On constructing models for arithmetic

DANA SCOTT (Chicago)

§ 0. Introduction. In geometry models have been used with great success for proofs of independence. In arithmetic the situation is considerably different: even though one can construct many kinds of models for this theory using general metamathematical methods, it has not yet been possible to apply these models in new independence proofs. No doubt one important fact is that arithmetic has a recursively unsolvable decision problem. Simple questions about existence of solutions of polynomial equations probably lead to unsolvable problems, though this fact has not yet been proved. Thus the first attempt to examine a proposed model will lead at once to difficult situations with the most straightforward combinations of elements under addition and multiplication. Of course, one would hope for an indirect proof that the model satisfies the axioms of arithmetic which would avoid such direct verifications, but this indirect method has not yet been found. Another point to remember in comparing geometry and arithmetic is that the axioms for first-order geometry can be given with sentences of universal-existential type (cf. Tarski [23]), while the axioms of first-order arithmetic must always involve arbitrarily many changes of quantifiers in their formulation. The effect of this state of affairs on building models is clear. One conclusion is that it may be more reasonable to try to construct models for interesting *fragments* or *subtheories* of arithmetic rather than for the whole of first-order arithmetic. Another conclusion is that one might well turn one's attention to questions of *definability* rather than independence, for such problems may find a more workable translation into model-theoretical terms. In any case only a scant beginning has been made in any of these directions.

In this paper in Section 1 some simple algebraic facts about ordered rings are given together with a result about

finite generation of models for arithmetic. In Section 2 a method is given for constructing models for all true sentences of arithmetic as homomorphic images of function rings which can be stated in purely ring-theoretical terms. The method is related to the well-known Skolem construction and is a special case of a general procedure that has been used by several authors. Certain natural modifications of the idea do not lead to models for all provable sentences as will be indicated. In Section 3 constructions within polynomial rings are shown not to give models, but some unsolved questions in this direction are stated. Finally in Section 4 topics of recursiveness and definability are discussed, and the ideas are related to Gödel's Incompleteness Theorem yielding another proof of this result.

The author should like to record his indebtedness to Simon Kochen, Georg Kreisel and Stanley Tennenbaum, with whom he has had many long hours of discussion. The enthusiastic and original ideas of these people have had considerable influence on the author's point of view, no doubt to a greater extent than has been properly indicated here in this expository account.

§ 1. Ordered rings. All rings considered will be *commutative rings with unit*. The notion of a (totally or linearly) *ordered ring* is assumed as known. To be somewhat more specific a ring is an algebraic structure of the form $\langle R, +, \cdot, 0, 1\rangle$, while an ordered ring is of the form $\langle R, +, \cdot, 0, 1, \leqslant\rangle$. This distinction is only important when we wish to discuss the first-order theory corresponding to a given ring, for the ordering relation is not always definable in terms of the plain ring structure. An *integral domain* (or simply *domain*) is a ring without zero divisors. A ring is called *formally real* if the zero of the ring is not the finite sum of any number of non-zero squares in the ring.

In the sequel in stating results the word "Proposition" will be used to apply to those facts that are either well-known or particularly easy to prove. They have been included only for emphasis and completeness.

PROPOSITION 1.1. *An ordered ring is always a formally real integral domain.*

Conversely, every formally real domain can be ordered, though not always in a unique way. In this connection see

van der Waerden [25], p. 242-244. An ordered domain is *densely ordered* if the ordering is dense in the sense that between any two elements there is a third. An ordered domain is *discretely ordered* if there are no "fractions" in the sense that there is no element between 0 and 1.

PROPOSITION 1.2. *An ordered domain is either densely ordered or discretely ordered.*

Proof. Suppose that the domain is not discretely ordered and let $0 < x < 1$. Suppose $a < b$, then $a < xa + (1-x)b < b$. Hence, the domain is densely ordered.

An ordered domain is *well-ordered* if every bounded non-empty subset has a least element. An ordered domain is *archimedean ordered* if whenever for elements a, b in the ring, $0 < a \leqslant b$, then there is an integer n such that $b \leqslant na$.

PROPOSITION 1.3. (i) *Every well-ordered domain is isomorphic to the rings of integers*;

(ii) *Every discretely and archimedean ordered domain is isomorphic to the ring of integers.*

The ring of integers will be denoted by Z. Clearly if we are to study other similar kinds of domains, the notion of well-ordering is too strong. The requirement can be weakened by applying the minimum condition not to all subsets of the ordered domain but only to those that are algebraically defined. An *algebraically defined* subset of a domain (ordered domain) consists exactly of those elements of the domain satisfying relative to the domain a certain first-order formula with one free variable involving symbols for $-$, $\cdot$, 0, 1 ($\leqslant$). An *algebraically well-ordered* domain is an ordered domain in which every non-empty bounded algebraically defined subset has a least element. An ordered domain is *inductive* if every algebraically defined subset containing 0 and closed under the function $x+1$ always includes all non-negative elements.

PROPOSITION 1.4. *An ordered domain is inductive if and only if it is algebraically well-ordered.*

PROPOSITION 1.5. *An inductive domain is always discretely ordered.*

It will be noticed that the usual terminology has been changed somewhat in this discussion. Instead of *models for arithmetic* we use the term *inductive domain*, and instead of *non-standard model for arithmetic* we refer to *non-archimedean*

inductive domains. This rather more colorful algebraic terminology, it is felt, conveys a better indication of the nature of the objects studied from a mathematical point of view.

In the integers and in many other rings, the ordering is uniquely determined by the ring structure. In particular, an ordered ring is *quadratically ordered* if every non-negative element is a (finite) sum of squares. The usual proofs in books on number theory can be used to establish the following.

PROPOSITION 1.6. *In an inductive domain every non-negative element is a sum of four squares.*

It turns out that the proper homomorphic images of inductive rings are never inductive (cf. Mendelson [12]). Indeed we can prove even more.

PROPOSITION 1.7. *If a quadratically ordered domain is discretely ordered, then no proper homomorphic image of the domain is formally real.*

Proof. Let D be a domain satisfying the hypothesis and let h be a (ring) homomorphism onto another domain which is not an isomorphism. Hence, there must be a *positive* element $a \in D$ such that $h(a) = 0$. Now $a \geqslant 1$, so that $a-1 = \sum_{i<n} b_i^2$, for suitable elements $b_0, \ldots, b_{n-1} \in D$. Thus $-1 = \sum_{i<n} (h(b_i))^2$ in the image domain which clearly implies that it is not formally real.

Finally we shall discuss in this section questions of how inductive domains can (or better cannot) be generated. The notion of an algebraically (first-order) definable set was explained above, and *algebraically definable* functions may be introduced in a similar way. A function ($f(x)$ say) will be called *parametrically definable* in a domain D, if there is an element a in D and an algebraically definable function $g(x, y)$ over D such that $f(x) = g(x, a)$ for all x in D. A sequence $\langle f_0(x), f_1(x), \ldots \rangle$ of functions indexed by integers will be called *parametrically definable* if there is an a in D and an algebraically definable function $g(x, y, z)$ such that $f_n(x) = g(x, a, n)$ for all elements x of D and integers n. Here we consider the integer n also as an element of D. The notion of a *parametrically definable sequence of elements* can be explained in an analogous way.

A straight-forward use of algebraic well-ordering or the induction axiom will show that parameters (which were not used at first) can be allowed. In particular one proves

LEMMA 1.8. *If $f(x)$ is a parametrically definable function in an inductive domain D and $a \geqslant 0$, then the set*

$$\{f(x):\ 0 \leqslant x < a\}$$

has a least upper bound in D.

COROLLARY 1.9. *In a non-archimedean inductive domain, no parametrically definable sequence of elements can contain all elements of the domain.*

Proof. Let the sequence be given by $f(n)$ where $f(x)$ is parametrically definable. Let a be chosen so that $a > n$ for all integers n. Then apply 1.8.

THEOREM 1.10. *No non-archimedean inductive domain can be generated from a parametrically definable sequence of elements by making use of a parametrically definable sequence of functions.*

Proof (in outline). Let the sequence of elements be given by $f(n)$ and the sequence of functions by $g(x, m)$. In an inductive domain consider the least subring containing the elements and closed under the given functions. All the possible ways of writing down elements made up from the $f(n)$'s by applying the $g(x, m)$'s and addition and multiplication can be indexed in a recursive way independent of any special character of f and g. Thus, I say that the subring of this inductive domain is the range of a parametrically definable sequence of elements. The conclusion follows by 1.9.

It of course follows that no non-archimedean inductive domain can be a finitely generated ring. Further, no finite number of definable functions can be of any help in generating the whole domain. This fact at once rules out many standard algebraic ways of obtaining domains which would be inductive.

§ 2. Function rings. Let Z be the ring of integers, and let I be an infinite index set. (The cardinal number of I should not be too large because of some technical reasons. Cardinals such as $\aleph_0$, $2^{\aleph_0}$, $2^{2^{\aleph_0}}$ are quite suitable.) By Z^I we shall understand the *complete direct power* of Z with index I, that is the ring of all functions from I into Z with the usual pointwise operations. Notice that Z^I is not integral domain and only is endowed with a *partial ordering* rather than a linear ordering (the pointwise partial ordering, of course). Now Z^I has many ideals, and in particular it has many prime ideals P which give integral domains Z^I/P. Maximal ideals M are prime, but Z^I/M is always a field and not an inductive domain.

Consider then the question whether any homomorphic images of Z^I are inductive domains. Projection of Z^I onto a particular coordinate gives Z as an image. The corresponding ideal of Z^I is principal. Indeed all principal prime ideals of Z^I are either of this form or come from the composition of a projection of Z^I onto Z followed by a homomorphism onto $Z/(p)$, where p is a prime. These homomorphisms are not interesting. What needs to be investigated is whether a quotient Z^I/P, where P is a non-principal ideal, is ever inductive. Since maximal ideals did not yield the desired result, one should apply the principle of passing from one extreme to another.

THEOREM 2.1. *If P is a non-principal minimal prime ideal of Z^I, then Z^I/P is a non-archimedean inductive domain of uncountable cardinality.*

To understand the hypothesis of 2.1 better, recall the fact that the class of prime ideals of a ring is closed under the intersection of chains. Hence, by Zorn's Lemma every prime ideal contains a minimal prime. Now it is very easy to construct in Z^I a maximal ideal which contains no principal prime ideals simply by taking a maximal extension of the ideal of those functions in Z^I which are zero on all but a finite number of coordinates. These two applications of Zorn's Lemma show that the hypothesis is not vacuous. However, a closer analysis of the notion of a minimal prime ideal will show that so many uses of the axiom of choice were unnecessary.

Suppose that R is any ring with unit. We shall say that R has *enough idempotents* if there is a function e: $R \to R$ such that for all x, y in R the following equations are satisfied:

(i) $e(0) = 0$;

(ii) $e(x \cdot y) = e(x) \cdot e(y)$;

(iii) $e\big(e(x)\big) = e(x)$;

(iv) $e(x) \cdot x = x$.

It is easy to show from these conditions that if $x^2 = x$, then $e(x) = x$, that $e(x)^2 = e(x)$, and that the function e is unique. Professor I. Kaplansky pointed out to the author that the existence of the function e is equivalent to assuming that the annihilator of every element of R is a principal ideal generated by an idempotent. He had used this latter condition in investigating minimal prime ideals in another connection. It is clear that integral domains have enough idempotents, for set $e(x)$ equal to 0, if $x = 0$, and equal to 1, if $x \neq 0$. Also

Z^I has such a function e: if x is in Z^I, then $e(x)$ is the characteristic function of the non-zero coordinates of x. (In fact, the class of rings satisfying the condition is closed under arbitrary direct product.)

LEMMA 2.2. *If R has enough idempotents, and P is a prime ideal of R, then P is minimal if and only if $e(P) \subseteq P$.*

Remark. The condition given in 2.2 means that P is closed under e, or in other words the homomorphism determined by P also preserves the function e. If $e(P) \subseteq P$, it is easy to see that $P = R \cdot e(P)$, that is, P is completely determined by the idempotents it contains. Also, $e(P)$ will be a prime ideal in the Boolean algebra of idempotents of R.

Proof of 2.2 (in outline). Let P be any prime ideal. Consider

$$Q = e^{-1}(P) = \{x \in R: \ e(x) \in P\}.$$

By direct computation one proves that $Q \subseteq P$, Q is a prime ideal, and $e(Q) \subseteq Q$. Hence, if P is minimal, then $P = Q$ and $e(P) \subseteq P$. Next if $e(P) \subseteq P$ and not minimal, take $P_1 \subseteq P$ which is a minimal prime. Now $e(P_1) \subseteq P_1$ by the first argument, and $e(P_1) \subseteq e(P)$. But $e(P_1)$ is a maximal ideal in the Boolean algebra of idempotents. Hence $e(P_1) = e(P)$, and so $P_1 = P$, a contradiction.

COROLLARY 2.3. *The function e gives a one-one correspondence between the minimal prime ideals of R and the prime ideals of the Boolean algebra of idempotents of R making principal ideals correspond to principal ideals.*

Next the partial ordering of Z^I must be related to the structure of the homomorphic images by minimal prime ideals. The ring Z^I is a special case of a ring R *partially ordered by idempotents* in the sense that R has enough idempotents and in addition possesses a function p: $R \to R$ such that for all x, y in R the following equations are satisfied:

(i) $p(x) \cdot p(-x) = 0$;

(ii) $p(x) + p(-x) = e(x)$;

(iii) $p(x + y) \cdot p(-x) \cdot p(-y) = 0$;

(iv) $p(x \cdot y) = p(x) \cdot p(y) + p(-x) \cdot p(-y)$.

The partial ordering of R may now be introduced by the definition:

$$x \leqslant y \quad \text{if and only if} \quad p(x - y) = 0,$$

and the desired properties of the relation follow easily from the above equations. If R is an ordered integral domain set $p(x) = 1$, if $x > 0$, and $p(x) = 0$, if $x \leqslant 0$. In the ring Z^I, $p(x)$ for x in Z^I is the characteristic function of the positive coordinates of x. In as much as the ordering of an integral domain need not be unique, the same R may possess many different such functions p, even though the function e is unique. Notice that the class of rings partially ordered by idempotents is closed under direct products.

As a matter of fact, in the ring Z^I the function p is uniquely determined, for Z^I is *quadratically partially ordered* in the sense that each element x in Z^I can be written in the form

$$x = \sum_{i<n} y_i^2 - \sum_{j<n} z_j^2, \quad \textit{where} \quad y_i \cdot z_j = 0 \quad \textit{for} \quad i, j < n.$$

Hence, from the equations (i)-(iv) one can prove

$$p(x) = e\Big(\sum_{i<n} y_i^2\Big).$$

In other words, the non-negative elements of Z^I are just the sums of (four) squares. Notice also that Z^I is *discretely partially ordered* in the sense that for each x in Z^I,

$$\textit{if} \quad x \geqslant 0, \quad \textit{then} \quad x \geqslant e(x).$$

Consider now a homomorphic image of a ring R partially ordered by idempotents. From the characterization of the function p, it is a simple matter to show that if the homomorphism preserves the function e, then it must also preserve the function p. Hence, the image ring can also be partially ordered by idempotents. In particular, if the image is an integral domain and if the function e is preserved, then the image is an ordered integral domain; further, if R is quadratically and discretely partially ordered by idempotents, then this image is a quadratically and discretely ordered domain. The next proposition can now be established at once by making use of 1.7 and 2.2.

PROPOSITION 2.4. *If R is quadratically and discretely partially ordered by idempotents, and if P is an ideal, then R/P is a formally real integral domain if and only if P is a minimal prime ideal.*

As a consequence of 2.4 we see that 2.1 cannot be improved: the only inductive domains that are images of Z^I are those

obtained by minimal primes. Of course, we have not yet seen why every such image is inductive. There is no room here for the full proof of 2.1, for in any case a more general result with all details is to appear elsewhere. But the main outlines of the method can be indicated.

Let P be a minimal prime of Z^I. By 2.2 and 2.3, $e(P)$ is a prime ideal in the algebra of idempotents of Z^I. The algebra of idempotents of Z^I is nothing more than the Boolean algebra of all subsets of I, where sets have been replaced by their characteristic functions. Let $\mathfrak{P}$ be the corresponding prime (maximal) ideal in the algebra of all subsets of I. The fact that $e(P)$ completely determines P may now be expressed in the following equivalence which holds for all x in Z^I:

$$x \in P \quad \textit{if and only if} \quad \{i \in I\colon x_i = 0\} \notin \mathfrak{P}\,.$$

Further all the basic operations and relations in Z^I/P can be translated into this set language as follows:

$$\begin{aligned}
x/P = y/P \quad &\textit{if and only if} \quad \{i \in I\colon x_i = y_i\} \notin \mathfrak{P}\,;\\
x/P \leqslant y/P \quad &\textit{if and only if} \quad \{i \in I\colon x_i \leqslant y_i\} \notin \mathfrak{P}\,;\\
x/P + y/P = z/P \quad &\textit{if and only if} \quad \{i \in I\colon x_i + y_i = z_i\} \notin \mathfrak{P}\colon\\
x/P \cdot y/P = z/P \quad &\textit{if and only if} \quad \{i \in I\colon x_i \cdot y_i = z_i\} \notin \mathfrak{P}\,.
\end{aligned}$$

Having these formulas to begin the induction, one now proves by a straight forward method of elimination of quantifiers that for every first-order formula Φ of elementary ordered ring theory

$$\Phi(x/P, y/P, \ldots) \textit{ holds in } Z^I/P \textit{ if and only if } \{i \in I\colon \Phi(x_i, y_i, \ldots) \textit{ holds in } Z\} \notin \mathfrak{P}\,.$$

This method proves that not only is Z^I/P inductive, but that Z^I/P and Z satisfy exactly the same first-order sentences. Even stronger is the conclusion that Z^I/P is isomorphic to an elementary extension of Z in the sense of Tarski-Vaught [22], where Z is embedded in Z^I/P by use of the constant sequences in Z^I. Actually, all these consequences hold for an arbitrary integral domain D in place of Z, and there is a generalization to any relational system as shown in Frayne-Morel-Scott [4]. However, certain special properties of Z were obviously necessary to apply 2.4. The proof that Z^I/P is uncoutable involves certain technical details about the relation of the cardinality of I to the structure of P and can be found in [4].

One of the most pleasant features of 2.1 is that a method for constructing inductive domains can be stated in ordinary algebraical terms with a minimum of machinery. However, one feels disappointment upon learning that no independence results can be obtained this way for the new inductive domains share the same elementary properties with the ring of integers. Thus in the hope that something may come out of these ideas one may ask whether other kinds of function rings can lead to inductive domains.

Several rings at once come to mind, and all of them turn out to be quadratically and discretely partially ordered by idempotents. These rings are the following:

(1) *the ring PR of all primitive recursive functions*;

(2) *the ring GR of all general recursive functions*;

(3) *the ring $GR(A)$ of all functions general recursive in some definable (arithmetical) predicate A*;

(4) *the ring DF of all algebraically (first-order) definable functions from integers to integers*;

(5) *the ring CN of all definable constants (μ-terms without free variables) in the formal first-order theory of arithmetic (inductive domains)*.

The last mentioned ring does not degenerate simply to the integers in view of the incompleteness of the axioms for inductive domains. For let Φ be any sentence undecidable on the basis of the axioms. Then the following property defines an idempotent in CN:

$$[x = 1 \wedge \Phi] \vee [x = 0 \wedge \neg \Phi] .$$

Indeed all the idempotents of CN can be given definitions of this form.

By virtue of 2.4 we know exactly which homomorphic images of these rings can conceivably yield inductive domains. The results, however, are not comforting. In joint work with S. Feferman [3] it has been shown that if P is a non-principal minimal prime, then none of the rings PR/P, GR/P, $GR(A)/P$ is inductive. In fact, in each separate case there is a corresponding single formula provable by means of the induction axioms which fails in all of the homomorphic images. This is closely related to the fact that one cannot derive all true sentences about integers from any class of true sentences involving a fixed, bounded number of changes of quantifiers,

for even some instances of the induction axioms are not so derivable (cf. Kreisel [8] and Ryll-Nardzewski [16]).

In the case of the ring DF all quotients DF/P, P a minimal prime, are isomorphic to elementary extensions of Z. This is simply an algebraic reformulation of the original result of Skolem (cf. [19]) and, in a slightly different form, was first called to the author's attention by S. Kochen (cf. [6]). To understand the connection with Skolem's method, recall that we have shown in 2.3 that the minimal prime ideals correspond to the prime ideals in the Boolean algebra of idempotents. Now the idempotents of DF are simply the characteristic functions of (first-order) definable sets of integers, which form a denumerable Boolean algebra. The non-principal ideals of a denumerable algebra can always be given an *ordered basis*. For example if $\mathfrak{P}$ is a non-principal prime ideal in the algebra of definable sets, then there exists a sequence of sets $X_n \in \mathfrak{P}$ such that $X_n \neq X_{n+1}$ and $X_n \subseteq X_{n+1}$ for all $n = 0, 1, 2, \ldots$ Further the sets X_n form a *basis* in the sense that $Y \in \mathfrak{P}$ if and only if $Y \subseteq X_n$ for some n, where Y is in the algebra. Now since we have an algebra of sets, let a set S be chosen so that $S = \{s_0, s_1, s_2, \ldots, s_n, \ldots\}$ and $s_n \in X_{n+1} - X_n$. It is easy to conclude that S is not (first-order) definable. However, S does determine $\mathfrak{P}$, for one may show directly that for all Y in the algebra, $Y \in \mathfrak{P}$ if and only if $Y \cap S$ is finite. In particular, if $f, g \in DF$, then

$f/P = g/P$ if and only if there is an N such that

$$f(s_n) = g(s_n) \text{ for all } n \geqslant N .$$

And similar equivalences hold for the relations $f/P \leqslant g/P$, etc. Thus the sequence s_n is exactly the *comparing function* used by Skolem to divide the definable functions into congruence classes.

In the case of the ring of functions GR the Boolean algebra is the algebra of recursive sets and many non-principal prime ideals correspond to sets similar to the S above but which may be taken as the complements of the recursively enumerable *maximal simple sets* constructed by Friedberg in [5]. It was this remark showing the interesting way in which Skolem's method for constructing non-archimedean domains could be applied to the recursive functions that was made to the author by D. Tennenbaum and stimulated much of our present research in these directions.

It would seem fair to say that the method of Theorem 2.1 for obtaining non-archimedean inductive domains is the correct generalization of Skolem's method to non-denumerable function rings.

Finally, we may examine the ring CN, which was included only for illustration. The minimal prime ideals of this ring correspond exactly to the complete extensions of the axioms for inductive domains (because of the nature of the Boolean algebra of idempotents). The quotiens CN/P are exactly the *prime models* for arithmetic considered by A. Robinson in [14].

§ 3. Polynomial rings. In an attempt to construct models for any theory one very attractive procedure is to carry out the construction by successive adjunctions of new elements, as in the construction of the algebraic closure of a field or indeed as in some proofs of the Completeness Theorem for first-order logic. In the case of arithmetic we shall see that this method cannot be applied without discrimination. The first question that comes to mind is whether an arbitrary discretely ordered domain can be extended to an inductive domain. To this end note first of all two simple facts.

PROPOSITION 3.1. (i) *In a discretely ordered domain no element can be both even and odd*;

(ii) *in an inductive domain every element is either even or odd.*

Proof. (ii) is obvious; for (i) notice that if $2x = 2y+1$, then $2(x-y) = 1$. Hence, $x-y > 0$, and therefore $x-y \geqslant 1$, which is impossible.

THEOREM 3.2. *There is a discretely ordered domain in which the equation*

$$t^2+t+1 = 2u$$

has a solution.

This statement at once answers our question above for we have the

COLLORARY 3.3. *The discretely ordered domain of Theorem* 3.2 *cannot be extended to an inductive domain.*

Proof. One need only recall that from knowing every element is either even or odd, it follows that the polynomial x^2+x+1 takes on only odd values. The conslusion follows from 3.1.

It remains now to establish the existence of required domain.

LEMMA 3.4. *If R is an ordered domain, then there is a unique ordering of the polynomial domain $R[t]$ of polynomials in one indeterminate t such that $t > r$ for all constant polynomials $r \in R$. If in addition R is discretely ordered, then under this ordering so is $R[t]$.*

Notice that if $p(t) \in R[t]$ and $r \leqslant p(t) \leqslant s$ for $r, s \in R$, then $p(t)$ is constant, i.e., $p(t) \in R$ also. The ordering of $R[t]$ is of course always non-archimedean under the stipulation in 3.4.

Proof of 3.2. Let Q be the (ordered) field of rationals and consider the polynomial domain $Q[t]$, ordered as in 3.4. Let

$$u = \tfrac{1}{2}(t^2 + t + 1),$$

and let D be the ordered subdomain of $Q[t]$ generated by t and u. If we can show that D is discretely ordered, the proof will be complete.

First of all it is easy to verify that D consists exactly of those polynomials of the form

$$2p(t) + \sum_{k=0}^{n} \frac{a_k(t)}{2^k}(t^2 + t + 1)^k,$$

where $p(t) \in Z[t]$ is an integral polynomial and the $a_k(t)$ have as coefficients only 0 or 1. If in D there were an element between 0 and 1, we would find in $Z[t]$ an inequality of the form

$$0 < 2^{n+1}p(t) - \sum_{k=0}^{n} 2^{n-k}a_k(t)(t^2 + t + 1)^k < 2^n.$$

But this would mean that the polynomial mentioned is a *constant* in $Z[t]$. Reducing modulo 2 we find that the polynomial $a_n(t)(t^2 + t + 1)^n$ is constant in $Z_2[t]$, where Z_2 is the two element ring. However, the polynomial $t^2 + t - 1$ is neither a divisor of zero nor a unit in $Z_2[t]$. Assuming that if $n \neq 0$, then in the original polynomial $a_n(t) \neq 0$, we conclude that $n = 0$. In other words we have in $Z[t]$,

$$0 < 2p(t) - a_0(t) < 1,$$

which is impossible in the discretely ordered domain $Z[t]$.

In general, even though polynomial rings are seen to yield many discretely ordered domains, they do not seem to lead

very directly to inductive domains. In a (negative) direction somewhat different from 3.2 we have the next result.

THEOREM 3.5. *If R is a formally real domain and $D \subseteq R[t]$ is quadratically ordered, then $D \subseteq R$.*

Before giving the proof, notice that 1.7 shows at once that if D were discretely ordered, D must be isomorphic to a subdomain of R, for there is a homomorphism $h\colon D \to R$ such that $h(p(t)) = p(0)$. However, the stronger conclusion can be derived by making use of some simple ideas from the theory of valuations.

Let D by any ordered domain and consider a function $w\colon D \to Z \cup \{-\infty\}$. This function w is called an *integral order preserving valuation* over D if the following four conditions are satisfied for all elements $x, y \in D$:

(i) $w(0) = -\infty$,

(ii) $w(x \cdot y) = w(x) + w(y)$,

(iii) $w(x+y) \leqslant \max(w(x), w(y))$,

(iv) *if* $0 \leqslant x \leqslant y$, *then* $w(x) \leqslant w(y)$.

These conditions on a valuation are slightly different from the ordinary ones (in, say, van der Waerden [25], p. 252-254) because the non-archimedean elements emphasized here are infinitely large rather than infinitely small. Notice that condition (iv) may be replaced by

(iv′) *if* $x, y \geqslant 0$, *then* $w(x+y) = \max(w(x), w(y))$.

Notice also that (i)-(iv) imply that if $x \neq 0$, then $w(x) \geqslant 0$. Such a valuation is *trivial* if it takes on only the values $-\infty$ and 0. The essential step in proving 3.5 may be formulated as follows:

LEMMA 3.6. *No quadratically ordered domain can have a non-trivial integral order-preserving valuation.*

Proof. Suppose that D is the domain and w the valuation. Choose an element x so that $w(x)$ is a minimum among the non-zero (positive) values of w. Since $w(x) = w(-x)$, we may assume $x > 0$. Now $x = \sum_{i<n} y_i^2$, and by (iv′) above $w(x) = \max_{i<n} w(y_i^2)$. Clearly we can assume that $y_0^2 \geqslant y_i^2$ for $i < n$. Hence $w(y_0^2) \geqslant w(y_i^2)$ for $i < n$, and $w(x) = w(y_0^2) = 2w(y_0)$. Now $y_0 \neq 0$, and so $w(y_0) < w(x)$. Whence, $w(y_0) = 0 = 2w(y_0) = w(x)$, which is a contradiction.

Proof of 3.5. In the polynomial domain $R[t]$ define a function w such that $w(p(t)) = -\infty$ if $p(t) = 0$, otherwise $w(p(t)) =$ the degree of $p(t)$. Notice that $p(t) \in R$ if and only if $w(p(t)) = -\infty$ or 0. Thus, if we can show that w restricted to the quadratically ordered subdomain D is an order preserving valuation, then an application of 3.6 will complete the proof. Now the conditions (i), (ii), (iii) are satisfied throughout $R[t]$. Thus it remains only to verify condition (iv), or better (iv'), on D. Let $x, y \in D$, $x, y \geqslant 0$. Then $x = \sum_{i<n} p_i(t)^2$ and $y = \sum_{i<m} q_i(t)^2$. Thus the coefficients of the highest powers of t in both x and y are sums of squares, and hence in $x+y$ the larger of these two powers must still appear, because no non-trivial sum of squares is zero in R. In other words $w(x-y) = \max(w(x), w(y))$, as was to be shown.

Comparing 3.5 and 3.6 with 1.10 we see that inductive domains cannot be finitely generated or even be included in finitely generated rings in a non-trivial way. Indeed it might be possible to give a common generalization of these results, but the author has been unable to isolate the essential fact that seems to be contained in all of these proofs. In any case, one has many danger signals to watch for in any attempt at constructing an inductive domain.

In 3.2 the discretely ordered domain constructed fails to satisfy the condition that every element is either even or odd. One might ask whether a discretely ordered domain in which finite congruences are solvable can be extended to an inductive domain. To be more specific, we shall say that *finite congruences are solvable* in D if for each m, $D/(m)$ is isomorphic to $Z/(m)$; i.e., each element in D congruent to $0, 1, \ldots,$ or $m-1$ modulo m. Note first that the square root of 2 is irrational in the following sense.

PROPOSITION 3.7. *In an inductive domain there are no non-zero solutions of the equation*

$$t^2 = 2u^2 .$$

Again a polynomial ring leads to a counterexample.

THEOREM 3.8. *There is a discretely ordered domain in which all finite congruences are solvable and in which the equation*

$$t^2 = 2u^2$$

has a non-zero solution.

Proof. Let Re be the field of real numbers and let D be the subdomain of $Re[t]$ consisting of those polynomials $p(t)$ such that $p(0) \in Z$ (i.e., integral constant term). $Re[t]$ is ordered as in 3.4, and it is easy to show that D is discretely ordered and that finite congruences are solvable in D. However, $u = \sqrt{2}t$ is in D, which completes the proof.

A way of recasting the results in 3.2 and 3.8 is to say that both of the (universal) sentences

$$t^2 + t + 1 \neq 2u; \tag{1}$$

$$t^2 = 2u^2 \quad \textit{implies} \quad t = 0\,, \tag{2}$$

are independent of the axioms for discretely ordered domains. In fact, the independence result in the case of (2) is slightly stronger. Both (1) and (2) are provable by the induction axiom for inductive domains, but every such application of induction axiom seems to require a formula with at least one quantifier in the inductive hypothesis. Hence we may ask whether these sentences can be proved from the axioms of discretely ordered domains by means of a rule of induction applied only to free variable formulas.

In other words, if we take statement (2) above as an example, the fact that the square root of 2 is irrational can be expressed by a universal sentence involving only the functions of addition and multiplication. Now the simple algebraic properties of these operations are embodied in the axioms for discretely ordered domains, and the rule of free variable inductions allows us to deduce further consequences from these axioms which correspond to directly understandable algebraic properties of the integers. However, in every proof of (2) in ordinary number theory some new functions must be introduced by recursive definitions to carry out the argument (e.g. the $gcd(x, y)$ or 2^x, etc.). Can this necessity for using notions in the proof that do not appear in the statement of the problem be made precise? One method is to ask whether (2) can be proved by free variable induction. Presumably the answer is *no*, but the demonstration is lacking.

This question about proving (2) was first raised by Skolem in [19], and similar questions have been emphasized by Kreisel in [27]. The only positive results known to the author are contained in the interesting paper of Shoenfield [17] where the problem is treated in the theory of addition alone.

Unfortunately, none of Shoenfield's models for addition can be ordered, and so his method does not seem to generalize. Is it possible that the domain constructed in the proof of 3.2 satisfies the rule of free variable induction? The author was not able to decide this question.

The question discussed above is closely related to Hilbert's Problem about which diophantine equations have solutions in the integers. Hilbert's Problem can be rephrased as asking which universal sentences in terms of addition, multiplication and order are true in the domain of integers. It seems unlikely that there is a decision method for such sentences (cf. Robinson [15] and Davis-Putnam [1]), but even if Hilbert's Problem is not recursively solvable, one still would like to know what is the relation between the universal sentences true in the integers and those provable by the induction axiom. (If every true universal sentence is provable, then Hilbert's Problem is recursively solvable.)

In particular, can the provable universal sentences about all inductive domains be characterized in a natural way making use of simple algebraically meaningful rules involving only universal sentences? The rule of free variable induction probably is inadequate, but it would seem to be of real interest to understand the complete situation.

The questions about universal sentences are also closely related to the extension problem. A general theorem in [4] shows that if D and D' are two domains, then every universal sentence true in D is true in D' if and only if D' is isomorphic to a subdomain of some D^I/P where P is a minimal prime ideal of D^I. Looking back to 2.1 and its generalizations mentioned in the discussion, we conclude that a domain D can be extended to an inductive domain if and only if every universal sentence true in all inductive domains is true in D. (For a simpler discussion of this type of conclusion cf. Tarski [21]).

§ 4. Recursive and definable rings. If a denumerable ring R is put into a one-one correspondence with the integers Z by a function ε: $Z \to R$, then the addition and multiplication of R induce two functions α, μ: $Z \times Z \to Z$ by the relations

$$\varepsilon(n) - \varepsilon(m) = \varepsilon\big(\alpha(n, m)\big), \qquad \varepsilon(n) \cdot \varepsilon(m) = \varepsilon\big(\mu(n, m)\big).$$

The functions α and μ are called the *addition and multiplication tables* of R relative to the enumeration ε. We may ask whether algebraic properties of R influence the nature of the possible

addition and multiplication tables which the ring may possess. In particular, can the a and μ ever be recursive for a suitable ε? or can they be functions on Z algebraically (first-order) definable in the doman Z? In these two cases we shall say for short that the ring R is *recursive* or *definable*. An analysis of the original proof in Gödel [10] or Hilbert-Bernays [9] of the Completeness Theorem allows us to conclude the following

PROPOSITION 4.1. *There exist definable non-archimedean inductive domains.*

It should be stressed that the proof of 4.1 does not require the method of *arithmetization of syntax* which plays such a central role in the proof of incompleteness in Gödel [11]. For we need only note that there are finitely axiomatizable theories involving other predicate constants beyond those for addition and multiplication from which the inductive axiom schema for arithmetic can be deduced. A system close to the set-theory of Bernays-Gödel can be used for example. Call the axiom for this (consistent) theory A. To this sentence we shall adjoin a new sentence involving a new monadic predicate symbol $\boldsymbol{P}$ as follows:

$$\left[\boldsymbol{P}(0)\wedge(x)[\boldsymbol{P}(x)\rightarrow\boldsymbol{P}(x+1)\wedge\boldsymbol{P}(x-1)]\wedge\neg(x)\boldsymbol{P}(x)\right].$$

There are several ways to show that if A is consistent, then the resulting conjunction is also consistent. It is at once clear that in every model for this extended theory the domain involved is a non-archimedean inductive domain. Now it is exactly the point of Gödel's proof of completeness that one may write out directly a definition in aritmetic of predicates satisfying this single sentence.

In other words, an explicitly definable non-archimedean inductive domain can be given. Of course, the actual definitions required would be far from short. In particular the model in arithmetic is constructed as the union of finite "partial" models, and the structure of these finite systems must be described in algebraic terms. This description can be carried out by the use of the Chinese remainder theorem for representing finite sets, sequences, and functions in arithmetic. Of course, it is just the use of this kind of representation of sequences that permits the arithmetization of syntax; however, the description of the finite relational systems is far simpler than the explicit definitions of the necessary syntactical notions. The author definitely feels that a complete proof of 4.1 would require much less in

the way of preparation and comprehension than the usual proofs of incompleteness of arithmetic. We note next that Tennenbaum has proved in [24] the following result first proved by Feferman [2].

THEOREM 4.2. *Every definable non-archimedean inductive domain satisfies a sentence false in the integers.*

The proof shows that the sentence in question is one of the instances of the formula that defines the addition table $a(n, m)$ of the definable domain. A slightly different method of proof not requiring the more advanced ideas from recursive function theory is given in [18]. There the sentence in question is constructed by a simple diagonal argument. The method of proof applies when there are additional predicates besides addition and multiplication giving a common generalization of 4.2 and the result of Rabin [13] (Theorem 6). We thus obtain as a consequence of 4.1 and 4.2 the Incompleteness Theorem. Indeed, this method is adequate to show that any theory which has a set of axioms definable in arithmetic is inadequate for proving all true sentences of arithmetic—a result which is of course already known. The method of proof of incompleteness outlined here should be compared with that of Kreisel in [7] and Wang in [26].

Another result of Tennenbaum [24] closely related to 4.2 is as follows:

THEOREM 4.3. *No non-archimedean inductive domain is recursive.*

Thus, if we try to construct a non-archimedean domain to prove incompleteness by showing by means of the model that a certain true sentence is independent of the inductive axioms, then this domain cannot have effectively computable addition and multiplication tables. For example, the domain constructed in 3.2 is recursive and hence not inductive. (Actually it fails to be inductive for a very simple reason as shown in the proof of 3.2.) Hence, we have a new warning sign in our search for models of arithmetic: *Do not use addition and multiplication tables that are too simple.* Nevertheless the investigation of certain recursive discretely ordered domains may be of real interest, for these may be models for useful fragments of arithmetic, as in the problem of Skolem mentioned in Section 3.

Another way to phrase the content of 4.3 uses the sequences of finite residues by finite moduli of elements of an inductive

domain. In the notation of Specker [20], the sequence is $(a_1, a_2, a_3, a_4, \ldots)$ where a is some element of the domain and a_n is the residue modulo n. We can interpret a_n as an actual integer, where $0 \leqslant a_n < n$, rather than as a (finite) element of the domain. With this terminology the result of Tennenbaum shows that *in any non-archimedean inductive domain there must exist an element a such that the sequence of residues $(a_1, a_2, a_3, \ldots)$ is not recursive.* This rephrasing higlights in a different way the complexity of inductive domains that are not the integers.

The author sincerely hopes that the discussion presented here, which is rather weighted to the side of negative results, is not discouraging. Even though the problem of constructing inductive domains is clearly extremely difficult to solve in useful ways, a deeper study of this question can surely bring us better understanding of the nature of arithmetic.

References

[1] M. Davis and H. Putnam, *Reduction of Hilbert's tenth problem*, Journ. Symb. Logic 23 (1958), pp. 183-187.

[2] S. Feferman, *Arithmetically definable models of formalized arithmetic*, Notices Amer. Math. Soc. 5 (1958), pp. 679-680 (Abstract 550-21).

[3] — D. Scott and S. Tennenbaum, *Models of arithmetic through function rings*, Notices Amer. Math. Soc. 6 (1959), pp. 173-174 (Abstract 556-31).

[4] T. Frayne, A. C. Morel and D. Scott, *Reduced direct products*, to appear.

[5] R. M. Friedberg, *Three theorems on recursive enumeration*, Journ. Symb. Logic 23 (1958), pp. 309-316.

[6] S. Kochen, *Filtration systems, I*, Notices Amer. Math. Soc. 5 (1958), p. 605 (Abstract 549-24).

[7] G. Kreisel, *Note on arithmetic models for consistent formulae of the predicate calculus. Part I*, Fund. Math. 37 (1950), pp. 265-285.

[8] — *Some concepts concerning formal systems of number theory*, Math. Zeit. 57 (1952), pp. 1-12.

[9] D. Hilbert and P. Bernays, *Grundlagen der Mathematik*, vol. 2, Berlin 1939.

[10] K. Gödel, *Die Vollstandigkeit der Axiome des logischen Funktionenkalküls*, Monatshefte für Mathematik und Physik 37 (1930), pp. 349-360.

[11] — *Über formal unentscheidbare Sätze der Principia Mathematica und verwandter Systeme, I*, Monatshefte für Mathematik und Physik 38 (1931), pp. 173-198.

[12] E. Mendelson, *A proposed non-standard model*, Notices Amer. Math. Soc. 6 (1959), pp. 143-144 (Abstract 554-31).

[13] M. O. Rabin, *Arithmetical extensions with prescribed cardinality*, Indag. Math. 21 (1959), pp. 439-446.

[14] A. Robinson, *Model theory and non-standard arithmetic,* this volume, pp. 265-303.

[15] R. M. Robinson, *Arithmetical representations of recursively enumerable sets*, Journ. Symb. Logic 21 (1956), pp. 162-186.

[16] C. Ryll-Nardzewski, *The role of the axiom of induction in elementary arithmetic,* Fund. Math. 39 (1953), pp. 239-263.

[17] J. R. Shoenfield, *Open sentences and the induction axiom*, Journ. Symb. Logic 23 (1958), pp. 7-12.

[18] D. Scott, *On a theorem of Rabin*, to appear.

[19] T. Skolem, *Peano's axioms and models od arithmetic*, Mathematical interpretations of formal systems, Amsterdam 1955, pp. 1-14.

[20] E. Specker und R. Mac Dowell, *Modelle der Arithmetik,* this volume, pp. 257-263.

[21] A. Tarski, *Contributions to the theory of models, I-II*, Indag. Math. 16 (1954), pp. 572-588.

[22] A. Tarski and R. L. Vaught, *Arithmetical extensions of relational systems*, Compositio Math. 13 (1957), pp. 81-102.

[23] A. Tarski, *What is elementary geometry? The axiomatic method, with special reference to geometry and physics*, Amsterdam 1957, pp. 16-29.

[24] S. Tennenbaum, *Non-archimedean systems of arithmetic*, to appear.

[25] B. L. van der Waerden, *Moderne Algebra*, 3rd edition, Berlin 1950.

[26] H. Wang, *Undecidable sentences generated by semantic paradoxes*, Journ. Symb. Logic 20 (1955), pp. 31-43.

[27] G. Kreisel, *Applications of mathematical logic to various branches of mathematics,* Colloque de la Logique Mathématique, Paris 1954, pp. 37-49.

THE UNIVERSITY OF CHICAGO