COMMUNICATIONS ON PURE AND APPLIED MATHEMATICS, VOL. XXII, 131–151 (1969)

Decision Procedures for Real and p-Adic Fields*†

PAUL J. COHEN
Stanford University

In this paper we are concerned with the question of how to decide, by means of a recursive procedure, elementary statements about real or p-adic fields. Let us recall what we mean by an elementary statement. Assume we are given a set M and certain relations R_α defined on M, i.e., each R_α is a subset of the direct product of M with itself n_α times for some integer n_α. An elementary statement about the R_α is then a statement formed by using the logical symbols $\&$, $\sim$, $\vee$, $\Rightarrow$, $\Leftrightarrow$, $=$, symbols for variables x_1, $x_2 \cdots$, quantifiers, $\forall$, $\exists$, and the relation symbols R_α. Of course, these symbols must be used in the grammatically correct fashion with which we are all familiar. In the case of a field, we may take as the relations $R_1(x, y, z) \equiv (x + y = z)$ and $R_2(x, y, z) \equiv (x \cdot y = z)$. The important restriction on elementary statements is that they do not speak about *sets* of elements of M but only about individual elements of M. If we are given a set of statements, Σ, we say M is a model for Σ if the statements in Σ all hold in M.

1. Real Fields

Let us first examine the field of real numbers. Here we take $R_1(x, y, z) \equiv (x + y = z)$, $R_2(x, y, z) \equiv (x \cdot y = z)$, and $R_3(x, y) \equiv (x < y)$. Tarski [8] proved that the elementary theory of these relations is decidable, i.e., he gave a recursive procedure to decide the truth or falsity of any statement. Actually, his proof shows how the truth or falsity of any statement can be logically deduced from a certain set of statements about the real field. These are the axioms for a real closed field, [9]. They consist of the following:

(i) *The axioms for a field.* These involve only R_1 and R_2 and are well known.

(ii) *The order axioms.* These involve R_3 as well as R_1 and R_2, and say that $<$ is an ordering, and that $0 < x$, $0 < y$ implies $0 < x + y$ and $0 < xy$.

---

* This paper is a slightly revised version of the lecture given at the Courant Institute of Mathematical Sciences on the occasion of the Conference to dedicate Warren Weaver Hall in March, 1966. Reproduction in whole or in part is permitted for any purpose of the United States Government.

† The author wishes to acknowledge the support of the Office of Naval Research and the National Science Foundation during the preparation of this paper.

(iii) *The real-closure property.* This can be stated by saying that if $f(x) \equiv a_n x^n + \cdots + a_0$ is a polynomial and, for some $x_1 < x_2$, $f(x_1) < 0$ and $f(x_2) > 0$, then, for some y, $x_1 < y < x_2$, $f(y) = 0$. For each n this is clearly an elementary statement, and we take as axioms the statements corresponding to every integer n. Thus our set of axioms is countable.

We shall now prove Tarski's theorem. We shall use the symbols 0 and 1 with their customary meaning. Throughout the proof we use no properties of the real numbers other than those implied by the axioms for a real-closed field.

DEFINITION. A *polynomial relation* is a relation $A(x_1, \cdots, x_n)$ which is a Boolean function of relations of the form $p(x_1, \cdots, x_n) > 0$, where p is a polynomial with integral coefficients.

It is easy to verify that all the elementary statements of our theory can be brought into the form $Q_1 x_1 \cdots Q_n x_n A(x_1, \cdots, x_n)$, where the Q_i are quantifiers (either $\forall$ or $\exists$) and A is a polynomial relation.

THEOREM (*Tarski*). *If $A(x_1, \cdots, x_n)$ is a polynomial relation, $n > 1$, then we can find by a primitive recursive procedure a polynomial relation $B(x_2, \cdots, x_n)$ such that $\exists x_1 A(x_1, \cdots, x_n) \Leftrightarrow B(x_2, \cdots, x_n)$. If $n = 1$, there is a primitive recursive procedure which decides $\exists x_1 A(x_1)$.*

Since the polynomial relations can be enumerated in a natural fashion, it is clear what we mean by a primitive recursive procedure. By successively eliminating quantifiers, the theorem yields a procedure to decide any statement. The proof we give is similar in spirit to that of Tarski, although we believe ours is simpler. Another proof has been given by Seidenberg [7] who used a generalized version of Sturm's theorem. Our proof, although it uses ideas which are found in the proof of Sturm's theorem, proceeds directly by an induction on the theorem itself. We use the notation sgn x to mean -1, 0, 1 according as $x < 0$, $x = 0$ or $x > 0$.

DEFINITION. A real-valued function $f(x_1, \cdots, x_n)$ is *effective* if there is a primitive recursive procedure which to every polynomial relation $A(y, t_1, \cdots, t_m)$ assigns a polynomial relation $B(x_1, \cdots, x_n, t_1, \cdots, t_m)$ such that

$$A(f(x), t_1, \cdots, t_m) \Leftrightarrow B(x_1, \cdots, x_n, t_1, \cdots, t_m).$$

We observe some simple facts about effective functions. The effective functions are closed under composition. The functions $x + y$, $x \cdot y$, sgn x are effective. If $f(x)$ takes only finitely many values, all of which are integers, then f is effective if and only if for each k the relation $f(x) = k$ is equivalent to a

polynomial relation $B(x)$. If f is effective and takes only the values 0 and 1, and if g_1 and g_2 are effective, and if $h \equiv g_1$ if $f = 0$, $h \equiv g_2$ if $f = 1$, then h is effective.

LEMMA. 1.1. *$f(x_1, \cdots, x_n)$ is effective if there is a primitive recursive function which assigns to every d a polynomial relation $A(c_0, \cdots, c_d, x_1, \cdots, x_n, \lambda)$ such that*

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

Proof: This is just a simple consequence of the fact that all polynomial relations are constructed from inequalities $p(x) > 0$. A rigorous proof proceeds by induction on the number of terms in the polynomial relation.

The idea motivating the definition of effective functions is that although certain functions, such as $\sqrt{x}$, cannot be effectively "computed" from x, any question concerning $\sqrt{x}$ can be effectively reduced to a question about x. Thus, $\sqrt{x} > 3 \Leftrightarrow x > 9$.

DEFINITION. Let $p(x)$ be a polynomial in one variable. By a *graph* for $p(x)$ we mean a k-tuple $t_1 < t_2 < \cdots < t_k$ such that, in each interval of the form $(-\infty, t_1)$, (t_i, t_{i+1}), (t_k, ∞), p is monotonic. By the data of the graph we mean the k-tuple $\langle t_1, \cdots, t_k \rangle$, $\operatorname{sgn} p(t_i)$ for $1 \leqq i \leqq k$, $\operatorname{sgn} p(t_1 - 1)$, and $\operatorname{sgn} p(t_k + 1)$.

We shall now prove the following two theorems by induction on n.

THEOREM A_n. *There are effective functions of $a_0, \cdots, a_n$ which give the data for a graph of $p(x) \equiv a_n x^n + \cdots + a_0$. More precisely, there are $2n$ effective functions of $a_0, \cdots, a_n$, namely, $t_i(a)$, $\operatorname{sgn} p(t_i(a))$, where $1 \leqq i \leqq n - 1$, $\operatorname{sgn} p(t_1(a) - 1)$ and $\operatorname{sgn} p(t_{n-1}(a) + 1)$, such that $t_1(a) < \cdots < t_{n-1}(a)$ form a graph for $p(x)$.*

THEOREM B_n. *Let $p(x) \equiv a_n x^n + \cdots + a_0$. There are $n + 1$ effective functions of $a_0, \cdots, a_n$, namely $k(a)$ and $\xi_1(a) < \xi_2(a) \cdots < \xi_n(a)$, such that $\xi_1(a), \cdots, \xi_{k(a)}(a)$ are all the roots of $p(x)$.*

In the proofs of these theorems we shall use without proving it the fact that certain simple functions we encounter are indeed effective. The case $n = 0$ of the theorem being trivial, assume both theorems have been proved for all values less than a given n. We now prove Theorem A_n as follows: Consider the polynomial $p'(x)$. Its coefficients are effective functions of those of p. By Theorem B_{n-1}, its zeros lie among $\xi_1, \cdots, \xi_{n-1}$, where ξ_i are effective. These ξ_i can be taken as defining a graph for p and since ξ_i are effective, so are $\operatorname{sgn} p(\xi_i)$, $\operatorname{sgn} p(\xi_1 - 1)$, $\operatorname{sgn} p(\xi_{n-1} + 1)$.

To prove Theorem B_n, let $t_1 < \cdots < t_{n-1}$ define an effective graph for p, which is possible by virtue of Theorem A_n. By examining $\operatorname{sgn} p(t_i)$, $\operatorname{sgn} p(t_1 - 1)$, $\operatorname{sgn} p(t_{n-1} + 1)$, we can determine the number of roots of p effectively. In each interval $(-\infty, t_1)$, (t_i, t_{i+1}), (t_{n-1}, ∞) there is at most one root of p, and there is also the possibility that some of the t_i are roots of p. To show that the roots of p are effective, we consider for example the case of a possible root ξ between t_i and t_{i+1}. The other cases are handled quite similarly. By virtue of Lemma 1.1, it is sufficient to show that if $q(x) \equiv c_0 x^m + \cdots + c_m$, $\operatorname{sgn} q(\xi)$ is an effective function of c_i and the coefficients of p. Let $\tilde{q}(x)$ be the remainder obtained by dividing $p(x)$ into $q(x)$. Its coefficients are effective functions of the coefficients of p and the c_i. Also $\deg \tilde{q} < n$, and $\tilde{q}(\xi) = q(\xi)$. This means that by replacing q by $\tilde{q}$ we can assume that $\deg q < n$. Let $u_1 < u_2 < \cdots < u_n$ define an effective graph for q. We now claim that there is an effective function of the coefficients of p and q which gives us the position of ξ relative to the u_i, i.e., tells us, for which i, $u_i > \xi$ or whether $u_i = \xi$. This, of course, will in turn determine $\operatorname{sgn} q(\xi)$ and prove the theorem. Suppose, for definiteness, $t_1 < \xi < t_2$. There are two cases to distinguish:

(i) no u_i is in $[t_1, t_2]$,

(ii) only $u_\alpha, u_{\alpha+1}, \cdots, u_{\alpha+l}$ are in $[t_1, t_2]$.

Since the u_i and t_j are given effectively, these cases can be distinguished effectively. In the first case, the position of ξ relative to u_i is determined by the position of t_1 and t_2 relative to u_i. In the second case, by examining $\operatorname{sgn} p(u_\alpha), \cdots, \operatorname{sgn} p(u_{\alpha+l})$, $\operatorname{sgn} p(t_1)$ and $\operatorname{sgn} p(t_2)$ we can determine the position of ξ relative to the u_i. Thus, Theorem B_n is proved.

We can now prove Tarski's theorem. Let $A(x_1, \cdots, x_n)$ be a polynomial relation. Then A is a Boolean function of finitely many relations $p_i(x_1) > 0$, where each p_i is a polynomial whose coefficients are polynomials in $x_2, \cdots, x_n$. Since the roots of p_i are effective functions of $x_2, \cdots, x_n$, and there exist graphs for p_i which are effective functions of $x_2, \cdots, x_n$, it is clear that by examining the relative position of these various points one can easily determine what the various possibilities are for the sequence $\{\operatorname{sgn} p_i(x)\}$ for arbitrary x. This in turn means that we can find a polynomial relation $B(x_2, \cdots, x_n)$ such that $\exists x_1 A(x_1, \cdots, x_n) \equiv B(x_2, \cdots, x_n)$.

The theorem of Tarski has found several applications. In studying differential equations, one is led to consider the function

$$d(\xi) = \inf \{|\xi - \alpha| \,|\, p(\alpha) = 0\},$$

where $p = p(x_1, \cdots, x_n)$ is a polynomial and $\alpha = (\alpha_1, \cdots, \alpha_n)$, $\xi = (\xi_1, \cdots, \xi_n)$, [3] p. 276. By Tarski's theorem, we can say that such functions are definable by polynomial relations and hence for each value coincide with one of finitely many algebraic functions. This in turn can be used to

conclude that the rate of growth of $d^{-1}(\xi)$ can be at most of the form $|\xi|^a$, where ξ is the variable in question and $a > 0$.

Another application is to Hilbert's seventeenth problem which may be found in [6]. We repeat it here. We use the fact about real fields that, if K is a real field and $a \in K$ is not a sum of squares, then in some ordering of K, a is negative. Let $f(x_1, \cdots, x_n)$ be a rational function with real coefficients which is non-negative for all real values of x_i for which the denominator is not zero. Let S be any real-closed field containing the field of real numbers. The decision procedure for real-closed fields may be applied to the statement

$$A \equiv \exists x_1 \cdots x_n (f(x_1, \cdots, x_n) < 0 \text{ and the denominator of } f \text{ is not zero}).$$

This will yield a polynomial relation involving the coefficients of f which is necessary and sufficient for A to hold in S. Since the order relation of the reals is unique and the coefficients of f are real, this polynomial relation holds in S if and only if it holds in the real numbers. Thus we have shown that f is non-negative if the x_i range over any real-closed field S. Since every real field can be extended to a real-closed field, f is non-negative if the x_i range over any real field. Let K be the field of rational functions in $x_1, \cdots, x_n$ with real coefficients. Assume f is not a sum of squares. Then we can order K so that f is negative since K is a real field. This means that if we think of f as an element of $K(t_1, \cdots, t_n)$, then f assumes a negative value when the variables are replaced by the elements x_i lying in the real field K. This is a contradiction, so f must be a sum of squares.

Thus, we have given a proof of the theorem of Artin that a non-negative rational function is a sum of squares.

2. p-Adic Fields

By a discrete valuation of a field K, we mean a map v of $K - \{0\}$ onto the integers $\mathbb{Z}$, such that

(i) $v(xy) = v(x) + v(y)$,
(ii) $v(x + y) \geqq \min(v(x), v(y))$.

We formally write $v(0) = \infty$. The ring of integers we denote by $I = \{x \mid v(x) \geqq 0\}$. $P = \{x \mid v(x) > 0\}$ is a maximal ideal in I, and I/P is called the residue class field R. More generally, if $P_k = \{x \mid v(x) \geqq k\}$, we put $R_k = I/P_k$. We say K is complete under v if, whenever $v(x_m - x_n) \to \infty$ as $m, n \to \infty$, then, for some x in K, $v(x - x_n) \to \infty$ as $n \to \infty$. An example of such a field is the field of all formal Laurent series $\sum_{i>-n} c_i t^i$, where the c_i range over some field R and $v(\sum c_i t_i) = n$ if $c_n \neq 0$ and $c_i = 0$ for $i < n$. Another example is the field of p-adic numbers. This is defined as follows: Let Q be the field of

rationals, p a prime, and let $v(n) = r$ if $n = p^r a/b$, where $(p, a) = (p, b) = 1$. The completion of Q with respect to v is called the field of p-adic numbers.

Throughout this section we shall assume that K is of characteristic zero and is complete under a discrete valuation v. The letter p will denote a fixed element of K such that $v(p) = 1$. We shall sometimes write $a \equiv b(\mathrm{mod}\, p^r)$ in place of $v(a - b) \geqq r$. The following theorem is the classical result known as Hensel's lemma.

THEOREM 2.1. *Let* $f(x) \equiv a_0 x^n + \cdots + a_n$, $a_i \in I$. *Assume* $\alpha \in I$ *and* $f(\alpha) \equiv 0(\mathrm{mod}\, p^{2r+1})$, $f'(\alpha) \not\equiv 0(\mathrm{mod}\, p^{r+1})$, $r \geqq 0$. *Then there is a unique* $\bar{\alpha}$ *in* I *such that* $f(\bar{\alpha}) = 0$ *and* $\alpha \equiv \bar{\alpha}(\mathrm{mod}\, p^{r+1})$.

Proof: We shall define a sequence α_n such that $f(\alpha_n) \equiv 0(\mathrm{mod}\, p^{2r+n})$, $\alpha_{n+1} \equiv \alpha_n(\mathrm{mod}\, p^{r+n})$, $\alpha_1 = \alpha$. Observe that, if the α_n satisfy the second condition, $f'(\alpha_n) \equiv f'(\alpha)(\mathrm{mod}\, p^{r+1})$, so $f'(\alpha_n) \not\equiv 0(\mathrm{mod}\, p^{r+1})$. To define α_n inductively, we set $\alpha_{n+1} = \alpha_n + p^{r+n}x$, and note that, for x in I,

$$f(\alpha_{n+1}) \equiv f(\alpha_n + p^{r+n}x) \equiv f(\alpha_n) + p^{r+n}xf'(\alpha_n)(\mathrm{mod}\, p^{2r+2n}) .$$

Since $2r + 2n \geqq 2r + n + 1$, setting $x = -f(\alpha_n)/p^{r+n}f'(\alpha_n)$, we have x in I and $f(\alpha_{n+1}) \equiv 0(\mathrm{mod}\, p^{2r+n+1})$ and $\alpha_{n+1} \equiv \alpha_n(\mathrm{mod}\, p^{r+n})$. Clearly, the α_n converge to the desired $\bar{\alpha}$. The uniqueness follows from the fact that any such $\bar{\alpha}$ is seen by induction to satisfy $\bar{\alpha} \equiv \alpha_n(\mathrm{mod}\, p^{r+n})$.

Our basic object now is to show that there is a decision procedure for classical p-adic fields. More generally, we shall show that there is a procedure to reduce any question about any field K which is complete under a discrete valuation to questions concerning the residue class field R or the rings R_k for some finitely many k. Our example of formal power series shows that we can indeed only hope to reduce questions to questions about R at best, since otherwise we would have a decision procedure valid for any field R. Our idea is to imitate what was done in the case of the real field. Complications are introduced because of the fact that the value group in this case is the group of integers $\mathbb{Z}$, whereas in the real case sgn x takes only three values. Also, the statements we consider will include questions about $\mathbb{Z}$ so that we essentially must reprove the result of [5] giving a decision procedure for $\mathbb{Z}$ as an additive group. Our first task is to give the analogue of polynomial relations. This means, intuitively, saying which relations $A(x_1, \cdots, x_n)$ can be determined by performing certain calculations on $x_1, \cdots, x_n$. We do this by speaking in terms of functions. The functions we shall consider may have their variables in four possible types of domains, and similarly for their ranges. Of course, the domains and ranges are

to be specified when the function is given. These domains are as follows:

(i) the field K,

(ii) the rings R_k for some fixed $k \geqq 0$,

(iii) the integers $\mathbb{Z}$ considered as an additive group,

(iv) a fixed finite set depending upon the function. For definiteness we can take this set as $\{0, 1, \cdots, n\}$ for some n. A variable ranging over such a set will be called a *discrete* variable.

We next define a class of functions which we call *simple* functions. In our definition, we do not always make explicit the type of domain and range these functions have if it is clear from the context.

DEFINITION 1. The class of simple functions is defined as the smallest class $\mathscr{S}$ of functions satisfying the following properties:

1. $f(x_1, \cdots, x_n) \in \mathscr{S}$, where f is a polynomial with integral coefficients and the x_i are either all K variables or R_k variables for some k.

2. Let $f(x) = 0$ if x is not integral and let $f(x)$ be the image of x in R_k if it is. Then $f \in \mathscr{S}$.

3. The function $v(x)$ is in $\mathscr{S}$, where x is either a K variable or R_k variable. (Recall that $v(0)$ is undefined.)

4. $x + y$, $x - y$, $x + a$, $[x/n]$ are in $\mathscr{S}$, where x, y are $\mathbb{Z}$ variables, a is a fixed element of $\mathbb{Z}$, and n is a fixed positive integer. Here $[y]$ denotes the greatest integer in y.

5. sgn x is in $\mathscr{S}$, where x is a $\mathbb{Z}$ variable and the range is the set $(-1, 0, 1)$.

6. If $f(0) = 0$, $f(x) = 1$ if $x \neq 0$, then $f \in \mathscr{S}$, where x is either a K variable or R_k variable.

7. Let x_1 be a discrete variable (by definition taking only finitely many values), and $f(x_1, \cdots, x_n)$ such that $f(c, x_2, \cdots, x_n)$ is in $\mathscr{S}$ for each discrete value c. Then $f(x_1, \cdots, x_n)$ is in $\mathscr{S}$.

8. The composition of functions in $\mathscr{S}$ is in $\mathscr{S}$. The projections

$$f(x_1, \cdots, x_n) = x_i$$

are in $\mathscr{S}$. The constant functions are in $\mathscr{S}$.

9. The function $a \to p^a$ from $\mathbb{Z}$ into K is in $\mathscr{S}$.

10. Let $A(x_1, \cdots, x_n)$ be a formula involving possibly bound variables. *All* variables including bound variables are assumed to be R_k variables and the formula is constructed from the relations $=$, $+$, $\cdot$, the constants 0, 1 and p considered as elements of R_k and the relation $v(x) = i$, where $0 \leqq i < k$. The function $f(x_1, \cdots, x_n)$ defined to be 0 or 1 according as $A(x_1, \cdots, x_n)$ does or does not hold is a simple function.

DEFINITION 2. A simple function which takes only the values 0 and 1 is called a *test function*.

DEFINITION 3. A function $f(x_1, \cdots, x_n)$ is an *effective function* if there is a primitive recursive procedure which assigns to every test function

$$\varphi(u, t_1, \cdots, t_r)$$

another test function ψ such that $\varphi(f, t_1, \cdots, t_r) = \psi(x_1, \cdots, x_n, t_1, \cdots, t_r)$.

DEFINITION 4. Assume we have a k-valued function of $x_1, \cdots, x_n$, i.e., we assign to $(x_1, \cdots, x_n)$ a k-tuple $(f_1, \cdots, f_k)$ defined up to order. We say that our function is effective if there is a primitive recursive procedure which assigns to every finite set of test functions φ_i test functions ψ_i such that for each $x_1, \cdots, x_n$, and *some* permutation of $f_1, \cdots, f_k$, we have

$$\varphi_i(f_1, \cdots, f_k, t_1, \cdots, t_r) = \psi_i(x_1, \cdots, x_n, t_1, \cdots, t_r) .$$

Remark. The point of the above definition is that we are not interested in actually ordering the k-tuple, since that would involve introducing a choice function, but only in asking questions about the f_k. Clearly by enumerating all the test functions we could even assume that we can find a correspondence $\varphi_i \to \psi_i$ such that for, some fixed permutation of the f_j, the statement in the definition holds for all i. However, we do not need this fact.

LEMMA 2.1. *Let $A(x, t_1, \cdots, t_m)$ be a formula as in Definition* 1.10. *Assume that for all t_i there are at most n values of x satisfying A. If $f_1, \cdots, f_r$ represent these solutions and $f_{r+1} = \cdots = f_n = 0$, where r depends on the t_i, then the f_j are effective functions in the sense of Definition* 4.

Proof: If we have an R_k variable x and apply a succession of simple functions to it, we either do this by means of Definition 1.10 or else we must at some stage apply the valuation function to some polynomial in x. In the latter case, since v takes only finitely many values on R_k, we can split into cases using Definition 1.10. In this way, it is easy to see that for R_k valued functions $f(x_1, \cdots, x_n)$, f is effective if and only if the conditions in Definitions 3 and 4 hold only for test functions ψ which are of the type of Definition 1.10. For the functions f_i which occur in Lemma 2.1 this is obvious.

LEMMA 2.2. *The composition of effective functions is effective. All simple functions are effective.*

Our next objective is to introduce the concept of the graph of a polynomial. In the real case this essentially meant trying to determine the intervals of positivity and negativity. For the p-adic case it will mean determining how $v(f(x))$ depends on x. In the real case we divided the line into intervals. For the present case we give

DEFINITION 5. By a *cell* C in K we mean a set of the form

$$\{x \mid x = x_0 + p^a u, \ u \text{ integral}\}.$$

We say C has center x_0 and width a, and we call u a *parameter* for C. (Note that x_0 and u are not unique.) We call x_0, a the *data* for the cell. An *infinite cell* is a set of the form $\{x \mid v(x) < a\}$ and its *data* is the integer a.

Fact. Two finite cells are disjoint or else one contains the other.

DEFINITION 6. A *covering* of K by cells consists of finitely many cells and one infinite cell whose union is K. We say x belongs *properly* to C in the covering, if $x \in C$ and, if C' is in the covering, $x \in C'$, then $C \subset C'$.

Our object is now to show how to cover the p-adic numbers by cells in each of which a given polynomial behaves in a simple fashion. Actually, a polynomial will not necessarily behave well in an entire cell, but rather in a cell minus certain other cells in which the behavior is described differently. This is why we speak of *properly* belonging to a cell in the previous definition.

DEFINITION 7. Let $f(x) \equiv a_n x^n + \cdots + a_0$. By a *graph* for $f(x)$ we mean a covering of K with the following properties:

1. If the infinite cell is $\{x \mid v(x) \geqq \alpha\}$, then $n\alpha + v(a_n) < i\alpha + v(a_i)$ for $i < n$. Thus $v(f(x)) = v(a_n x^n)$ for x in the infinite cell.

2. Let $C = \{x \mid x = x_0 + p^\alpha u, \ u \text{ integral}\}$ be a cell in the covering. Expressed in terms of u, let $f(x) \equiv g(u) \equiv b_n u^n + \cdots + b_0$. Then one of the following cases holds:

Case I. For some c, $v(f(x)) = v(g(u)) \leqq \min_i v(b_i) + c$ for all x which belong properly to C. Clearly we have for all x in C, $v(f(x)) \geqq \min_i v(b_i)$.

Case II. For some $i \leqq n$, $v(b_i) + is < v(b_j) + js$ for $j \neq i$ and $0 \leqq s < \beta$, where β is some number possibly $+\infty$. We further assume that the points of $\{u \mid v(u) \geqq \beta\}$ do not belong properly to C and hence

$$v(f(x)) = v(g(u)) = v(b_i u^i)$$

for all x which belong properly to C.

Case III. There is exactly one root ξ of $g(u)$ in C and

$$g(u) = d_r(u - \xi)^r + \cdots + d_n(u - \xi)^n .$$

Also $v(d_i) > v(d_r)$ for $i > r$, and hence $v(g(u)) = v(d_r(u - \xi)^r)$.

It is seen that Case III is actually included in Case II but we prefer to call attention to it and treat it separately. In Case I, various terms of the polynomial

may have equal valuation and thus conceivably the valuation of the sum might be much greater than any term, but this is expressly forbidden. Thus no "hidden" cancellations take place in Case I. In Cases II and III, the behavior of the polynomial is more complicated but because of the special uniformizing parameter used we can read off $v(f(u))$.

DEFINITION 8. The *data* of a graph for $f(x)$ consists of

(i) data for the cells and the assignment to each cell of the case that covers it,

(ii) the integer c for each cell in which case I applies,

(iii) the root ξ and the numbers r and $v(d_r)$ for each cell in which case III applies.

The *order* of the graph is the maximum of the integers c in (i) and the number of cells.

We can now state our basic theorem.

THEOREM A_n. *If* $f(x) \equiv a_n x^n + \cdots + a_0$, *then there is a graph for* f *whose data are effective functions of* $a_0, \cdots, a_n$. *The order of the graph is bounded by a function depending only on* n *and* $v(j)$ *for* $j \leqq n$.

The method of proof is by induction on n. The case $n = 0$ is trivial so we assume the theorem is true for smaller values of n and proceed to prove Theorem A_n. For simplicity, we shall say that a function is effective if it is an effective function of the coefficients a_i. Assume we have a graph for

$$f'(x) \equiv na_n x^{n-1} + \cdots + a_1$$

given by a covering whose data are effective functions of ia_i and hence of a_i. (Recall that K is of characteristic zero so that $ia_i = 0$ implies $a_i = 0$.) It is clear, using Definition 1.4, that we can effectively determine finitely many α_i so that if $v(x) \neq \alpha_i$, then $v(a_j x^j) \neq v(a_k x^k)$ for $j \neq k$. Assume $\alpha_1 < \alpha_2 \cdots < \alpha_s$. Clearly Definition 7.1 holds in the infinite cell $\{x \mid v(x) < \alpha_i\}$. If we put $C_i = \{x \mid v(x) \geqq \alpha_i\}$, $D_i = \{x \mid v(x) \geqq \alpha_i + 1\}$, it is clear that for x in $D_i - C_{i+1}$, Case II holds, except that for D_s if $f(0) = 0$, Case III holds. Thus, our problem is to examine $f(x)$ in the sets $C_i - D_i$. Let Γ_j be the cells in an effective graph for $f'(x)$. The Γ_j then cover the sets $C_i - D_i$ and we shall examine the behavior of $f(x)$ in each $\Gamma_j \cap (C_i - D_i)$. Let us first consider the infinite cell Γ_1 which occurs in that graph. Let $\Gamma_1 = \{x \mid v(x) < \beta\}$, and assume some

$$S = C_i - D_i = \{x \mid v(x) = \alpha\}$$

is contained in Γ_1. This means that, since $f'(x) \equiv na_n x^{n-1} + \cdots + a_1$, if we put

$$(1) \qquad \gamma = v(na_n) + (n-1)\alpha < v(ia_i) + (i-1)\alpha \qquad \text{for} \qquad 1 \leqq i < n,$$

then $v(f'(x)) = \gamma$ for x in S. Put $x = p^{\alpha}y$ and

$$f(x) \equiv f_1(y) \equiv a_n p^{\alpha n} y^n + \cdots + a_0 .$$

Now, (1) implies that for $\gamma_1 = \gamma - c$, where $c = \sup v(i)$ for $1 < i < n$, $a_i p^{\alpha i}$ for $i \geqq 1$ is divisible by $p^{\gamma_1+\alpha}$. If $p^{\gamma_1+\alpha}$ does not divide a_0, then we are clearly in Case II. If $p^{\gamma_1+\alpha}$ does divide a_0, then $f_1(y) = p^{\gamma_1+\alpha}q(y)$, where

$$q(y) \equiv b_n y^n + \cdots + b_0$$

has integral coefficients. Also, $q'(y) = p^{-\gamma_1-\alpha}f_1'(y) = p^{-\gamma_1}f'(x)$, hence $v(q'(y)) = c$ for $v(y) = 0$. We are thus reduced to considering the behavior of $q(y)$ in $T = \{y \mid v(y) = 0\}$, and q has integral coefficients and $v(q'(y)) = c$ for y in T. By Hensel's lemma, if, for some y in T, $v(q(y)) \geqq 2c + 1$, then there is a unique root ξ with $y \equiv \xi(\mathrm{mod}\, p^{c+1})$. This means that in T, $v(q(y)) < 2c + 1$, except possibly for finitely many residue classes modulo p^{c+1} which contain roots. Using Lemma 2.1, we can effectively determine if there are any elements η of R_{2c+1} such that $q(\eta) \equiv 0(\mathrm{mod}\, p^{2c+1})$. For each such η, we consider the corresponding cell modulo p^{c+1} and observe that there are at most n such cells. In T minus the union of these cells, we have $v(q(y)) < 2c + 1$, and hence we are exactly in Case I for the polynomial $q(y)$. This in turn means that we are in Case I for the original polynomial $f(x)$.

For the exceptional cells, let us review the situation. We have a polynomial $q(y)$ with integral coefficients. The cell which we denote by I is defined by $y \equiv \xi(\mathrm{mod}\, p^{c+1})$, with $v(\xi) \geqq 0$, and $0 \leqq v(q'(y)) \leqq c$ for y in I, and $q(y) \equiv 0(\mathrm{mod}\, p^{2c+1})$ for some y in I. We defer the analysis of such a case, but since it will occur again, we call it the *root case*.

Let us now turn to the behavior of the original polynomial $f(x)$ inside a cell Γ of the graph for $f'(x)$, where Γ is not an infinite cell. The analysis is very similar. Suppose Case I holds, and let the cell be defined by $v(y) \geqq 0$, where $x = x_0 + p^{\alpha}y$. Let $f(x) \equiv g(y) \equiv b_n y^n + \cdots + b_0$. Then

$$f'(x) \equiv p^{-\alpha}g'(y) \equiv p^{-\alpha}nb_n y^{n-1} + \cdots + p^{-\alpha}b_1 .$$

Let $\beta = \min v(ib_i)$. Since we are in Case I, we can say that, for y properly in Γ, $-\alpha + \beta \leqq v(f'(x)) \leqq -\alpha + \beta + c$. Let $c' = \max v(i)$, $1 \leqq i \leqq n$, so that $p^{-\beta+c'}$ divides all the coefficients of $g(y)$ with the possible exception of b_0. If it does not divide b_0, then clearly $g(y)$ is in Case II with the term b_0 dominating. If it does divide b_0, then $p^{-\beta+c'}g(y) \equiv h(y) \equiv d_n y^n + \cdots + d_0$, where $v(d_i) \geqq 0$ and $0 \leqq v(h'(y)) \leqq c + c' = c''$ for y properly in Γ. Again, by Hensel's lemma, if any residue class of y modulo $p^{2c''+1}$ has any point belonging properly to Γ, and $v(h(y))$ is not bounded by $2c'' + 1$, then there is one and exactly one root in that

residue class. If $v(h(y))$ is bounded by $2c'' + 1$, we are in Case I for h and hence for $f(x)$. If there is a root, then the residue class is describable by an effective function and we are again in what we have called the root case, and we defer the analysis.

Assume Γ is a cell for which $f'(x)$ is in Case II. Again, let Γ be $\{y \mid v(y) \geqq 0\}$, where $x = x_0 + p^{\alpha}y$, and let $f(x) \equiv g(y) \equiv b_n y^n + \cdots + b_0$. As in our first analysis where Γ was infinite, we can cover Γ by cells so that $g(y)$ is always in Case II, except for finitely many sets of the form $S = \{y \mid v(y) = \beta\}$. The number of such S is clearly bounded by $(n + 1)^2$. Put $y = p^{\beta}z$, then

$$g(y) \equiv h(z) \equiv b_n p^{\beta n} z^n + \cdots + b_0 .$$

Since f' is in Case II and we assume that S belongs properly to Γ, we have for some i

$$\gamma = v(p^{\beta(i-1)} i b_i) < v(p^{\beta(j-1)} j b_j) \qquad \text{for} \qquad j \neq i .$$

As before, if $c = \max v(i)$, $1 \leqq i \leqq n$, $p^{-\gamma-\beta+c}$ divides the coefficients of $h(z)$ with the possible exception of b_0. If it does not divide b_0, then we are in Case II with b_0 dominating. If it does, then we set $k(z) = p^{-\gamma-\beta+v}h(z)$ so that $k(z)$ has integral coefficients and $v(k'(z)) \leqq c'$ for suitable c' if $v(z) = 0$. Using Hensel's lemma as before, we shall be in Case I except for possibly finitely many cells which will be in the root case.

The case when f' is in Case III is already covered by our discussion for Case II with the sole difference that the root ξ of f' may also be a root for f which may put f in Case III.

We now turn to the root case. Changing notation, we are given

$$f(x) \equiv a_n x^n + \cdots + a_0 ,$$

a_i integers, and a residue class V modulo p^{c+1} such that for some x_0 in V, $v(f'(x_0)) \leqq c$ and $v(f(x_0)) \geqq 2c + 1$. We shall first show that the unique root ξ of $f(x)$ in V is an effective function of the a_i. If we grant this and write $x = \xi + p^{c+1}y$, $f(x) \equiv g(y) \equiv b_n y^n + \cdots + b_1 y$, then $g(y)$ can be analyzed exactly as before but now with the assurance that the root case can no longer be encountered since the only root in V is $y = 0$. Thus we can construct a graph for $f(x)$ valid in V. We now show that ξ is effectively given.

LEMMA 2.3. *Let $h(x_1, \cdots, x_n)$ be a K-valued function. Assume that for each m, if $g(y) = u_m y^m + \cdots + u_0$, then $v(g(h))$ is an effective function of the x_i and u_j, and that for each c the residue class of $g(h)$ modulo p^c is also an effective function of the same variables. Further, assume that the dependence on m is recursive, i.e., in Definition 3 the*

function which assigns ψ_i to φ_i is recursive in m. Then $h(x_1, \cdots, x_n)$ is an effective function of the x_i.

The proof of this lemma is a formal consequence of the definitions and is left to the reader.

Now, in the root case, we must thus investigate $v(g(\xi))$ and the residue class of $g(\xi)$ modulo $p^{c'}$ for some c'. (In the following, c' will always represent an integer which is uniformly bounded from above.) By the Euclidean algorithm we may assume that $\deg g < \deg f$, so that g has an effective graph. If ξ lies in a cell Γ of the graph of g, by examining the various cases it is clear that both $v(g(\xi))$ and the residue class of $g(\xi)$ modulo $p^{c'}$ can be computed, provided we know $v(\xi - a)$, where a is some point in Γ, and the residue class of $p^{-\alpha}(\xi - a)$ modulo $p^{c'}$, where α is some integer. Thus our problem is to show that $v(\xi - a)$ is an effective function of a, and that the residue class of $p^{-\alpha}(\xi - a)$ is an effective function of a and α.

The residue class V which contains ξ is a residue class modulo p^{c+1}, but clearly for any $c' \geqq 2c + 1$ we can replace V by a residue class modulo $p^{c'}$ which contains ξ, since it is an effective operation to solve the equation $f(\eta) \equiv 0 (\mathrm{mod}\, p^{c'})$. If a is not in V, $v(\xi - a)$ is easily computable. As for the residue class of $p^{-\alpha}(\xi - \alpha)$ modulo $p^{c'}$, this is obvious unless

$$v(\xi - a) - c' \leqq \alpha \leqq v(\xi - a) .$$

Since $v(\xi - a) \geqq c'$, this class can be computed from that of ξ modulo $p^{c'}$ for some suitable c', which is again an effective operation.

Assume thus that a is in V. By expanding around a we obtain

$$f(x) = f(a) + f'(a)(x - a) + e_2(x - a)^2 + \cdots + e_n(x - a)^n ,$$

where e_i are integral. Thus

$$0 = f(a) + f'(a)(\xi - a) + e_2(\xi - a)^2 + \cdots + e_n(\xi - a)^n .$$

Recall that $v(f'(a)) \leqq c$. Since V is a residue class modulo $p^{c'}$ with $c' \geqq 2c + 1$, $v(\xi - a) \geqq c + 1$. Then

$$v\left(\frac{-f(a)}{f'(a)} - (\xi - a)\right) = v\left(\frac{1}{f'(a)}(e_2(\xi - a)^2 + \cdots)\right) \geqq v(\xi - a) + 1 .$$

Thus $v(\xi - a) = v(f(a)/f'(a))$, and so $v(\xi - a)$ has been computed effectively. Let $\beta = v(\xi - a)$ and assume we are required to compute the class of $p^{-\alpha}(\xi - a)$

modulo $p^{c'}$. We can assume of course that $\alpha \leqq \beta$. The above equation yields

$$v\left(-p^{-\alpha}\frac{f(a)}{f'(a)} - p^{-\alpha}(\xi - a)\right) \geqq v(p^{-\alpha}(\xi - a)) + v(\xi - a) - c \geqq v(\xi - a) - c\,.$$

This means that if V is a class modulo $p^{c''}$ and c'' is large enough, then the residue classes of $p^{-\alpha}(\xi - a)$ and $-p^{-\alpha}f(a)/f'(a)$ agree modulo $p^{c'}$. Thus, that residue class is effectively computable. This in turn completes the proof of our theorem.

3. Elimination of Quantifiers

Having shown that polynomials have effective graphs, we next show how to eliminate quantifiers.

THEOREM 3.1. *Let $T(x_1, \cdots, x_n)$ be a test function. Then there is a test function U such that $\exists x_1 T(x_1, \cdots, x_n) = 1 \Leftrightarrow U(x_2, \cdots, x_n) = 1$.*

Proof: Let T be a test function and assume first that x_1 is a field variable. Writing x in place of x_1, it is clear that eventually the variable x must occur in the form $v(p(x))$ or Res $(p(x))$ for some polynomial p. In the first case, by looking at the graph for $p(x)$ we can distinguish finitely many cases, according to which cell x lies in. Then $v(p(x))$ will be simply a function of $v(x - \xi)$, where ξ is a suitable element in the cell, and possibly the residue class of $p^{-\alpha}(x - \xi)$ for suitable α and ξ. In either case, we introduce new variables $v(x - \xi)$ and the class of $p^{-\alpha}(x - \xi)$, and express $v(p(x))$ in terms of that variable. One treats the case of Res $(p(x))$ similarly. Thus we have replaced every occurrence of x by new $\mathbb{Z}$ or R_k variables which are functions of x, but we must add a condition which expresses the fact that the cells represented by these variables have a non-empty intersection so that they all arise from the same x. We have thus reduced the relation $\exists x T(x) = 1$ to the form

$$\exists z_1 \exists z_1 \cdots \exists z_r U(z_1, \cdots, z_r, x_2, \cdots, x_n) = 1\,,$$

where z_i are $\mathbb{Z}$ or R_k variables. We next show how to eliminate R_k variables. If ξ is such a variable, eventually every occurrence of ξ must terminate in an expression of the form $v(p(\xi))$. Since $v(p(\xi))$ takes only k possible values, we can see that the truth value of the relation depends only upon knowing what the possible distributions of $v(p_i(\xi))$ are. By Definition 1.10, the unbound variables can be replaced by simple functions. It remains to show how to eliminate $\mathbb{Z}$ variables.

Suppose we have a test function $T(n)$ depending only on a $\mathbb{Z}$ variable but involving other quantities to be thought of as parameters. We can apply to n

the functions within $\mathbb{Z}$, namely $cn + k$, $[n/c]$, and sgn n, where c is a fixed integer. One can also form p^n and then treat that quantity as a K-variable, which means ultimately that one encounters expressions such as $v(Q(p^{n_1}, \cdots, p^{n_r}))$ or $\mathrm{Res}_k\, Q(p^{n_1}, \cdots, p^{n_r})$. We shall show that the functions of n we generate in this fashion are of a very elementary character.

DEFINITION. A function h from $\mathbb{Z}$ to $\mathbb{Z}$ is called piecewise linear if for some constant c and each j, $0 \leqq j < c$, we have finitely many $\alpha_1, \cdots, \alpha_s$ such that $h(j + cx) = c^i x + m^i$ for $\alpha_i \leqq x \leqq \alpha_{i+1}$ (where $\alpha_0 = -\infty$, $\alpha_{s+1} = \infty$). The quantities α_i, c^i, m^i are called the data of the function. If h is defined on $\mathbb{Z}$ taking values in some arbitrary set but only finitely many different values, we say h is piecewise linear if, in the above notation, $h(j + cx)$ is constant for $\alpha_i \leqq x \leqq \alpha_{i+1}$. We define piecewise linear functions of more than one variable in the obvious analogous fashion.

We observe that the functions of Definition 1.4–5 are piecewise linear, and that the composition of piecewise linear functions is piecewise linear.

LEMMA 3.1. *If Q is a polynomial, $v(Q(p^{n_1}, \cdots, p^{n_r}))$ and $\mathrm{Res}_k\,(Q(p^{n_1}, \cdots, p^{n_r}))$ are piecewise linear functions of $n_1, \cdots, n_r$ whose data depend effectively on the coefficients of Q. Also the quantities c^i and c occurring in the definition of piecewise linear are uniformly bounded in terms of the degree of Q.*

Proof: Consider first $v(Q(p^{n_1}, \cdots, p^{n_r}))$. The proof proceeds by the number of *terms* in the polynomial Q. As a piecewise linear function of the n_i we can determine the terms of least valuation. If only one such term occurs, $v(Q)$ is determined. Assume two such terms occur for some values of the n_i. Let the terms be $a_1 x_1^{\lambda_1} \cdots x_r^{\lambda_r}$ and $a_2 x_1^{\mu_1} \cdots x_r^{\mu_r}$ and $a_1 = \epsilon_1 p^\alpha$, $a_2 = \epsilon_2 p^\beta$, where $v(\epsilon_1) = v(\epsilon_2) = 0$, then $p^\alpha x_1^{\lambda_1} \cdots x_r^{\lambda_r} = p^\beta x_1^{\mu_1} \cdots x_r^{\mu_r}$ for $x_i = p^{n_i}$. Then the sum of these two terms can be replaced by $(\epsilon_1 + \epsilon_2) p^\alpha x_1^{\lambda_1} \cdots x_r^{\lambda_r}$. Thus in this case $v(Q)$ can be reduced to $v(\bar{Q})$, where $\bar{Q}$ is a polynomial with one less term, and the result is proved. The function $\mathrm{Res}_k\,(Q)$ is handled by the same induction and we leave the proof to the reader.

If $T(n)$ is a simple function from $\mathbb{Z}$ to $\mathbb{Z}$, it follows by successive applications of the lemma that T is piecewise linear with data depending effectively on the parameters of T. Thus, if T is a test function, one can determine effectively if $\exists n(T(n) = 1)$. This completes the proof that all bound variables can be eliminated, and gives the required decision procedure.

4. Remarks

The fact that there is a decision procedure for the p-adic numbers was first proved by Ax and Kochen [1] and by a different method by Ershov [2]. Their

methods do not yield a primitive recursive procedure but are model-theoretic in nature. This means that they show that every statement is decidable from a certain set of axioms, and thus that if one enumerates the countably many possible proofs one will encounter either a proof or disproof of a given statement. Also their work held only for certain residue class fields, e.g., finite fields for which statements can be decided. Our method is in the nature of a relative decision procedure which reduces questions to questions about R_k.

By examining our proof, one can isolate the properties of fields with valuations that we have used. We have used the field axioms and the axioms for the valuation function. We have used Hensel's lemma which consists of countably many statements, one for each degree of the polynomial and for each integer k for which we hypothesize a root modulo p^{2k+1}. We also used certain properties of the additive group $\mathbb{Z}$ in our arguments and definitions concerning $[n/a]$. Namely, for each k, $\mathbb{Z}/k\mathbb{Z}$ is isomorphic to $\{0, 1, \cdots, k-1\}$. The particular value of $v(p_0)$ occurred where p_0 is a rational prime such that $v(p_0) > 0$ and both p_0 and $v(p_0)$ must be given as particular integers. Finally, we used the existence of a map $n \to p^n$ which is homomorphism of $\mathbb{Z}$ into K. We can say therefore that, if K and K' are two fields satisfying these axioms with the same values of p_0 and $v(p_0)$, and such that for each k the rings R_k and R'_k have the same true statements, K and K' have the same true statements.

All the operations we introduced for our simple functions seem natural, with the possible exception of the map $n \to p^n$. This map cannot be entirely avoided as is seen by the following: For given a, we can ask what is the condition that $\exists x(x^2 = a)$. If we assume $v(2) = 0$, Hensel's lemma implies that if $v(a) = 0$, the condition is that a have a square root modulo p. If $v(a) \neq 0$, then clearly $v(a)$ must be even, and if $n = \frac{1}{2}v(a)$, then a has a square root if and only if $b = ap^{-2n}$ does and $v(b) = 0$. This is the natural condition and it would seem there is no way to avoid introducing p^{-2n}. However, one can proceed as follows: In any given application, one encounters only finitely many cases of the exponentation function and only finitely many times that the homomorphism property of $n \to p^n$ is used. It is easy to prove, from the axioms put on the valuation group, that for finitely many n_i there exist $f(n_i) \in K$, such that, for finitely many relations of the form $\sum a_i n_i = 0$, $\prod_i f(n_i)^{a_i} = 1$. Using this, the condition that a have a square root, for example, can be formulated as follows: $v(a)$ is even and if b is any element of valuation $\frac{1}{2}v(a)$, then ab^{-2} has a square root modulo p_0. In general, one can obtain the result that, without assuming the existence of an exponential map, a decision procedure exists for our fields relative to questions about the residue class rings.

5. *p*-Adic Fields Versus Formal Power Series Fields

It is a theorem that if K is complete under a discrete valuation and R is its residue class field, then, if char $R = 0$, there exists a subfield $\bar{R}$ of K such that $\bar{R}$

is mapped isomorphically onto R by reduction modulo p. For the sake of completeness, we sketch the proof. We define a map φ of R into K such that Res $\circ$ φ = identity. Clearly char $K = 0$, so we define φ on the rationals to be the identity. If we let ξ_α be a transcendence basis of R over the rationals, then, if Res $\xi'_\alpha = \xi_\alpha$, clearly ξ'_α are algebraically independent over the rationals and we put $\varphi(\xi_\alpha) = \xi'_\alpha$. Assume φ has been defined on a subfield F of R. It will suffice to show that if α is algebraic over F, we can extend φ to $F(\alpha)$. Let $\alpha^n + c_1\alpha^{n-1} + \cdots + c_n = 0$ be the irreducible equation for α over F. Since char $F = 0$, the discriminant is not zero. Let $c'_i = \varphi(c_i)$. Then the equation $x^n + c'_1x^{n-1} + \cdots + c'_n = 0$ has a root modulo p in K. Also its discriminant is not congruent zero modulo p, so Hensel's lemma implies that there is a root α' such that α' modulo p is α. Putting $\varphi(\alpha) = \alpha'$ gives the required extension.

As a consequence of this theorem, we have that if char $R = 0$, the field K is isomorphic to the field of formal Laurent series with coefficients in R. On the other hand, if char $R \neq$ char K, as in the case of the p-adic number fields, K cannot possibly be a field of formal Laurent series. Nevertheless, the following result, in slightly less generality due to Ax and Kochen, holds:

THEOREM 5.1. *Let A be a statement about a field K complete under a discrete valuation which is constructed from simple functions. There exist finitely many primes p_i, such that if* char $R \neq p_i$, *where R is the residue class field, then the truth or falsity of A depends only on R (but not on R_k) and $v(n)$, where n ranges over some finite set S of rational integers.*

COROLLARY. *If A is a given statement, for all but finitely many p, it holds in the p-adic numbers if and only if it holds in $F_p((t))$, the field of formal Laurent series over $\mathbb{Z}_p$.*

The decision procedure we have given involves reducing questions to R_k so that it suffices to show that questions about R_k are already determined by R for all but finitely many primes.

The idea of the proof is that although we may not have formal power series expansions in R_k, we can always form such formal expansions relative to any finite number of conditions.

DEFINITION. If S is a finite set of polynomials in $\mathbb{Z}[x_1, \cdots, x_n]$, we say that the integers α_i are *independent* with respect to S if for every Q in S either $v(Q(\alpha_1, \cdots, \alpha_n)) = 0$ or $Q(\alpha_1, \cdots, \alpha_n) = 0$. Similarly if the α_i are in R_k.

Since we allow Q to have degree zero, our condition may mean that we are asserting that char R is not one of finitely many primes.

LEMMA 5.1. *Let S be a finite set of polynomials in $\mathbb{Z}[x_1, \cdots, x_m, y_1, \cdots, y_n]$. There is a set T of polynomials in $\mathbb{Z}[x_1, \cdots, x_m]$ such that if $\alpha_1, \cdots, \alpha_m$ are*

integers and independent with respect to T and $\beta_1, \cdots, \beta_n$ are elements in R, there exist integers β_i' such that $\beta_i \equiv \beta_i'(\mathrm{mod}\, p)$ and $\alpha_1, \cdots, \alpha_m, \beta_1', \cdots, \beta_n'$ are independent with respect to S.

Proof: We first reduce to the case $n = 1$. If we assume the result for $n = 1$, there is a set T' of polynomials in $\mathbb{Z}[x_1, \cdots, x_m ; y_1, \cdots, y_{n-1}]$ which have the required relation to S. By the result for $n - 1$, there is a set T in $\mathbb{Z}[x_1, \cdots, x_m]$ with the required relation to T'. If $\alpha_1, \cdots, \alpha_m$ are given and free with respect to T, there exist $\beta_1', \cdots, \beta_{n-1}'$ such that $\beta_i \equiv \beta_i'(\mathrm{mod}\, p)$ and $\alpha_1, \cdots, \alpha_m, \beta_1', \cdots, \beta_{n-1}'$ are free with respect to T'. Then there exists β_1' such that $\beta_1' \equiv \beta_1(\mathrm{mod}\, p)$ and α_i and β_j' are free with respect to S.

Assume $n = 1$. The proof proceeds by induction on the degrees in y of the polynomials in S according to the usual "lexicographic" ordering. We define the set T as the union of finitely many finite sets each corresponding to various possible cases. Since, if the result holds for a set T, it holds for any larger sets, this is justified. Let $P(x_1, \cdots, x_m, y)$ be the polynomial in S of least degree in y. If $v(P(\alpha_1, \cdots, \alpha_m, \beta)) = 0$, then P can be omitted from S since the condition is trivially fulfilled. Thus, first put in T the set T' corresponding to the set S with P removed. (This set has lower lexicographic ordering.) Assume then that $v(P(\alpha, \beta)) > 0$. Let

$$P = a_0(x_1, \cdots, x_m)y^r + \cdots + a_r(x_1, \cdots, x_m) .$$

Adjoin to T the set T' corresponding to the set S with P replaced by $a_1(x)y^{r-1} + \cdots + a_r(x)$ (which again has lower lexicographic ordering). Thus if $a_0(\alpha_1, \cdots, \alpha_m) = 0$ we are done. Assume $a_0(\alpha_1, \cdots, \alpha_m) \neq 0$. Add $a_0(x_1, \cdots, x_m)$ to T, which means that we can assume $v(a_0(\alpha)) = 0$. Now consider S' which is obtained from S as follows: First, P is in S'. If Q is in S, by the division algorithm we have

$$a_0^s(x_1, \cdots, x_m)Q = P \cdot A + Q_1 ,$$

where A and Q_1 are in $\mathbb{Z}[x_i, y]$ and the degree of Q_1 in y is smaller than that of Q. For each Q in S, put Q_1 in S'. Clearly S' has lower ordering than S. Adjoin to T the set corresponding to S'. Now, if $\alpha_1, \cdots, \alpha_m$ are independent with respect to T, let β' be chosen so that it satisfies the independence conditions for S'. Then $P(\alpha_i, \beta') = 0$. If $v(Q(\alpha_i, \beta)) > 0$, then $v(Q_1(\alpha_i, \beta)) > 0$; hence $Q_1(\alpha_i, \beta') = 0$, and thus $Q(\alpha_i, \beta') = 0$ and we are done. The only case left to consider is the case in which S consists of one polynomial P. Again, we can assume $v(P(\alpha_i, \beta)) > 0$. Let P' denote the derivative with respect to y, then, if $v(P'(\alpha_i, \beta)) = 0$, Hensel's lemma gives the result. If $v(P'(\alpha_i, \beta)) > 0$, let

$P'(x_i, y) = a_0(x_i)y^r + \cdots + a_r(x_i)$ and

$$a_0^s P = P' \cdot A + P_1,$$

where the degree of P_1 in y is less than that of P. Adjoin $a_0(x_i)$ to T as well as the set T' corresponding to the case where S' is the single polynomial $a_1(x_i)y^{r-1} + \cdots + a_r(x_i)$. Furthermore, if S' now denotes the set of P' and P_1, we also add to T the set T' corresponding to this last S'. As before, it is easy to see that the result then holds for the original set S. This proves the lemma.

Remark. We have also proved the lemma in the case in which the variables are all R_k variables since the proof carries over with no change.

LEMMA 5.2. *Let S be a finite set of polynomials in $\mathbb{Z}[x_1, \cdots, x_n, y_1, \cdots, y_k]$. There is a finite set T of polynomials in $\mathbb{Z}[x_1, \cdots, x_n]$ such that if $\alpha_1, \cdots, \alpha_n$ and β are elements in R_k, such that the α_i are independent with respect to T, then we can expand $\beta = \beta_1 + \beta_2 p + \cdots + \beta_k p^{k-1}$ such that $\alpha_1, \cdots, \alpha_n, \beta_1, \cdots, \beta_k$ are independent with respect to S.*

Proof: By Lemma 5.1, there are finite sets $T_0, T_1, T_2, \cdots, T_k$, where T_i consists of polynomials in $\mathbb{Z}[x_1, \cdots, x_n, y_1, \cdots, y_i]$, $T_k = S$, and each T_i bears the relation of Lemma 5.1 to T_{i+1}. We now assert that T_0 satisfies the requirements of Lemma 5.2. For, if $\alpha_1, \cdots, \alpha_n$ are independent with respect to T_0, then there is β_1 such that $\beta_1 \equiv \beta \pmod{p}$ and such that $\alpha_1, \cdots, \alpha_n, \beta_1$ are independent with respect to T_1. If $\beta \equiv \beta_1 + \beta_2 p + \cdots + \beta_i p^{i-1} \pmod{p^i}$ and $\alpha_1, \cdots, \alpha_n, \beta_1, \cdots \beta_i$ are independent with respect to T_i, there is a β_{i+1} in R_k such that $\beta_{i+1} \equiv p^{-i}(\beta - \beta_1 - \beta_2 p - \cdots - \beta_i p^{i-1})$ and $\alpha_1, \cdots, \alpha_n, \beta_1, \cdots, \beta_{i+1}$ are independent with respect to T_{i+1}. Since $T_k = S$, the lemma is proved.

In the following we use $\bar{t}$ to denote the residue class modulo p of t if t is integral.

LEMMA 5.3. *Let $A(x_1, \cdots, x_n)$ be a relation in R_k. Let R_k' be another residue class ring and φ an isomorphism from R onto R'. There exists a finite set S of polynomials depending only on A (and not on R_k or R_k') such that if*

$$x_i = \sum_{j=0}^{k-1} \alpha_{i,j} p^j, \qquad x_i \in R_k,$$

and

$$x_i' = \sum_{j=0}^{k-1} \alpha_{i,j}' p^j, \qquad x_i' \in R_k',$$

and $\alpha_{i,j}$ and $\alpha'_{i,j}$ are independent with respect to S and $\varphi(\bar{\alpha}_{i,j}) = \bar{\alpha}'_{i,j}$, then $A(x_1, \cdots, x_n)$ holds in R_k if and only if $A(x'_1, \cdots, x'_n)$ holds in R'_k.

Proof: We proceed by induction on the number of bound variables in A. If A has no bound variables, then A merely speaks about the valuation of certain polynomials in $\alpha_{i,j}$ and p^j. If we define S as the set of all polynomials which occur as coefficients of p^j, the lemma is clearly true. Thus it suffices to prove the lemma where A is of the form $\exists y B(x_1, \cdots, x_n, y)$, and the lemma is known to hold for B. Let T be the corresponding polynomials for B. Let us write

$$y = \beta_1 + \beta_2 p + \cdots + \beta_{k-1} p^{k-1}.$$

By Lemma 5.2, there is a set of polynomials S in $\alpha_{i,j}$ such that if $\alpha_{i,j}$ are free with respect to S, *any* y can be expanded so that $\alpha_{i,j}$ and β_i are free with respect to S. This means that if A is true in R_k and the element y is so expanded, we can find β'_i in R'_k such that $\beta'_i \equiv \varphi(\bar{\beta}_i) (\mathrm{mod}\, p)$ and $\alpha'_{i,j}$, β'_i are independent with respect to T. Clearly, if $y' = \beta'_1 + \beta'_2 p + \cdots + \beta'_k p^{k-1}$, then $B(x'_1, \cdots, x'_n, y')$ holds in R'_k which means $A(x'_1, \cdots, x'_n)$ holds in R'_k. This proves the lemma.

If there are no free variables, then the set S in Lemma 5.3 can only consist of constants, so that we have merely ruled out certain characteristics for R. This completes the proof of Theorem 5.1.

In [1], Ax and Kochen made a remarkable application of this result. In [4], Lang had proved the following theorem:

THEOREM 5.2. *In $F_p((t))$ or in any field of formal Laurent series over a finite field, let P be a homogeneous polynomial of degree d and n variables. If $n > d^2$, P has a non-trivial zero.*

For each d, if we consider a form of $d^2 + 1$ variables and degree d, the above theorem is a statement of the type we have investigated. Since the field $F_p((A))$ and the p-adic numbers have the same residue class rings, Theorem 5.1 implies:

THEOREM 5.3. *For each d, there are finitely many primes such that, in any field F complete with respect to a discrete valuation, if* char $\bar{F}$ *is not one of their primes, then any homogeneous polynomial of degree d, n variables, $n > d^2$, has a non-trivial zero.*

Our present method yields the possible exceptional primes as a primitive recursive function of the degree d.

Bibliography

[1] Ax, J., and Kochen, S., *Diophantine problems over local fields, I*, Amer. J. Math., Vol. 87, 1965, pp. 605–630. *II*, ibid., pp. 631–648. *III*, Amer. J. Math., Vol. 88, 1966, pp. 437–456.

[2] Ershov, Ju. L., *On the elementary theory of maximal normed fields*, Doklady Akad. Nauk USSR, Vol. 165, 1965, pp. 21–23. Translation, Soviet Math., Vol. 6, 1965, pp. 1390–1393.
[3] Hörmander, L., *Linear Partial Differential Operators*, Springer Verlag, Berlin, 1963.
[4] Lang, S., *On quasi algebraic closure*, Ann. of Math., Vol. 55, 1952, pp. 373–390.
[5] Presburger, M., *Über die Vollständigkeit eines gewissen Systems der Arithmetik ganzer Zahlen, in welchem die Addition als einzige Operation hervortritt*, Comptes-rendus du I Congrés des Mathématiciens des Pays Slaves, Warsaw, 1929, pp. 92–101, 395.
[6] Robinson, A., *Introduction to Model Theory and to the Metamathematics of Algebra*, North-Holland Publ. Co., Amsterdam, 1963.
[7] Seidenberg, A., *A new decision method for elementary algebra*, Ann. of Math., Ser. 2, Vol. 60, 1954, pp. 365–374.
[8] Tarski, A., *A Decision Method for Elementary Algebra and Geometry*, 2nd edit., revised, Berkeley and Los Angeles, 1951.
[9] van der Waerden, *Modern Algebra*, F. Ungar, New York, 1953.

Received September, 1968