar{c}, \bar{y})$ holds in $\mathbb{R}$ iff for some $t \geq 1$, $\bigwedge_i y_i = f_i(t)$. Each of the c_i is algebraic over the field $\mathbb{Q}(\bar{r})$. Therefore each c_i is definable from $\bar{r}$ in $\mathbb{R}$. (This follows from Proposition 2.11.) Part (1) now follows from the fact that RCF admits elimination of quantifiers.

To prove (2), suppose, first, that $\mathbb{Z}[\bar{f}]$ is Diophantine correct. Let $\bar{r}$, θ be as in (1).

Let $U \subseteq \mathbb{R}^l$ be an open set containing $\bar{r}$. Suppose $M > 0$. We have to find $\bar{s} \in U$ and $\bar{m} \in \mathbb{Z}^n$ such that

$$\mathbb{R} \models \bigwedge_i |m_i| > M \wedge \theta(\bar{s}, \bar{m}).$$

We can assume M is an integer.

Let $\gamma(\bar{x})$ be an open formula in the Language of Ordered Rings defining a neighborhood of $\bar{r}$ included in U. There is such a γ since, e.g., we can place a box containing $\bar{r}$ with rational corners inside of U. Choose, by quantifier elimination, an open formula $\theta_1(\bar{y})$ such that RCF proves

$$\theta_1(\bar{y}) \longleftrightarrow \exists \bar{x} \, ((\bigwedge_i |y_i| > M) \wedge \gamma(\bar{x}) \wedge \theta(\bar{x}, \bar{y})). \tag{6.1}$$

Each function $|f_i(t)|$ tends to infinity as t tends to infinity, according to our assumptions. Thus, for all sufficiently large t,

$$\mathbb{R} \models \theta_1(f_1(t), \ldots, f_n(t)).$$

(We can witness the existential quantifier in (6.1) with $\bar{r}$.) Thus, by Lemma 6.1,

$$\mathbb{Z}[\bar{f}] \models \theta_1(\bar{f}).$$

Since $\mathbb{Z}[\bar{f}]$ is Diophantine correct, there are integers $\bar{m} \in \mathbb{Z}^n$ such that

$$\mathbb{Z} \models \theta_1(\bar{m}).$$

Since RCF proves sentence (6.1), we conclude that $\bigwedge_i |m_i| > M$, and that, for some $\bar{s} \in \mathbb{R}^l$,

$$\mathbb{R} \models \gamma(\bar{s}) \wedge \theta(\bar{s}, \bar{m}).$$

The definition of γ implies that $\bar{s} \in U$.

Conversely, suppose that for every neighborhood U of $\bar{r}$ and every $M \in \mathbb{R}$, there are points $\bar{s} \in U$, $\bar{m} \in \mathbb{Z}^n$ such that

$$\mathbb{R} \models \bigwedge_i |m_i| > M \wedge \theta(\bar{s}, \bar{m}).$$

We want to show that A is Diophantine Correct. Let ϕ be an open formula such that $A \models \phi(\bar{f})$. By Lemma 6.2, it suffices to find integers $\bar{m}$ such that $\phi(\bar{m})$ holds in $\mathbb{Z}$.

Since ϕ is open and $\mathbb{Z}[\bar{f}] \models \phi(\bar{f})$, by Lemma 6.1 there is a $k > 1$ such that

$$\forall t > k,\ \mathbb{R} \models \phi(f_1(t), \ldots, f_n(t)). \tag{6.2}$$

The set of points $(f_1(t), \ldots, f_n(t))$ such that $1 \leq t \leq k$ is compact. Call it S. Choose

$M \in \mathbb{Z}$ so large that, for all $\bar{y} \in \mathbb{R}^n$,

$$\min |y_i| > M \Longrightarrow \bar{y} \notin S.$$

Then, for all $t > 1$,

$$\min |f_i(t)| > M \Longrightarrow t > k.$$

Thus, from (6.2) and the definition of θ,

$$\mathbb{R} \models \psi(\bar{r}), \tag{6.3}$$

where $\psi(\bar{x})$ is the formula

$$\forall \bar{y}\ ((\theta(\bar{x}, \bar{y}) \wedge (\bigwedge_i |y_i| > M)) \rightarrow \phi(\bar{y})).$$

Since $\bar{r}$ is algebraically independent over $\mathbb{Q}$, the subset of $\mathbb{R}^l$ defined by ψ must include a neighborhood U of $\bar{r}$. (See Lemma 6.3.) By our initial hypothesis, we can choose $\bar{s} \in U$ and $\bar{m} \in \mathbb{Z}^n$ such that

$$\mathbb{R} \models \bigwedge_i |m_i| > M \wedge \theta(\bar{s}, \bar{m}).$$

Since $\mathbb{R} \models \psi(\bar{s})$, we conclude from (6.3) that $\mathbb{R} \models \phi(\bar{m})$, as required. ■

Next, we describe the algebraic case:

Theorem 6.5. *Suppose $f_1 \dots f_n \in \wp$ have algebraic coefficients. Assume that for every i, $|f_i(t)|$ tends to infinity as t tends to infinity. Then $\mathbb{Z}[\bar{f}]$ is Diophantine correct iff there are arbitrarily large real numbers u such that $\bar{f}(u) \in \mathbb{Z}^n$.*

Proof. Since much of the proof is a simplified version of the proof of Theorem 6.4, we shall be brief. Suppose $\mathbb{Z}[\bar{f}]$ is Diophantine correct. Then there is an open formula $\theta(\bar{y})$ such that for all $\bar{y} \in \mathbb{R}$, $\mathbb{R} \models \theta(\bar{y})$ iff for some $t \geq 1$. $\bigwedge_i y_i = f_i(t)$. Using Lemma 6.1 we deduce that for every integer M,

$$\mathbb{Z}[\bar{f}] \models \theta(\bar{f}) \wedge \bigwedge_i |f_i| > M.$$

Since $\mathbb{Z}[\bar{f}]$ is Diophantine correct, we can choose $\bar{m} \in \mathbb{Z}$ such that

$$\mathbb{Z} \models \theta(\bar{m}) \wedge \bigwedge_i |\bar{m}| > M.$$

Let $v \in \mathbb{R}$. We have to find $u \in R$ such that $u > v$, and $\bar{f}(u) \in \mathbb{Z}^n$. Since the f_i are bounded on compact subsets of $[1, \infty)$, we can choose M so large that if $1 \leq u \leq v$ then $|\bar{f}(u)| \leq M$. By our choice of θ, there is some $u \geq 1$ such that $\bar{f}(u) = \bar{m}$. But $|\bar{m}| > M$, therefore $u > v$, as required.

Conversely, suppose there are arbitrarily large real numbers u such that $\bar{f}(u) \in \mathbb{Z}^n$.

Let ϕ be an open formula such that $\mathbb{Z}[\bar{f}] \models \phi(\bar{f})$. We shall prove that ϕ holds at some tuple of integers. It will follow from Lemma 6.2 that $\mathbb{Z}[\bar{f}]$ is Diophantine correct. But according to Lemma 6.1, for all sufficiently large $u \in \mathbb{R}$, $\mathbb{R} \models \phi(\bar{f}(u))$. Therefore, if we choose $u \in \mathbb{R}$ sufficiently large, with $\bar{f}(u) \in \mathbb{Z}^n$, then $\bar{f}(\bar{u})$ will be the required tuple of integers. ■

The following examples showing how these theorems relate to number-theoretic problems. In each case we will consider a family of rings parametrized by an algebraically independent tuple $\bar{r}$ varying over an open set $U \subseteq \mathbb{R}^n$, and we will use Theorem 6.4 to describe the $\bar{r} \in U$ for which the corresponding ring is Diophantine correct.

As a concession to readability, we shall make use of radicals to abbreviate formulas belonging to the language of ordered rings.

Example 1.

Let $A_{\bar{r}} = \mathbb{Z}[t, f_1(t) - r_1, \ldots, f_n(t) - r_n]$, where the f_i are nonconstant polynomials with real algebraic coefficients. Theorem 6.4 implies that $A_{\bar{r}}$ is Diophantine correct (for $\bar{r}$ algebraically independent) iff for every $\epsilon > 0$, and every $M > 0$, there are integers $m_0 \ldots m_n$ such that

$$\bigwedge_i (|m_i| > M) \wedge |f_i(m_0) - m_i - r_i| < \epsilon) . \tag{6.4}$$

The conditions for these inequalities to hold are described in [KO Kap. VIII Satz 9.10].

They are as follows: (6.4) is solvable in integers $\bar{m}$ for every $\bar{r}$ and ϵ iff no integer-linear combination of the f_i differs from an integer polynomial by a constant.

Example 2.

Let S be the closure, in $\mathbb{R}$, of the set of all real numbers of the form $\left|\frac{n^3-m^2}{\sqrt{n}}\right|$, as n and m range over the positive integers. Let A_r be the ring $\mathbb{Z}[t^2, t^3-\frac{r}{2t^2}]$, where r is a real transcendental. We shall prove that A is diophantine correct iff $r \in S$. Hall's conjecture [RI, Section C2, page 249] asserts that the non-zero values of $\left|\frac{n^3-m^2}{\sqrt{n}}\right|$, where n and m range over the positive integers, are all greater than some fixed positive constant c. Thus for $|r| < c$, A_r would fail to be Diophantine correct.

Following Theorem 6.4, we begin by eliminating t from the formula

$$\exists t \geq 1(y_1 = t^2 \wedge y_2 = t^3 - \frac{r}{2t^2}).$$

to obtain

$$r = 2y_1(y_1^{\frac{3}{2}} - y_2), \tag{6.5}$$

together with lower bounds $y_1 \geq k$, $y_2 \geq k$ for some k. Theorem (6.4) implies that A_r is Diophantine correct iff there are sequences of positive integers Y_1, Y_2 such that $2Y_1(Y_1^{\frac{3}{2}} - Y_2)$ tends to r.

To connect this with Hall's conjecture, observe that the ratio

$$\frac{\frac{y_1^3 - y_2^2}{\sqrt{y_1}}}{2y_1(y_1^{\frac{3}{2}} - y_2)} \tag{6.6}$$

is equal to

$$\frac{(y_1^{\frac{3}{2}} + y_2)}{2y_1^{\frac{3}{2}}}. \tag{6.7}$$

(We assume here that the y_i are chosen so that $y_1^{\frac{3}{2}} - y_2 \neq 0$.) If either the numerator or the denominator of (6.6) tends to r, then $y_1^{\frac{3}{2}} - y_2$ tends to 0. Hence (6.7) tends to 1. The numerator and denominator of (6.6) therefore have the same limit points as the y_i run through positive integers such that $y_1^{\frac{3}{2}} - y_2 \neq 0$.

Example 3.

Let S be the (topological) closure, in $\mathbb{R}$, of the set of values assumed by the quadratic form $x(2^{\frac{1}{3}}x - y)$, as x and y range over the integers. We shall prove that the ring $A_r = \mathbb{Z}[t, 2^{\frac{1}{3}}t - \frac{r}{t}]$, where r is a real number transcendental over $\mathbb{Q}$, is Diophantine correct iff $r \in S$. It is not known whether S has elements arbitrarily close to zero. See [LDA II.2, page 25].

Following Theorem 6.4, we eliminate t from

$$\exists t \geq 1(y_1 = t \wedge y_2 = 2^{\frac{1}{3}}t - \frac{r}{t}),$$

to obtain

$$r = y_1(2^{\frac{1}{3}}y_1 - y_2),$$

together with lower bounds $y_1 \geq k$, $y_2 \geq k$ for some k. By Theorem 6.4, it is now immediate that A_r is Diophantine correct iff $r \in S$.

Example 4.

Let

$$A_r = \mathbb{Z}[t, \alpha t - \frac{r}{t^{\frac{3}{2}}}],$$

where α is an algebraic irrational and r is transcendental. Then A_r is not Diophantine correct. To see this, we use Theorem 6.4 to obtain the condition: A_r is Diophantine correct iff there are sequences of positive integers X and Y tending to infinity, such that $X^{\frac{3}{2}}(\alpha X - Y)$ tends to r. Roth's theorem (see [CA, Chapter 6, Theorem 1]) implies that for any algebraic α, this sequence tends to $\pm\infty$.

Example 5.

Let $A = \mathbb{Z}[t, \sqrt{2}t - r_1, \sqrt{2}r_1 t - r_2]$, where r_1 and r_2 are algebraically independent over $\mathbb{Q}$. We will use Theorem 6.4 to show that A is not Diophantine correct. The field of coefficients has transcendence base r_1, r_2. By Eliminating quantifiers from

$$\exists t \geq 1\,(y_1 = t \wedge y_2 = \sqrt{2}t - r_1 \wedge y_3 = \sqrt{2}r_1 t - r_2),$$

we obtain, for θ,

$$r_1 = \sqrt{2}y_1 - y_2 \wedge r_2 = 2y_1^2 - \sqrt{2}y_1y_2 - y_3,$$

together with unimportant lower bounds on the y_i. By Theorem 6.4, A is Diophantine correct iff every open set in $\mathbb{R}^2$ containing (r_1, r_2) contains a point of the form

$$(\sqrt{2}m_1 - m_2, 2m_1^2 - \sqrt{2}m_1m_2 - m_3), \tag{6.8}$$

for integers m_i greater than any prescribed M. We can see that this is not the case from the identity

$$2m_1^2 - m_2^2 - 2m_3 = 2(2m_1^2 - \sqrt{2}m_1m_2 - m_3) - (\sqrt{2}m_1 - m_2)^2.$$

If we write (6.8) as (u, v), then the identity implies that $2v - u^2 \in \mathbb{Z}$. If there were a sequence of points (u_i, v_i) of the form (6.8) tending to (r, s), then $2v_i - u_i^2$ would eventually be equal to some fixed integer. This would imply $2s - r^2 \in \mathbb{Z}$. But this is impossible since r and s are algebraically independent. Thus A is not Diophantine correct.

7. References

[AML] Z. Adamowicz and G. Morales-Luna. *A Recursive Model For Arithmetic With Weak Induction.* The Journal of Symbolic Logic. vol. 50, 1985, 49-54.

[AS] E. Artin and O. Schreier. *Algebraische Konstruktion realler Körper.* Hamb. Abh. 5, 1927, 85-99.

[BO] A. Berarducci and M. Otero. *A Recursive Nonstandard Model of Normal Open Induction.* The Journal of Symbolic Logic. vol. 61, 1996, 1-14.

[BRU] G. Brumfiel. **Partially Ordered Rings and Semi-Algebraic Geometry**. Cambridge: Cambridge University Press: 1979.

[BS] Z. I. Borevich and I. R. Shafarevich. **Number Theory**. New York: Academic Press, 1966.

[CA] J. W. S. Cassels. **An Introduction to Diophantine Approximation**. New York: Haffner, 1972.

[CF] J. W. S. Cassels and A. Fröhlich. **Algebraic Number Theory**. New York: Academic Press, 1967.

[CHK] C. C. Chang and H. J. Kiesler. **Model Theory**. New York: American Elsevier, 1973.

[HO] W. Hodges. **Model Theory**. Cambridge: Cambridge University Press, 1994.

[HW] G.H. Hardy and E.M. Wright. **An Introduction to the Theory of Numbers**. Oxford: Oxford University Press, 1979.

[KO] J. F. Koksma. **Diophantische Approximationen**. New York: Chelsea, 1936.

[LA] S. Lang. **Algebra**. New York: Addison Wesley, 1993.

[LDA] S. Lang. **Introduction to Diophantine Approximations**. New York: Springer, 1995.

[MMP] D. Marker M. Messmer and A. Pillay. **Model Theory of Fields**. New York: Springer, 1996.

[MAT] Y. Matiyasevich. **Hilbert's Tenth Problem**. Boston: The MIT Press, 1993.

[MON] M. Moniri. *Recursive Models of Open Induction of Prescribed Finite Transcendence Degree* > 1 *with Cofinal Twin Primes.* C. R. Acad. Sci. Paris, t.319, Série I, 1994, 903-908.

[MOR] L. J. Mordell. **Diophantine Equations**. New York: Academic Press, 1969.

[MM] A. Macintyre and D. Marker. *Primes and their Residue Rings in Models of Open Induction.* Ann. Pure and Applied Logic, vol.43, 1989, 57-77.

[NAR1] W. Narkiewicz. **Polynomial Mappings**. New York: Springer, 1991.

[NAR2] W. Narkiewicz. **Elementary and Analytic Theory of Algebraic Numbers**, New York: Springer, 1990.

[PF] A. Pfister. **Quadratic Forms with Applications to Algebraic Geometry and Topology**. Cambridge: Cambridge University Press, 1995.

[PS] S. Priess-Crampe. **Angeordnete Structuren: Gruppen Korper projektive Ebenen**. Berlin: Springer, 1983.

[RI] Paulo Ribenboim. **Catalan's Conjecture**. New York: Academic Press, 1994

[SE] J. P. Serre. **A Course in Arithmetic**. New York: Springer, 1973.

[SH] J. R. Schoenfield. **Mathematical Logic**. New York: Addison-Wesley, 1967.

[SHEP] J. Shepherdson. *A Nonstandard Model for a Free Variable Fragment of Number theory.* Bull. L'Acad, Pol. Sci., vol. 12, 1964, 79-86.

[VD1] Lou van den Dries. *Which Curves over* $\mathbb{Z}$ *Have Points in a Discretely Ordered Ring*? Trans. Am. Math. Soc., vol 264, 1981, 181-189.

[VD2] Lou van den Dries. *Some Model Theory and Number Theory for Models of Weak Systems of Arithmetic.* In **Model Theory of Algebra and Arithmetic** (L. Pacholski et al., editors), Lecture Notes in Mathematics, no. 834, New York: Springer, 1980, 346-362.

[VD3] Lou van den Dries. **Tame Topology and O-Minimal Structures**. Cambridge: Cambridge University Press, 1998.

[W] A. Wilkie. *Some Results and Problems on Weak Systems of Arithmetic.* **Logic Colloquium '77** (A. Macintyre et al., editors.) New York: North Holland, 1978, 285-297.