UNDECIDABLE RINGS

BY

RAPHAEL M. ROBINSON

TABLE OF CONTENTS

1a. **Introduction and summary of known results.** There is no general method of deciding whether a statement concerning the natural numbers, involving the operations of addition and multiplication and the concepts of elementary logic, is true or false. (See Gödel [2], Church [1], Rosser [8], Tarski and Mostowski [11], [5].) We express this fact by saying that the solution to the decision problem is negative for the arithmetic of natural numbers, or that the arithmetic of natural numbers is *undecidable*.

This conclusion is very plausible even without proof, because of the existence of many unsolved problems of just the character considered. For example, the conjecture that there are infinitely many prime-pairs may be written

$$(\wedge x)(\vee y)(\wedge u, v)[x + y = uv \vee x + y + 2 = uv \rightarrow u = 1 \vee v = 1].$$

It is therefore one of the statements considered in the first paragraph.

Here and throughout, we use the logical symbols $\wedge$ (and), $\vee$ (or), $\sim$ (not), $\rightarrow$ (if $\cdots$ then $\cdots$), $\leftrightarrow$ (if and only if), $\wedge$ (for every), and $\vee$ (there exists). These, together with $=$, represent the concepts of elementary logic. The formulas under consideration involve only these symbols, the symbols $+$ and $\cdot$, variables whose range is the set of natural numbers, and parentheses. In the above formula, $(\wedge u, v)$ is short for $(\wedge u)(\wedge v)$. We shall also use the convention that a formula containing free variables is to be interpreted as if these were bound by universal quantifiers at the beginning of the formula.

Presented to the Society, August 30, 1949; received by the editors February 11, 1950.

The prime-pair conjecture, as written, contains the symbols 1 and 2, in addition to those listed as permissible. These, and indeed the symbols for any specific natural numbers, can be eliminated by means of definitions such as

$$x = 0 \leftrightarrow x + x = x, \qquad x = 1 \leftrightarrow x^2 = x \wedge x \neq 0, \qquad 2 = 1 + 1.$$

Statements of the type which we have been considering will be called statements of the arithmetic of natural numbers, or *arithmetical statements* of the theory of natural numbers. We shall also consider arithmetical statements of other theories. These are statements involving specified mathematical concepts (operations, relations, and so on), the concepts of elementary logic, and variables with specified range. The mathematical concepts will always be the operations of addition and multiplication unless the contrary is stated.

Let us now consider the arithmetic of integers. In the ring of integers, we can define the concept natural number by

$$\text{Nat } x \leftrightarrow (\vee u, v, y, z)[x = u^2 + v^2 + y^2 + z^2],$$

or by

$$\text{Nat } x \leftrightarrow (\vee y, z)[x = y^2 \vee (y^2 = 1 + xz^2 \wedge y \neq 0 \wedge z \neq 0)].$$

In both cases, the range of the variables is the set of all integers. To verify these equivalences, we use in the first case the theorem of Lagrange, and in the second case known results concerning the so-called Pell equation.

Any statement in the arithmetic of natural numbers can be written as a statement about integers, each variable x being restricted by the condition Nat x; that is, we replace $(\wedge x)[\cdots]$ by $(\wedge x)[\text{Nat } x \rightarrow \cdots]$, and $(\vee x)[\cdots]$ by $(\vee x)[\text{Nat } x \wedge \cdots]$. Using either of the above definitions, we can eliminate Nat, obtaining a statement of the arithmetic of integers. Thus the solution to the decision problem is clearly negative for the arithmetic of integers, or, as we shall say, the ring of integers is undecidable.

Both of the definitions of Nat given above are examples of what we shall call *arithmetical definitions*. By this we mean that the definition has the form of an equivalence, with the concept to be defined on the left, whereas on the right occur only the concepts of elementary logic, the given mathematical concepts (here the operations of addition and multiplication), and variables with specified range (here the set of integers), all of the variables being bound except those which occur on the left. Only such a definition can serve to eliminate the defined concept and give an arithmetical statement as result. For example, the set-theoretical definition

$$\text{Nat } x \leftrightarrow (\wedge M)\{0 \in M \wedge (\wedge y)[y \in M \rightarrow y + 1 \in M] \rightarrow x \in M\},$$

where M ranges over sets of integers, would not serve this purpose.

Nat is also arithmetically definable in the field of rational numbers (Julia Robinson [7], Theorem 3.1), and hence this field is undecidable. On the other hand, any algebraically closed field or real closed field is decidable (Tarski [10]). In particular, there is an effective method of deciding whether a statement about real numbers involving addition, multiplication, and the concepts of elementary logic is true or false. Finite fields are of course also decidable. For all other fields, the decision problem is open. Notice that in a decidable field of characteristic zero, Nat is not arithmetically definable; for example, Nat is not definable in terms of addition and multiplication of real numbers.

Very few other results concerning the decision problem for particular rings are known. Mostowski and Tarski [5] have shown that any ordered ring with a unity element 1, and with no element between 0 and 1, is undecidable. Here we have an additional primitive concept $<$, so that the result does not concern the undecidability of rings as such. However, it follows that any ring in which such an ordering is arithmetically definable (in terms of addition and multiplication) is undecidable. There does not seem to be any simple example of such a ring, except for the ring of integers, though the existence of other such rings can be proved.

Tarski and Mostowski [11], [5] have also shown that the general theory of rings is undecidable, and Tarski has shown that the theory of Boolean rings is decidable. Some results concerning the decision problem in group theory are given by Presburger [6], Szmielew [9], and Tarski [12].

1b. **Plan of this paper and summary of new results.** We shall prove that various rings are undecidable. This will usually be done by showing that it is possible to formulate all statements of the arithmetic of natural numbers in the ring. For this purpose, we construct in the ring a model for the arithmetic of natural numbers. We shall be interested not only in the existence of such a model, but also in what kind of model it is possible to find.

For simplicity, we shall consider in this paper the decision problem only for ID_1's. Here ID_1 is an abbreviation of integral domain with unity element (that is, ring in which $xy=yx$, $xy=0 \rightarrow x=0 \vee y=0$, $x \cdot 1=x$, and $1 \neq 0$). In any ID_1, the elements 0 and 1 are arithmetically definable in terms of addition and multiplication, so that it is immaterial whether we take them as primitive concepts.

Divisibility is defined in any commutative ring, as well as in the arithmetic of natural numbers, by

$$x \mid y \leftrightarrow (\bigvee z)[y = xz].$$

However, the meaning of $x \mid y$ depends on what ring is being considered. In a field, the concept of divisibility is trivial, and indeed $x \mid y \leftrightarrow x \neq 0 \vee y=0$. Now in all our investigations, the concept of divisibility plays a central role. Thus to prove that a field is undecidable, some quite different method is needed

(perhaps based on the theory of quadratic forms, as was the proof in [7] that the field of rationals is undecidable).

In any ID_1 of characteristic zero, we identify the ring elements 0, 1, $2=1+1, \cdots$ with the natural numbers, and use Nat x to indicate that x is one of these elements. Similarly, we use Int x to indicate that x is one of the integers $0, \pm 1, \pm 2, \cdots$; thus Int $x \leftrightarrow$ Nat $x \vee$ Nat $(-x)$. These concepts are used only if the characteristic of the ring is zero. (The term integer is always used in the sense mentioned, and is not to be confused with algebraic integer, which we also use in certain places.)

If we can define Nat arithmetically in a given ID_1 of characteristic zero, then all statements of the arithmetic of natural numbers can also be formulated arithmetically in the ring; hence, in particular, the ring is undecidable. We draw the same conclusions if Int can be defined arithmetically, since Nat may then also be defined arithmetically.

More generally, all statements of the arithmetic of natural numbers can be formulated arithmetically in a given ring, if we can define arithmetically a model for the arithmetic of natural numbers; that is, if we can define arithmetically a set of ring elements, and two binary operations on them, so that the model obtained is isomorphic to the arithmetic of natural numbers. If Nat is defined arithmetically (in an ID_1 of characteristic zero), then we have of course such a model, where ring addition and multiplication also serve as addition and multiplication in the model.

Another model which proves useful has the natural numbers replaced by the corresponding powers $p^0, p^1, p^2, \cdots$ of some fixed element p. We must of course choose p so that these are all different. Here the ring multiplication serves as addition in the model. We must also arithmetically define multiplication in the model, as well as the set of powers of p itself. In this connection, we shall use the symbols Pow and Asp. By x Pow p, we shall mean that x is a power of p, and by x Asp p, that x is associated with a power of p, that is,

$$x \text{ Asp } p \leftrightarrow (\bigvee y, z)[x = yz \wedge y \mid 1 \wedge z \text{ Pow } p].$$

In practice, Asp will be defined arithmetically first, and used in the arithmetical definition of Pow.

Many of our results concern polynomial ID_1's (that is, polynomial rings over ID_1's). Elements of the base ring will be called constants, and Con x will mean that x is a constant. It should be pointed out however that the meaning of this symbol is not in general determined by merely knowing the polynomial ring, but only by knowing what ring is considered as base ring.

We shall use a variety of methods in our study of undecidable rings. The results of §2, §§3a–3b, §§4a–4d, §§5a–5c, §6, and §7 are substantially independent of each other, and hence these parts of the paper may be read in any order.

In §2, we define Nat in a polynomial ring over any field of characteristic zero, in a polynomial ring over the ring of p-adic integers, and in the ring of entire functions of a complex variable. In §§3a–3b, we define Int (and hence also Nat) in a quadratic ring (the ring of algebraic integers in a quadratic field), and in the ring of polynomials over the integers or over a quadratic ring. These are the only cases in which we have been able to define Nat.

In §§4a–4c, we prove that it is possible to formulate all statements of the arithmetic of natural numbers in various polynomial rings, including those for which the base ring is any field, or is the ring of algebraic integers in a field of finite degree over the rationals. We have not been able to obtain this conclusion for polynomial ID_1's in general, but in §4d, using the method of §§4a–4c combined with a result of Tarski and Mostowski [11], [5], we do show that all polynomial ID_1's are undecidable. This is the only place in the paper where we prove that a ring is undecidable without also showing that it is possible to formulate all statements of the arithmetic of natural numbers in it.

In §§5a–5c, we prove that all statements of the arithmetic of natural numbers can be formulated in algebraic rings with one fundamental unit. In §6, the same is done for the rings of formal power series with integer or rational coefficients. In §7, a result of a different character is proved, namely that in a polynomial ring in two or more variables over a finite field, there is no uniquely definable model for the arithmetic of natural numbers.

2. **Definition of natural numbers in certain function rings.** We shall show that Nat is arithmetically definable in any polynomial ID_1 of characteristic zero in which Con is arithmetically definable. This result applies in particular to any polynomial ring over a field of characteristic zero, since in this case we clearly have

$$\text{Con } x \leftrightarrow x = 0 \vee x \mid 1.$$

It also applies in certain other cases. For example, in a polynomial ring over the ring of p-adic integers, we have

$$\text{Con } x \leftrightarrow x \mid 1 \vee x + 1 \mid 1.$$

On the other hand, in the case of a polynomial ring over the integers, the present result is of no help, and is indeed trivial, since Con is the same as Int. This case is however treated below by another method (see §§3a–3b).

Suppose we are given the ring of polynomials in one or more variables $\alpha, \beta, \gamma, \cdots$, over any ID_1 of characteristic zero. We shall show that Nat can be defined in terms of Con by

$$\text{Nat } x \leftrightarrow (\vee u, v)\{\sim\text{Con } u \wedge v \neq 0 \wedge u \mid v \wedge (\wedge y)[\text{Con } y \wedge u + y \mid v \rightarrow u + y + 1 \mid v \vee y = x]\}.$$

First suppose that x is a natural number. Then the condition on the right

is satisfied with

$$u = \alpha, \qquad v = \alpha(\alpha + 1)(\alpha + 2) \cdots (\alpha + x).$$

To check this, notice that by the factor theorem, the only factors of v of the form $\alpha+y$, with y a constant, are α, $\alpha+1$, $\alpha+2$, $\cdots$, $\alpha+x$.

Conversely, suppose that x satisfies the right side of the equivalence. Choose suitable u and v. Enlarge our polynomial ring by embedding the ring of constants in a field. In this new polynomial ring, we have unique factorization. Since u, $u+1$, $u+2$, $\cdots$ are relatively prime and not constant, and $v \neq 0$, only a finite number of them can divide v. Returning to the original ring, no more of them can divide v. Now $u \mid v$, thus there must be a natural number n such that

$$u + n \mid v, \qquad u + n + 1 \nmid v.$$

It then follows that $x=n$, that is, that x is a natural number.

A quite similar method of defining natural numbers may be used in the ring of entire functions of a complex variable α. Here the formula $x \mid 1$ expresses that the entire function x has no zeros. Now according to Picard's theorem, an entire function which is not constant must assume every value with at most one exception. Thus

$$\sim \text{Con } x \rightarrow x \nmid 1 \vee x - 1 \nmid 1.$$

It follows that we can define Con by

$$\text{Con } x \leftrightarrow x = 0 \vee x = 1 \vee (x \mid 1 \wedge x - 1 \mid 1).$$

Finally, we shall show that Nat may be defined by

$$\text{Nat } x \leftrightarrow \text{Con } x$$
$$\wedge (\wedge u, v)\{u \mid v \wedge (\wedge y)[\text{Con } y \wedge u + y \mid v \rightarrow u + y + 1 \mid v] \rightarrow u + x \mid v\}.$$

The right side is clearly satisfied if x is a natural number. Conversely, suppose that the right side is satisfied. In particular, we may take $u=\alpha$, and for v any entire function whose only zeros are at $0, -1, -2, -3, \cdots$, for example, $v=1/\Gamma(\alpha)$. With this choice of v, we see that for constant y, $\alpha+y \mid v$ if and only if y is a natural number. We conclude that $\alpha+x \mid v$, and hence that x is a natural number.

If instead of entire functions, we consider the ring of analytic functions regular in the unit circle, I do not know how to arithmetically define Nat or even Con.

3a. **Definition of integers in quadratic rings.** In this section and the next, we shall define integers in quadratic rings. The method given also applies, without any essential modification, to the problem of defining integers in a polynomial ring over the integers or over a quadratic ring.

A quadratic field is obtained by adjoining $m^{1/2}$ to the field of rationals,

where m is an integer which is not a square. We shall suppose that m is square-free. By a quadratic ring, we understand the ring of algebraic integers in a quadratic field. The algebraic integers of the field have the form $a+bm^{1/2}$, where a and b are integers, if $m \not\equiv 1 \pmod 4$, and the form $(a+bm^{1/2})/2$, with $a \equiv b \pmod 2$, if $m \equiv 1 \pmod 4$.

We shall show first that, in a quadratic ring, Int can be defined in terms of Pow by any formula of the form

$$\text{Int } x \leftrightarrow (\wedge u)(\vee v, y)[u \text{ Pow } p \rightarrow v \text{ Pow } q \wedge px + 1 = v + uy],$$

where p and q are replaced by two prime numbers for which $p>2$ and q is a primitive root mod p^2. (This result holds indeed in the ring of algebraic integers in any field of finite degree over the rationals.)

It is known that under the stated conditions, q will also be a primitive root mod p^k for every k. Consequently, if x is any integer, we can find l so that

$$q^l \equiv px + 1 \pmod{p^k},$$

or $px+1=q^l+p^ky$ with some integer y. Thus if Int x, we can satisfy the right side of the equivalence, and indeed with y an integer.

Conversely, if the right side is satisfied, then $px+1$ has the form q^l+p^ky for every k, where y is an element of the ring. If x' denotes the conjugate of x in the quadratic ring, then also $px'+1=q^l+p^ky'$, and hence $p(x-x')=p^k(y-y')$. Thus $p^{k-1} \mid x-x'$ for every k, so we must have $x-x'=0$. Hence x is equal to its conjugate, and is therefore an integer.

To complete the arithmetic definition of Int, it remains to define Pow. We do not however have to give an arithmetic definition of x Pow p in general, but only for two suitable primes p. We shall show in §3b how to define x Pow p when p is any natural number for which (p) is a prime ideal in the ring. This condition is stronger than supposing that p is a prime number, but we shall see that two suitable primes can be found among such values of p.

If p is an odd prime, it is known that (p) is a prime ideal if and only if $(m/p)=-1$, that is, if and only if m is not a quadratic residue mod p (Hecke [3], Satz 90). For a given m, this restricts p to certain residue classes mod $4m$. Choose a suitable p, which certainly exists by Dirichlet's theorem. Now the primitive roots mod p^2 fill certain residue classes mod p^2. Since $(p^2, 4m)=1$, we can find an odd prime q with $(m/q)=-1$ and q a primitive root mod p^2. Indeed, both conditions are satisfied by every prime q in certain residue classes mod $4mp^2$. Thus the p and q in the definition of Int may be chosen so that (p) and (q) are prime ideals.

3b. **Definition of prime-powers in quadratic rings.** To complete the considerations of §3a, we must show how to define x Pow p arithmetically when p is a natural number for which (p) is a prime ideal in the ring. Throughout this section, p will denote a fixed prime of this sort.

In the first place, x Asp p may be defined arithmetically by the formula

$$x \text{ Asp } p \leftrightarrow (\wedge y)[y \mid x \rightarrow y \mid 1 \vee p \mid y].$$

Indeed, if x Asp p and $y \mid x$, then clearly y Asp p, and hence $y \mid 1$ or $p \mid y$. (We have used the uniqueness of factorization into prime ideal factors.) Conversely, suppose the right side holds. Then $x \neq 0$, hence we may put $x = p^k u$ with $p \nmid u$. Since $u \mid x$, we must therefore have $u \mid 1$, and hence x Asp p.

The units in the imaginary quadratic ring are ± 1, $\pm i$ if $m = -1$, the sixth roots of 1 if $m = -3$, and otherwise just ± 1. Hence we may put

$$x \text{ Pow } p \leftrightarrow (\vee z)[z \text{ Asp } p \wedge (x = z^2 \vee x = pz^2)],$$

if m is negative but not -1 or -3. If $m = -1$, we put

$$x \text{ Pow } p \leftrightarrow (\vee z)[z \text{ Asp } p \wedge (x = z^4 \vee x = pz^4 \vee x = p^2z^4 \vee x = p^3z^4)],$$

and an analogous definition may be given when $m = -3$. Thus the required arithmetical definition of x Pow p has been given for $m < 0$. Unfortunately, we cannot extend this definition to positive values of m, since there are then infinitely many units.

An alternative definition for negative m, valid however only for $p > 3$ (which would be enough for the purposes of §3a), is

$$x \text{ Pow } p \leftrightarrow x \text{ Asp } p \wedge p - 1 \mid x - 1.$$

Indeed, if $x = p^k u$ with $u \mid 1$, and $p-1 \mid x-1$, then $p-1 \mid (p^k-1)u+u-1$, and hence $p-1 \mid u-1$. Thus $N(p-1) \mid N(u-1)$, and hence either $u = 1$ or $N(p-1) \leqq N(u-1)$. In the latter case, $|p-1| \leqq |u-1| \leqq 2$; hence if $p > 3$, we must have $u = 1$, or $x = p^k$ as required. It may be shown that this definition also fails for $m > 0$.

We must therefore find a new method of defining x Pow p if $m > 0$. It is known that in this case there is a fundamental unit $\eta > 1$, such that every unit has the form $\pm \eta^n$, where n is an integer (which may be negative). We put

$$\text{Luc } y \leftrightarrow (\vee u, v)[uv = 1 \wedge y = u^2 + v^2].$$

Then Luc y if and only if y has the form $\eta^{2k} + \eta^{-2k}$, where k is a natural number. These numbers y are all positive integers, and form a so-called Lucas sequence. We have used the fact that $N(\eta) = \pm 1$, that is, $\eta\eta' = \pm 1$, where η' is the conjugate of η.

In a real quadratic field, a number is the sum of four squares if and only if it is totally non-negative, that is, if and only if neither it nor its conjugate is negative (Landau [4]). In terms of elements of the quadratic ring we may define totally non-negative by

$$\text{Tot } x \leftrightarrow (\vee y, z_1, z_2, z_3, z_4)[y \neq 0 \wedge xy^2 = z_1^2 + z_2^2 + z_3^2 + z_4^2].$$

We are now in a position to define x Pow p in a real quadratic ring. We shall show that

$$x \text{ Pow } p \leftrightarrow x = 1 \vee \{x \text{ Asp } p \wedge \text{Tot } (x-2) \wedge (\wedge y)[\text{Luc } y \rightarrow \text{Tot } (x-y) \vee \text{Tot } (y-x)]\}.$$

If x Pow p, then the right side is clearly satisfied. Conversely, suppose that the right side is satisfied, but $x \neq 1$. Then x Asp p, hence $x = \pm p^k \eta^l$, where k is a natural number and l an integer. Since $x \geqq 2$, we must have $x = p^k \eta^l$. If x' denotes the conjugate of x, then $x' = p^k \eta'^l$, where $\eta' = \pm \eta^{-1}$; and since $x' \geqq 2$, we must have $x' = p^k \eta^{-l}$. Furthermore, x and x' are not separated by any term of the Lucas sequence, hence both lie in one and the same interval

$$[\eta^{2j} + \eta^{-2j}, \eta^{2j+2} + \eta^{-2j-2}].$$

Since $\eta^{2j+2} + \eta^{-2j-2} < \eta^2(\eta^{2j} + \eta^{-2j})$, it follows that

$$\eta^{-2} < x/x' < \eta^2.$$

But $x/x' = \eta^{2l}$, hence $l = 0$; thus $x = p^k$, that is x Pow p.

4a. **Definition of prime-powers in an arbitrary ID_1.** Let any fixed ID_1 be given. We shall formulate in this section sufficient conditions on p in order that x Pow p should be arithmetically definable in terms of p. The results obtained are applied in §§4b–4d.

While the considerations of this section apply to an arbitrary ID_1, it may happen in some cases that no p satisfies the conditions found. For this reason, the present results do not supersede those of §3b.

The first condition on p is that it should be prime in a strict sense, namely that (p) should be a prime ideal different from (0) or (1). In other words, p should satisfy the condition Pri p given by

$$\text{Pri } p \leftrightarrow p \neq 0 \wedge p \nmid 1 \wedge (\wedge x, y)[p \mid xy \rightarrow p \mid x \vee p \mid y].$$

We notice first that the powers of a prime element p are all different. For if $p^k = p^l$ with $k > l$, then either $p = 0$ or else $p^{k-l} = 1$ and hence $p \mid 1$.

From the definition we can readily show that

$$\text{Pri } p \wedge x \mid py \rightarrow p \mid x \vee x \mid y.$$

Indeed, by hypothesis there is a z such that $py = xz$, or $p \mid xz$. Thus $p \mid x \vee p \mid z$. If $p \mid z$, then $z = pu$, or $py = xpu$. Since $p \neq 0$, we have $y = xu$, and hence $x \mid y$. We therefore conclude that $p \mid x$ or $x \mid y$.

In particular, for any natural number n, Pri $p \wedge x \mid p^{n+1} \rightarrow p \mid x \vee x \mid p^n$. Using this, we see by induction that

$$\text{Pri } p \wedge x \mid p^n \rightarrow p \mid x \vee x \mid 1.$$

In order to define the powers of p, we impose on p two further conditions, one arithmetical in form and the other non-arithmetical. The non-arithmetical condition Nam p is needed in order to define x Asp p, and is given by

$$\text{Nam } p \leftrightarrow (\wedge x)\{(\wedge n)[p^n \mid x] \rightarrow x = 0\},$$

where n ranges over the natural numbers. The condition Nam p evidently implies that every ring element $x \neq 0$ can be put in the form $x = p^n u$ where $p \nmid u$. We then see that

$$\text{Pri } p \wedge \text{Nam } p \rightarrow \{x \text{ Asp } p \leftrightarrow x \neq 0 \wedge (\wedge y)[y \mid x \rightarrow y \mid 1 \vee p \mid y]\}.$$

Indeed, if $x = p^n u$ with $p \nmid u$, then each side of the equivalence is satisfied if and only if $u \mid 1$.

The arithmetical condition Arm p which we shall use is given by

$$\text{Arm } p \leftrightarrow (\wedge u)[p - 1 \mid u - 1 \wedge u \mid 1 \rightarrow u = 1].$$

We shall show that

$$\text{Arm } p \rightarrow \{x \text{ Pow } p \leftrightarrow x \text{ Asp } p \wedge p - 1 \mid x - 1\}.$$

Clearly, x Pow $p \rightarrow x$ Asp $p \vee p-1 \mid x-1$. Conversely, if x Asp p, then $x = p^n u$ where n is a natural number and $u \mid 1$. From $p-1 \mid x-1$, we find $p-1 \mid (p^n-1)u+u-1$, and hence $p-1 \mid u-1$. The condition Arm p then gives $u = 1$, that is, x Pow p.

Thus if p satisfies the conditions Pri p, Nam p, and Arm p, then x Pow p is arithmetically definable in terms of p. If p itself is arithmetically definable, then the set of powers of p is also.

4b. **The prime-power arithmetical model.** Among the natural numbers, it is possible to define multiplication in terms of addition and divisibility (Tarski [12]). We need only note the formulas

$$n = k(k+1) \leftrightarrow (\wedge m)[n \mid m \leftrightarrow k \mid m \wedge k + 1 \mid m],$$
$$n = kl \leftrightarrow (k+l)(k+l+1) = k(k+1) + l(l+1) + n + n.$$

Thus in any model for the arithmetic of natural numbers, it is sufficient to define arithmetically an operation and a relation corresponding to addition and divisibility.

A convenient method of constructing a model is to make correspond to the natural numbers the powers $p^0, p^1, p^2, p^3, \cdots$ of a prime element of the ring. We know that these are all different. Clearly, the ring multiplication defines addition in the model. It remains to define divisibility in the model. We know that $k \mid l \rightarrow p^k - 1 \mid p^l - 1$. If the converse were true, we should have the required definition. We therefore impose on p the (non-arithmetical) condition Div p defined by

$$\text{Div } p \leftrightarrow (\wedge k, l)[p^k - 1 \mid p^l - 1 \rightarrow k \mid l],$$

where k and l range over the natural numbers. If p satisfies this condition, and if x and y are powers of p, then the divisibility of y by x in the model is expressed by $x-1 \mid y-1$.

Div may be defined arithmetically in terms of Pow by the formula

$$\text{Div } p \leftrightarrow (\wedge x, y)[x \text{ Pow } p \wedge y \text{ Pow } p \wedge x - 1 \mid y - 1 \wedge y - 1 \mid x - 1 \rightarrow x = y].$$

This provides a condition equivalent to Div p which is more convenient to verify. In the first place, if Div p and $x=p^k$, $y=p^l$, $x-1 \mid y-1$, $y-1 \mid x-1$, we find that $k \mid l$ and $l \mid k$, hence $k=l$, and therefore $x=y$; that is, the condition on the right is satisfied. Conversely, suppose that the condition on the right is satisfied. We wish to prove Div p; that is, given natural numbers k and l with $p^k-1 \mid p^l-1$, we wish to conclude $k \mid l$. Let $d=(k, l)$, and choose natural numbers r and s so that $kr-ls=d$. From $p^k-1 \mid p^{kr}-1$ and $p^l-1 \mid p^{ls}-1$, we conclude

$$p^k - 1 \mid (p^{ls} - 1)p^d + p^d - 1, \qquad p^k - 1 \mid p^{ls} - 1,$$

and therefore

$$p^k - 1 \mid p^d - 1.$$

Since $d \mid k$, we also have $p^d-1 \mid p^k-1$, and hence by our hypothesis $k=d$, which is equivalent to $k \mid l$.

As a simple example, we construct a prime-power model in the ring of integers itself. We see that any prime $p>3$ satisfies the conditions Pri p, Nam p, Arm p, and Div p. We may thus use the set of powers of 5 as our model; notice that 5 is arithmetically definable. The powers of 5 are defined by

$$x \text{ Pow } 5 \leftrightarrow (\wedge y)[y \mid x \rightarrow y \mid 1 \vee 5 \mid y] \wedge 4 \mid x - 1.$$

Furthermore, every statement in the arithmetic of natural numbers can be replaced by an equivalent statement about this model. We first eliminate multiplication in favor of divisibility, obtaining an equivalent statement concerning the natural numbers. Then we restrict each variable x by the condition x Pow 5, and we replace 0 by 1, 1 by 5, each sum $x+y$ by xy, and each relation $x \mid y$ by $x-1 \mid y-1$. This statement, interpreted in the ring of integers, is equivalent to the original statement in the arithmetic of natural numbers.

For example, the prime-pair conjecture

$$(\wedge x)(\vee y)(\wedge z)[(z \mid x + y \rightarrow z = 1 \vee z = x + y) \wedge (z \mid x + y + 2 \rightarrow z = 1 \vee z = x + y + 2)]$$

is a formula of the arithmetic of natural numbers which is stated initially in a form involving only addition and divisibility. An equivalent statement in the ring of integers is

$$(\wedge x)\{x \text{ Pow } 5 \rightarrow (\vee y)[y \text{ Pow } 5 \wedge (\wedge z)\{z \text{ Pow } 5 \rightarrow (z - 1 \mid xy - 1 \rightarrow z = 5 \vee z = xy) \wedge (z - 1 \mid 25xy - 1 \rightarrow z = 5 \vee z = 25xy)\}]\}.$$

While this model was intended primarily as an example, we may notice

that in the statements about the model, we use only multiplication and the function $x-1$. We thus have a new proof that the arithmetic of integers is undecidable when the given operations are successor and multiplication. (For another proof, see Julia Robinson [7], §1.)

In a similar way, we can construct a prime-power model in an imaginary quadratic ring, or in a polynomial ring over the integers or over an imaginary quadratic ring. These are, however, all cases in which we know how to define the integers.

4c. **Prime-power models in polynomial rings.** Suppose that we are given the ring of polynomials in one or more variables $\alpha, \beta, \gamma, \cdots$, over any ID_1. The conditions Pri p, Nam p, Arm p, Div p are clearly all satisfied by $p=\alpha$. Thus a suitable model is definable arithmetically in terms of α. If α itself were definable, we would conclude that all problems of the arithmetic of natural numbers could be formulated in the polynomial ring. Unfortunately, however, α is not definable, and I do not know whether the conclusion mentioned is true or false.

We shall use in this section a generalization of the method of §4b. Instead of defining one model for the arithmetic of natural numbers, we shall define a non-empty family of such models. This is just as effective so far as formulating problems of the arithmetic of natural numbers in the ring is concerned. We do not have to find a suitable arithmetically definable element p, but only an arithmetically definable non-empty set of such elements.

It is clear that any non-constant element of the polynomial ring satisfies conditions Nam p, Arm p, and Div p. Thus the condition

$$\text{Pri } p \wedge \backsim \text{Con } p$$

serves to define a non-empty set of suitable values of p. If the set of constants is arithmetically definable, then the condition imposed on p is arithmetical. In this case, we have defined arithmetically a family of models of the arithmetic of natural numbers, hence any problem of this arithmetic can be formulated in our ring.

In particular, if the ring of constants is a field, then $\text{Con } p \leftrightarrow p=0 \vee p \mid 1$, so that Pri $p \wedge \backsim$ Con p reduces simply to Pri p. To formulate any statement of the arithmetic of natural numbers in the polynomial ring, we first eliminate multiplication in favor of divisibility, obtaining an equivalent statement concerning the natural numbers. Then we restrict every variable x by the condition x Pow p, replace 0 by 1, 1 by p, expressions of the form $x+y$ by xy, relations of the form $x \mid y$ by $x-1 \mid y-1$, and prefix the whole by either of the following:

$$(\wedge p)[\text{Pri } p \rightarrow \cdots] \quad \text{or} \quad (\vee p)[\text{Pri } p \wedge \cdots].$$

The two resulting formulas, considered as statements about the polynomial ring, are equivalent to each other, since any statement holding in one model

will hold in all models, and both are equivalent to the given statement in the arithmetic of natural numbers.

As an example, the conjecture that there are infinitely many primes of the form 2^n-1 may be stated in the arithmetic of natural numbers in the form

$$(\wedge x)(\vee y)(\wedge z)\{(z \mid x+y \to z = 1 \vee z = x+y) \wedge (z \mid x+y+1 \to z = 1 \vee 2 \mid z)\}.$$

The corresponding statement in any polynomial ring over a field has the form

$$(\wedge p)[\text{Pri } p \to (\wedge x)\{x \text{ Pow } p \to (\vee y)[y \text{ Pow } p \wedge (\wedge z)\{z \text{ Pow } p \to (z-1 \mid xy-1 \to z = p \vee z = xy) \wedge (z-1 \mid pxy-1 \to z = p \vee p^2-1 \mid z-1)\}]\}].$$

From this, we may eliminate Pri and Pow, thus obtaining an arithmetical statement concerning the polynomial ring, which is equivalent to the original conjecture.

Notice that the result obtained here is more general than that of §2, in that there is now no requirement that the field of constants have characteristic zero. The polynomial ring considered might for example be the ring of polynomials in α over the two element field.

Instead of supposing that Con is arithmetically definable, another adequate hypothesis is that the polynomial ring satisfies the condition

$$(\wedge p)[p \mid 1 \vee \text{Nam } p].$$

This will be the case if and only if the ring of constants satisfies the same condition. The condition

$$\text{Pri } p \wedge \text{Arm } p \wedge \text{Div } p$$

then serves to define a non-empty set of suitable values of p. This condition may be expressed in an arithmetic form, since Div p was expressed arithmetically in terms of x Pow p, x Pow p is arithmetically definable under the hypotheses Pri p, Nam p, and Arm p, and if the ring satisfies the assumed condition, Nam p follows from Pri p.

The condition $(\wedge p)[p \mid 1 \vee \text{Nam } p]$ is easily seen to hold in the ring of algebraic integers in a field of finite degree over the rationals, by making use of the norm. We conclude that any statement in the arithmetic of natural numbers can be formulated in a polynomial ring over such a ring.

It should be noticed that the formula $(\wedge p)[p \mid 1 \vee \text{Nam } p]$ is not true in every ID_1. This follows easily from the Skolem-Gödel theorem (according to which a consistent set of axioms has a model), as was pointed out to me by A. Tarski. A simple example of an ID_1 in which the formula fails was supplied by the referee. Consider the rational functions of α and β which have the

form $f(\alpha)+\alpha^{-n}\beta g(\alpha, \beta)$, where $f(\alpha)$ and $g(\alpha, \beta)$ are polynomials with integer coefficients, and n is a natural number. These form an ID_1 of which α and β are elements, and we have $\alpha^n \mid \beta$ for every n, although $\alpha \nmid 1$ and $\beta \neq 0$.

4d. **Proof that any polynomial ring over an ID_1 is undecidable.** An axiom system, with specified primitive concepts, is called decidable if there is a general method of deciding whether a statement involving the given primitive concepts and the concepts of elementary logic does or does not follow from the axioms; otherwise it is called undecidable. The set of axioms is called *essentially undecidable* if it is consistent, but has no consistent extension which is decidable. Mostowski and Tarski have found a finite set of axioms, with primitive concepts 0, 1, $+$, $\cdot$, which are true for the natural numbers, but are essentially undecidable. (See the abstracts [11] and [5], and the discussion in [7], §4.) Let the conjunction of these axioms be denoted by $\boldsymbol{M}$. The exact form of $\boldsymbol{M}$ is not important for our purposes.

If S is an arbitrary statement in the arithmetic of natural numbers, involving the primitive concepts 0, 1, $+$, $\cdot$, we may find an equivalent statement S', involving the primitive concepts 0, 1, $+$, $\mid$, by using the definition of multiplication in terms of divisibility given in §4b. From S' we construct $S^*(p)$ by restricting each variable x by the condition x POW p, and by replacing 0 by 1, 1 by p, expressions of the form $x+y$ by xy, and relations $x \mid y$ by $x-1 \mid y-1$, and then eliminating POW by means of the equivalences

$$x \text{ POW } p \leftrightarrow x \text{ ASP } p \wedge p - 1 \mid x - 1,$$

$$x \text{ ASP } p \leftrightarrow x \neq 0 \wedge (\wedge y)[y \mid x \rightarrow y \mid 1 \vee p \mid y].$$

(Notice that under certain conditions POW and ASP actually have the meanings Pow and Asp.) Interpreted in a given ID_1, $S^*(p)$ is a statement about p which is equivalent to the statement S, provided p satisfies the conditions Pri p, Nam p, Arm p, and Div p. In other words, if S is a true statement in the arithmetic of natural numbers, then $S^*(p)$ is satisfied by every such p; and if S is false, then $S^*(p)$ is satisfied by no such p.

For example, if S is any statement in the arithmetic of natural numbers, then $S^*(5)$ and $S^*(7)$ are both equivalent statements in the ring of integers, and

$$(\wedge p)[\text{Pri } p \rightarrow S^*(p)] \quad \text{and} \quad (\vee p)[\text{Pri } p \wedge S^*(p)]$$

are both equivalent statements in any polynomial ring over a field.

Let us suppose that in the given ring, there is at least one suitable value of p. This is the case in any polynomial ID_1. We know that if a non-empty set of such values of p is arithmetically definable, then all problems of the arithmetic of natural numbers can be stated in the ring. We shall no longer make this assumption, nor shall we be able to draw the same conclusion. We shall, however, show that the ring is undecidable.

Consider the set $\mathcal{A}$ of statements S in the arithmetic of natural numbers

for which

$$(\wedge p)[\boldsymbol{M}^*(p) \rightarrow \boldsymbol{S}^*(p)]$$

is a true statement in our ring. On the one hand, $\boldsymbol{M}$ itself is in $\mathcal{A}$. On the other hand, every such statement $\boldsymbol{S}$ must be true. In fact, the set $\mathcal{A}$ is just the set of statements true in all the "prime-power" models corresponding to values of p for which $\boldsymbol{M}^*(p)$ holds. These values of p include those for which Pri p, Nam p, Arm p, and Div p; by hypothesis, there is at least one such p. For the latter values of p, the model obtained is isomorphic to the arithmetic of natural numbers. If all values of p satisfying $\boldsymbol{M}^*(p)$ also satisfy the other conditions, then $\mathcal{A}$ is simply the set of true statements of the arithmetic of natural numbers. If there are additional values of p satisfying $\boldsymbol{M}^*(p)$, these need not be primes, and the "prime-power" models obtained using such values of p need not be isomorphic to the arithmetic of natural numbers. In this case, $\mathcal{A}$ may be a proper subset of the set of true statements in the arithmetic of natural numbers.

Furthermore, we see that if $\boldsymbol{S}$ is deducible from statements in $\mathcal{A}$, then $\boldsymbol{S}$ itself is in $\mathcal{A}$. Since $\mathcal{A}$ is consistent and contains the essentially undecidable axiom $\boldsymbol{M}$, there cannot be a general method of deciding whether a statement $\boldsymbol{S}$ is in $\mathcal{A}$ or not. Now if the given ring were decidable, there would be such a method; hence the given ring must be undecidable.

5a. **Algebraic rings with one fundamental unit.** Let us consider the ring of algebraic integers in a field of degree n over the rationals. This field may be generated by adjoining an algebraic number α to the field of rationals. Suppose that among the conjugates of α, including α itself, there are r_1 real numbers, and r_2 pairs of conjugate imaginary numbers, so that $n=r_1+2r_2$. The units in our ring form an Abelian group. According to a theorem of Dirichlet (Hecke [3], Satz 100), this group has a basis consisting of r_1+r_2 elements, one of finite order, the others of infinite order. The basis elements of infinite order are called the fundamental units of the ring.

In §§5a–5c, we shall study rings with one fundamental unit. Thus we suppose that $r_1+r_2=2$. There are three possibilities: $r_1=2$, $r_2=0$, hence $n=2$; $r_1=1$, $r_2=1$, hence $n=3$; $r_1=0$, $r_2=2$, hence $n=4$. Thus the present methods apply to certain cubic and quartic rings, as well as to real quadratic rings. The decision problem is open for rings with more than one fundamental unit.

We suppose that a fixed ring with one fundamental unit is given. The group of units in our ring has a basis consisting of a unit η of infinite order and a unit ζ of finite order. The order of ζ is clearly even, say $2s$, since -1 must be a power of ζ. Thus all units of the ring are expressible in the form $\eta^k\zeta^l$, where $k=0, \pm 1, \pm 2, \cdots$, and $l=0, 1, \cdots, 2s-1$.

We may of course take $\zeta=e^{\pi i/s}$. If $n=2$, we must have $s=1$, since the ring is real. In any case, we must have $\phi(2s) \mid n$, since ζ generates a field of degree $\phi(2s)$. Thus if $n=3$, we must again have $s=1$. But if $n=4$, we are allowed

$\phi(2s)=1$, 2, or 4, and hence $s=1$, 2, 3, 4, 5, or 6. If $s=4$, 5, or 6, then $\phi(2s)=4$, so that ζ itself generates the quartic field; that is, $s=4$, 5, or 6 occurs only for the ring of algebraic integers in the field generated by $e^{\pi i/s}$. The smaller values of s can occur in various cases. If the quartic field has no quadratic subfield, then we must have $s=1$.

In order to show that all problems of the arithmetic of natural numbers can be formulated in the ring, it is sufficient to construct a model for the arithmetic of integers. That is, we define arithmetically a set of ring elements, and two operations on them corresponding to addition and multiplication, so that the model obtained is isomorphic to the ring of integers. It is also sufficient to define a non-empty family of such models.

In the ring of integers, multiplication can be defined arithmetically in terms of addition, divisibility, and 1. (Compare Tarski [12]; the corresponding fact for the natural numbers was used in §4b.) It is sufficient to note the following equivalences:

$$n = k(k+1) \leftrightarrow (\wedge m)[n \mid m \leftrightarrow k \mid m \wedge k+1 \mid m] \wedge 2k+1 \mid 2n-k,$$

$$n = kl \leftrightarrow (k+l)(k+l+1) = k(k+1)+l(l+1)+2n,$$

where $2n$ stands for $n+n$. The condition $2k+1 \mid 2n-k$ is designed to eliminate the possibility $n=-k(k+1)$. In this case, $2n-k=-k(2k+3)$, which is prime to $2k+1$. Thus if $2k+1 \mid 2n-k$, we must have $2k+1 \mid 1$, and hence $k=0$ or $k=-1$; consequently, $k(k+1)=0$, so that the sign doesn't matter.

Thus in our model or models, it is sufficient to define addition, divisibility, and the unity element. As elements of the model, corresponding to the integers $\cdots, -2, -1, 0, 1, 2, \cdots$, we shall select the powers $\cdots, \theta^{-2}, \theta^{-1}, \theta^0, \theta^1, \theta^2, \cdots$ of some unit θ. If $\theta=\eta^m$, where m is a positive integer which is a multiple of $2s$, then we can express the fact that x is one of the selected elements by the arithmetical condition Sel x defined by

$$\text{Sel } x \leftrightarrow (\vee u)[u \mid 1 \wedge x = u^m].$$

For if $x=\theta^k$, we may take $u=\eta^k$; and if $u \mid 1$, then $u=\eta^k\zeta^l$, and hence $u^m=\eta^{km}=\theta^k$.

Clearly, the zero element of the model is 1, the unity element is θ, and addition is defined by ring multiplication. It remains to consider the definition of divisibility in the model, as well as the arithmetical definition of θ itself.

5b. **Definition of divisibility in the unit model.** We start with the observation that neither the fundamental unit η nor any of its conjugates can have absolute value 1. For among the conjugates $\eta_1, \eta_2, \cdots, \eta_n$, there are r_1 real numbers and r_2 pairs of conjugate complex numbers. Hence among $|\eta_1|, |\eta_2|, \cdots, |\eta_n|$, there are at most $r_1+r_2=2$ different numbers. Furthermore, their product is $|N(\eta)|=1$. Hence if one of the numbers $|\eta_j|$ were 1, all would

be 1. But if $|\eta_1| = |\eta_2| = \cdots = |\eta_n| = 1$, then by a theorem of Kronecker, η would be a root of unity, contrary to hypothesis.

We next note the following elementary inequality:

$$|z^k - 1| \cdot ||z| - 1| \leqq |z^{k+1} - 1|,$$

wherever z is a complex number and k a natural number. This is trivial if $k=0$ or $|z|=1$. If $k \geqq 1$ and $|z| > 1$, we have

$$\begin{aligned} |z^k - 1|(|z| - 1) &\leqq (|z|^k + 1)(|z| - 1) = |z|^{k+1} - |z|^k + |z| - 1 \\ &\leqq |z|^{k+1} - 1 \leqq |z^{k+1} - 1|. \end{aligned}$$

The case $k \geqq 1$ and $|z| < 1$ may be treated similarly, or derived from the preceding case by replacing z by $1/z$.

In particular, if $\theta_1, \theta_2, \cdots, \theta_n$ are the conjugates of the unit $\theta = \eta^m$, we have

$$|\theta_j^k - 1| \cdot ||\theta_j| - 1| \leqq |\theta_j^{k+1} - 1|$$

for $j = 1, 2, \cdots, n$. Multiplying these inequalities together, we find

$$|N(\theta^k - 1)| \cdot \prod_{j=1}^{n} ||\theta_j| - 1| \leqq |N(\theta^{k+1} - 1)|.$$

Now

$$\prod_{j=1}^{n} ||\theta_j| - 1| = \prod_{j=1}^{n} ||\eta_j|^m - 1|,$$

and as $m \to \infty$, the factors of the product on the right approach 1 or ∞ according as $|\eta_j| < 1$ or $|\eta_j| > 1$. The latter must happen for at least one value of j. Hence the product itself becomes infinite as $m \to \infty$. Choose m so large that the product is greater than 1. Then

$$|N(\theta^k - 1)| < |N(\theta^{k+1} - 1)|$$

for all natural numbers k. We shall suppose, in this section and the next, that $\theta = \eta^m$, where m is a positive integer which is a multiple of $2s$, and is large enough so that this inequality holds.

We shall now prove the truth of the equivalence

$$\theta^k - 1 \mid \theta^l - 1 \leftrightarrow k \mid l,$$

where k and l are any integers. This furnishes the required arithmetic definition of divisibility in the model. (A similar definition was used in §4b for the prime-power model.) It is sufficient to consider the cases $k \geqq 0$ and $l \geqq 0$, since $\theta^k - 1 \mid \theta^{-k} - 1$. We know of course that $k \mid l \to \theta^k - 1 \mid \theta^l - 1$, and it remains to consider the converse. Suppose that

$$\theta^k - 1 \mid \theta^l - 1.$$

If $k=0$, we have $\theta^l-1=0$, and hence $l=0$. Now suppose $k>0$, and put $l=ka+b$, with $0\leqq b<k$. We have

$$\theta^k - 1 \mid (\theta^{ka} - 1)\theta^b + \theta^b - 1,$$

hence $\theta^k-1\mid\theta^b-1$, and therefore

$$N(\theta^k - 1) \mid N(\theta^b - 1).$$

Since $|N(\theta^b-1)| < |N(\theta^k-1)|$, we must have $N(\theta^b-1)=0$, hence $\theta^b-1=0$, and thefore $b=0$. Thus $l=ka$, or $k\mid l$, as was to be shown.

5c. **Definition of the unity element in the unit model.** To complete the discussion of the model, we must consider the arithmetical definability of θ, which plays the role of unity element in the model. One method of treating this is by using the concept of divisibility just defined for the model.

Notice that in the ring of integers, 1 is not definable in terms of addition and divisibility, since changing the sign of all integers preserves both addition and divisibility. However, either of the two integers a satisfying $(\wedge b)[a\mid b]$ could equally well serve as unity element of the ring. If, using either value of a as unity element, we define multiplication as in §5a, we obtain either the ring of integers, with the usual definition of multiplication, or an isomorphic ring.

The same considerations, applied to the model, show that either of the two elements, $u=\theta$ or $u=\theta^{-1}$, which satisfy the arithmetical condition One u given by

$$\text{One } u \leftrightarrow \text{Sel } u \wedge (\wedge v)[\text{Sel } v \rightarrow u - 1 \mid v - 1],$$

can serve equally well as unity element of the model. Because of this ambiguity, we have defined arithmetically a pair of models for the arithmetic of integers, instead of a single model.

We now see that any statement in the arithmetic of natural numbers can be formulated in our ring. We first restate as a proposition about the ring of integers, and then eliminate multiplication in favor of divisibility. Finally, we restrict each variable x by Sel x, replace 0 by 1, 1 by u, each expression of the form $x+y$ by xy, relations of the form $x\mid y$ by $x-1\mid y-1$, and prefix the whole by either

$$(\wedge u)[\text{One } u \rightarrow \cdots] \quad \text{or} \quad (\vee u)[\text{One } u \wedge \cdots].$$

The resulting formula, interpreted in our ring, is equivalent to the original statement in the arithmetic of natural numbers.

It may be of interest to consider also a quite different method of defining θ, namely as a root of a certain equation. We put

$$\text{Req } u \leftrightarrow u^k + c_1u^{k-1} + \cdots + c_k = 0,$$

where the equation on the right is the irreducible equation over the field of

rationals of which θ is a root. Since θ is a unit, $c_1, c_2, \cdots, c_k$ are integers, and $c_k = \pm 1$. Indeed, since θ is an even power of η, we must have $N(\theta) = 1$, and hence $c_k = (-1)^k$.

Since θ is irrational, we must have $k > 1$; on the other hand, we must have $k \mid n$. Thus the only possible cases are $n = 2$, $k = 2$; $n = 3$, $k = 3$; $n = 4$, $k = 2$ or 4. In any case, Req u is satisfied by at most four values of u, one of which is θ. We shall show that in fact Req u is satisfied either by θ only, or by just θ and θ^{-1}.

In the first place, if $k = 2$ then Req u takes the form $u^2 + c_1 u + 1 = 0$, which clearly has the roots θ and θ^{-1}. In the remaining cases, $k = n$, and hence our ring is the ring of algebraic integers in the field generated by θ. If any conjugate of θ is in the ring, then there must be an automorphism of the ring taking θ into this conjugate. But any automorphism of the ring must take θ, which satisfies the arithmetical condition One u, into an element satisfying this same condition, that is, into either θ or θ^{-1}. Thus in case $k = n$, and hence in all cases, the condition Req u is satisfied either by θ alone or by θ and θ^{-1}.

It is of course absurd that θ and θ^{-1} should be two of the roots of an irreducible cubic. Hence if $k = 3$, Req u is satisfied only by θ. Consider next the case $k = 4$. If both θ and θ^{-1} satisfy Req u, then this condition must take the form $u^4 + c_1 u^3 + c_2 u^2 + c_1 u + 1 = 0$. It follows that $\theta + \theta^{-1}$ is a root of a quadratic equation, and hence that our quartic ring has a quadratic subring. Conversely, if there is a quadratic subring, then we see that θ has a conjugate in the quartic ring, and hence is not uniquely determined by the condition Req u.

Thus the condition Req u is satisfied by θ alone in the case of a cubic ring, or of a quartic ring with no quadratic subring, but is satisfied by both θ and θ^{-1} in the case of a quadratic ring, or of a quartic ring with a quadratic subring.

We now ask, if θ is not uniquely determined by the condition Req u, is it possible that θ is nevertheless arithmetically definable? This does indeed happen in certain cases. For example, suppose we are given the ring of algebraic integers in the field generated by $\alpha = (-3 + 2^{1/2})^{1/2}$. Then it may be shown that of the conjugates of α, that is, of the roots of $y^4 + 6y^2 + 7 = 0$, only $\pm\alpha$ belong to the ring. We may take $\theta = 3 + 2 \cdot 2^{1/2} = 2\alpha^2 + 9$. Hence θ is defined by

$$x = \theta \leftrightarrow (\vee y)[x = 2y^2 + 9 \wedge y^4 + 6y^2 + 7 = 0].$$

A similar procedure is possible whenever we are given the ring of algebraic integers in a quartic field which is generated by an element not all of whose conjugates lie in the field, provided there is a real quadratic subfield. It can be shown that this is the only case in which θ is arithmetically definable, except when it is the only ring element satisfying the condition Req u.

We have thus determined in exactly what cases it is possible to define the unit model uniquely, rather than as one of a pair of models.

6. **Undecidability of certain rings of formal power series.** In this section,

we shall consider only rings of formal power series, as opposed, for example, to the ring of entire functions of a complex variable studied in §2. The formal power series in α over a given ring of constants have the form

$$c_0 + c_1\alpha + c_2\alpha^2 + c_3\alpha^3 + \cdots,$$

where the coefficients are constants, no consideration being given to convergence.

Consider first the ring of formal power series in α with integer coefficients. Here it is easily seen that $x \mid 1$ if and only if the constant term of x is ± 1. Thus the constant term of x is zero if and only if $x-1 \mid 1$ and $x+1 \mid 1$. If we define equivalence by the condition

$$x \approx y \leftrightarrow x - y - 1 \mid 1 \wedge x - y + 1 \mid 1,$$

then we see that x and y are equivalent if and only if they have the same constant term.

The relation $\approx$ is indeed an equivalence relation. Furthermore,

$$u \approx x \wedge v \approx y \rightarrow u + v \approx x + y \wedge uv \approx xy.$$

Thus addition and multiplication are also defined for the equivalence classes, and these form a ring isomorphic to the ring of integers. This arithmetical model differs from those constructed in previous sections in having as elements classes of elements of the given ring, rather than single elements. We can conclude, nevertheless, that all statements of the arithmetic of integers (and hence all statements of the arithmetic of natural numbers) can be formulated in the ring. We need only to notice that in making the translation, we must replace $=$ by $\approx$ throughout. In particular, we conclude that the ring of formal power series with integer coefficients is undecidable.

A similar argument applies to the ring of formal power series in α with coefficients from an imaginary quadratic ring, and indeed exactly the same definition of equivalence may be used. The equivalence classes form a ring isomorphic to the ring of constants. Since the integers are arithmetically definable in the ring of constants, we again conclude that all statements of the arithmetic of integers can be formulated in the ring.

Finally, we consider the ring of formal power series in α over a field. Here $x \mid 1$ if and only if the constant term of x is not zero. If we define equivalence by the condition

$$x \approx y \leftrightarrow x - y \nmid 1,$$

then again x and y are equivalent if and only if they have the same constant term. The equivalence classes here form a field isomorphic to the field of constants. Since Int is arithmetically definable in the field of rationals (Julia Robinson [7], Theorem 3.1), we see that all problems of the arithmetic of integers can be stated in the ring of formal power series with rational coeffi-

cients, and hence that this ring is undecidable. If any other undecidable field were known, we could conclude that the power series ring over the field is also undecidable.

The method just considered gives us no information concerning the decidability of the rings of formal power series in α with real or complex coefficients, since in these cases the field of constants is decidable (Tarski [10]). The decision problem is open for these rings.

7. **A negative result on the unique definability of models.** We have shown that various rings are undecidable; this was done, except in §4d, by showing that all problems of the arithmetic of natural numbers can be stated in the ring. We defined arithmetically either a model for the arithmetic of natural numbers, or a non-empty family of such models, depending on a parameter subject to certain arithmetical conditions. (In some cases, we considered models for the arithmetic of integers, but this is immaterial, since the natural numbers are arithmetically definable in terms of the integers.)

In this section, we shall consider only models whose elements are single elements of the given ring, thus excluding models such as those considered in §6. In those cases where a single model is defined, rather than a family of models, we may speak of the model being *uniquely definable.*

If the natural numbers are themselves definable (in an ID_1 of characteristic zero), then we certainly have a uniquely definable model. Various other uniquely definable models have also been found; in particular, see §5c, where a pair of models is first defined, and then the unique definability of one of the models is considered. Another example is found at the end of this section.

The main result which we wish to prove in this section is that there are some ID_1's in which a non-empty family of models for the arithmetic of natural numbers is arithmetically definable, but no such model is uniquely definable. We shall show that this is the case in the ring of polynomials in two or more variables $\alpha, \beta, \gamma, \cdots$ over a finite field. A family of models was defined arithmetically in §4c; it remains to prove that no suitable model is uniquely definable.

Suppose that there were a uniquely definable model for the arithmetic of natural numbers in our polynomial ring. Since every natural number is arithmetically definable in the arithmetic of natural numbers, it would follow that every element of the model is arithmetically definable in the ring. Since the field of constants is finite, this implies that some non-constant elements of the polynomial ring would be arithmetically definable. We shall show that this is not the case.

In order that a ring element be arithmetically definable, or indeed definable in any sense in terms of addition and multiplication, it is necessary that it be invariant under all automorphisms of the ring. Among the automorphisms of the polynomial ring is σ, defined by the condition that all constants are fixed, together with the equations

$$\sigma(\alpha) = \alpha + \beta^n, \qquad \sigma(\beta) = \beta, \qquad \sigma(\gamma) = \gamma, \cdots,$$

where n is any natural number. Let x be any polynomial in the ring which contains α, and choose n greater than the degree of x. We see that $\sigma(x)$ will be of at least the nth degree, hence of a higher degree than x, and consequently $\sigma(x) \neq x$. A similar construction may be made if x does not contain α, but contains one of the other variables $\beta, \gamma, \cdots$. Thus to each non-constant polynomial x an automorphism σ can be found for which $\sigma(x) \neq x$. Hence a non-constant element x of the polynomial ring is not arithmetically definable.

The argument given does not apply to the ring of polynomials in one variable α over a finite field. In this case, there are indeed definable non-constant elements. In the first place, in such a ring (as in the ring of polynomials in α over any field), we may define constants by $\operatorname{Con} x \leftrightarrow x = 0 \vee x \mid 1$, and linear polynomials by

$$\operatorname{Lin} u \leftrightarrow \infty \operatorname{Con} u \wedge (\wedge y)(\vee z)[\operatorname{Con}(y - uz)].$$

Since there are but a finite number of linear polynomials in α over a finite field, their product is arithmetically definable.

This does not of course show that there is a uniquely definable model for the arithmetic of natural numbers in the polynomial ring. However, as we have seen in §4c, a suitable model is furnished by the powers of any irreducible polynomial. To uniquely define a model, it is thus necessary only to find some irreducible polynomial which is arithmetically definable. I do not know whether there is always such a polynomial. But if the field of constants contains but two elements, we see that $\alpha^2+\alpha+1$ is irreducible, and is defined by

$$x = \alpha^2 + \alpha + 1 \leftrightarrow (\vee u, v)[x = uv + 1 \wedge \operatorname{Lin} u \wedge \operatorname{Lin} v \wedge u \neq v].$$

Thus in the ring of polynomials in α over the field of residue classes modulo 2, there is indeed a uniquely definable model.

References

1. A. Church, *An unsolvable problem of elementary number theory*, Amer. J. Math. vol. 58 (1936) pp. 345–363.

2. K. Gödel, *Über formal unentscheidbare Sätze der Principia Mathematica und verwandter Systeme* I, Monatshefte für Mathematik und Physik vol. 38 (1931) pp. 173–198.

3. E. Hecke, *Vorlesungen über die Theorie der algebraischen Zahlen*, Leipzig, 1923.

4. E. Landau, *Über die Zerlegung total positiver Zahlen in Quadrate*, Nach. Ges. Wiss. Göttingen, 1919, pp. 392–396.

5. A. Mostowski and A. Tarski, *Undecidability in the arithmetic of integers and in the theory of rings* (abstract), J. Symbolic Logic vol. 14 (1949) p. 76.

6. M. Presburger, *Über die Vollständigkeit eines gewissen Systems der Arithmetik ganzer Zahlen, in welchem die Addition als einzige Operation hervortritt*, Comptes-rendus du I Congrès des Mathématiciens des Pays Slaves, Warsaw, 1929, pp. 92–101, 395.

7. Julia Robinson, *Definability and decision problems in arithmetic*, J. Symbolic Logic vol. 14 (1949) pp. 98–114.

8. B. Rosser, *Extensions of some theorems of Gödel and Church*, J. Symbolic Logic vol. 1 (1936) pp. 87–91.

9. W. Szmielew, *Decision problem in group theory*, Proceedings of the Tenth International Congress of Philosophy, Amsterdam, 1948, pp. 763–766.

10. A. Tarski, *A decision method for elementary algebra and geometry*, Rand Corporation, Santa Monica, Calif., 1948.

11. ———, *On essential undecidability* (abstract), J. Symbolic Logic vol. 14 (1949) pp. 75–76.

12. ———, *Undecidability of group theory* (abstract), J. Symbolic Logic vol. 14 (1949) pp. 76–77.

UNIVERSITY OF CALIFORNIA,
BERKELEY, CALIF.