THE JOURNAL OF SYMBOLIC LOGIC
Volume 14, Number 2, June 1949

DEFINABILITY AND DECISION PROBLEMS IN ARITHMETIC

JULIA ROBINSON

Introduction. In this paper, we are concerned with the arithmetical definability of certain notions of integers and rationals in terms of other notions. The results derived will be applied to obtain a negative solution of corresponding decision problems.[1]

In Section 1, we show that addition of positive integers can be defined arithmetically in terms of multiplication and the unary operation of successor S (where $Sa = a + 1$). Also, it is shown that both addition and multiplication can be defined arithmetically in terms of successor and the relation of divisibility $|$ (where $x|y$ means x divides y). Thus the elementary theory of integers with S and $\cdot$ (or S and $|$) as the only primitive notions, which may seem rather narrow, is sufficient to express every idea or result which can be expressed in elementary number theory, i.e., the arithmetic of integers with $+$ and $\cdot$. An axiomatic problem concerning the system of positive integers with S and $\cdot$ is discussed in Section 2.

In Section 3, we show that the notion of an integer can be defined arithmetically in terms of the notion of a rational number and the operations of $+$ and $\cdot$ on rationals. Hence the arithmetic of rationals is adequate for the formulation of all problems of elementary number theory.

Since the solution of the decision problem is known to be negative for elementary number theory, it follows from our results that the solution of the decision problem is negative for any of the related theories mentioned above. As a further consequence, we see that the solution of the decision problem for the arithmetical theory of arbitrary fields is also negative. These problems will be discussed in Section 4.

The way in which we use the terms "arithmetic," "arithmetical or elementary theory," and "arithmetical definability" calls for some comments. For example, by the arithmetic (or elementary theory) of integers, we mean that part of the general theory of integers which can be developed without using any notions of a set-theoretical nature; that is, the part of the theory which can be formalized within the lower predicate calculus. Thus in formulating statements of the arithmetic of integers, we use only variables representing arbitrary integers; logical constants of the lower predicate calculus: $\wedge$ (and), $\vee$ (or), $\sim$ (not), $\rightarrow$ (if, then), $\leftrightarrow$ (if and only if), $\bigwedge$ (for every), $\bigvee$ (there exists), $=$ (equals); and mathematical constants denoting individual integers such as 0 and 1, relations between integers such as $<$, and operations on integers such as $+$ and $\cdot$.

The notion of arithmetical definability will be explained by means of examples.

Received September 28, 1948.

[1] This paper was submitted as a dissertation in partial fulfillment of the requirements for the degree of Doctor of Philosophy at the University of California. I wish to express my appreciation for the many helpful suggestions of Professor Alfred Tarski, under whose direction the thesis was written. I am particularly indebted for his assistance in preparing Section 4.

By saying for instance that addition of positive integers is arithmetically definable in terms of $\cdot$ and S, we mean that there is a formula ϕ with the following properties:

(i) ϕ is a formula of the elementary theory of positive integers with S and $\cdot$ as the only mathematical constants (thus ϕ contains only variables representing positive integers, the logical constants listed above and the mathematical constants S and $\cdot$).

(ii) ϕ contains three distinct free variables say x, y and z.[2]

(iii) ϕ is satisfied by those and only those ordered triples of integers $\langle x, y, z\rangle$ for which $x + y = z$.[3] A formula ϕ with this property may be referred to as a defining formula for $+$ in terms of $\cdot$ and S. As we shall see in Section 1 such a defining formula actually exists, in fact we can take for ϕ the formula

$$S(x\cdot z)\cdot S(y\cdot z) = S(z\cdot z\cdot S(x\cdot y)).$$

To give another example, the formula

$$\bigvee_{y} x = y + y \tag{1}$$

of the elementary theory of positive integers is satisfied by those and only those positive integers x which are even. Hence this formula shows that the notion of an even integer is arithmetically definable in terms of addition. Now consider the formula

$$\bigwedge_{\mathfrak{A}} ([2 \in \mathfrak{A} \wedge \bigwedge_{y} (y \in \mathfrak{A} \leftrightarrow y + 2 \in \mathfrak{A})] \rightarrow x \in \mathfrak{A}). \tag{2}$$

This formula differs from (1) in that besides variables representing positive integers, it also contains a bound variable representing sets of integers; and in addition to logical constants of the lower predicate calculus it also contains the symbol ϵ denoting the membership relation. On the other hand (2) like (1) contains only one free variable x and is satisfied by those and only those positve integers which are even. If we knew only (2) without knowing (1), we could just say that the notion of an even integer is recursively definable (or recursively arithmetically definable) in terms of addition.

In this example, the explicit arithmetical definition is the simplest and most natural one; in other cases, set-theoretical or in particular recursive definitions may be easy while an explicit arithmetical definition is either impossible or hard to find.

The problem of the axiomatic foundation of the discussion will be disregarded in Sections 1 and 3. Thus when stating that a formula is a theorem, we do not try to derive this formula from any axioms but merely to show that it is true in the intuitive sense and can be so recognized by mathematicians. It will be

---

[2] No attempt is made in this paper to present the metamathematical fragments of the discussion in a rigorous, formal way or to carry through a sharp distinction between metamathematical and mathematical notions. In particular, quotation marks are omitted in most cases since we believe no confusion will arise from this negligence.

[3] For a precise formal definition of the notion of satisfaction and truth, see Tarski [10].

seen that the question of axiomatization will play a rather restricted rôle even in the results established in Section 4.

1. Problems of definability in the arithmetic of integers. In developing the arithmetic of positive integers, we usually consider addition and multiplication as fundamental operations. It is known that a great variety of other arithmetical notions are (explicitly) arithmetically definable in terms of these operations. The problem arises whether one of these operations is definable in terms of the other. Consider first the problem of defining $\cdot$ in terms of $+$. It is obvious that $\cdot$ can be defined recursively in terms of $+$; we first define 1 as the positive integer which is not the sum of two positive integers and then use the familiar recursive definition of multiplication.

The situation changes if we are interested in the arithmetical definability of multiplication in terms of addition. From a result of Presburger [8], we can easily obtain a detailed description of all relations between integers and operations on integers which can be defined arithmetically in terms of $+$; and we do not find $\cdot$ among them. It is easily seen that $+$ is not definable in terms of $\cdot$ in any sense of the word definable. For the system of positive integers has automorphisms with respect to multiplication which permute the primes in an arbitrary way, so that sum is certainly not preserved. This method of proof is due to Padoa [7].

Among the notions which are arithmetically definable in terms of addition, we find the relation $<$ in terms of which the successor operation is arithmetically definable. Conversely, $+$ can be defined in terms of $<$ and $<$ in terms of S by means of recursive definitions. However by an argument exactly analogous to that referred to above to show that $\cdot$ is not arithmetically definable in terms of $+$, it can be shown that $+$ is not arithmetically definable in terms of $<$ and that $<$, hence also $+$, is not arithmetically definable in terms of S.[4]

We can now ask the question whether addition is arithmetically definable in terms of one of these weaker notions combined with multiplication. In this connection we obtain:

THEOREM 1.1. *Addition of positive integers is arithmetically definable in terms of multiplication and the successor operation as well as in terms of multiplication and the relation of less-than.*

Proof. It is easily seen that for any three positive integers, we have $a + b = c$ if and only if a, b, and c satisfy the following formula:

$$S(a\cdot c)\cdot S(b\cdot c) = S[(c\cdot c)\cdot S(a\cdot b)]. \tag{1}$$

To verify this, write formula (1) using ordinary mathematical notation:

$$(1 + ac)\,(1 + bc) = 1 + c^2\,(1 + ab).$$

Multiplying out and cancelling terms appearing on both sides of the equation, we have $(a + b)c = c^2$. Since c is a positive number, this is true if and only if $a + b = c$.

From this argument it follows at once that $+$ is arithmetically definable in

[4] This follows from the results discussed in Hilbert-Bernays [6], vol. I, pp. 234–264.

terms of $\cdot$ and S. We now notice that (1) can be given the following equivalent form:

$$\bigvee_{x,y,z} [S(a\cdot b) = x \wedge S(a\cdot c) = y \wedge S(b\cdot c) = z \wedge S([c\cdot c]\cdot x) = y\cdot z].$$

This clearly remains valid if we eliminate the symbol S by replacing each partial formula of the form

$$Su = v$$

by

$$u < v \wedge \bigwedge_{w} \sim(u < w \wedge w < v).$$

In this way, we see that $+$ is arithmetically definable in terms of $\cdot$ and $<$.

We can now try to improve the results obtained in Theorem 1.1 by replacing multiplication by weaker notions. In the first place, we have in mind the relation of divisibility. This relation is of course arithmetically definable in terms of multiplication while it seems very likely that $\cdot$ is not arithmetically definable in terms of $|$. It can be shown however that $\cdot$ can be defined set-theoretically in terms of $|$. As an improvement of Theorem 1.1, we now obtain:

THEOREM 1.2. *Addition and multiplication of positive integers are arithmetically definable in terms of the successor operation and the relation of divisibility.*

Proof. It is clearly sufficient to show that $\cdot$ is arithmetically definable in terms of $|$ and S. We shall express the fact that two integers a and b are relatively prime by $a \perp b$ and denote the least common multiple of two numbers a and b by $a\circ b$. Then the following equivalence holds in the arithmetic of positive integers:

$$(2)\qquad a\cdot b = c \leftrightarrow \bigwedge_{x} (a|x \wedge b|x \wedge c|x) \vee \bigwedge_{x,y,m} \{[a \perp x \wedge b \perp y \wedge c \perp x \wedge c \perp y \wedge x \perp y \wedge m|S(a\circ x) \wedge m|S(b\circ y)] \rightarrow \bigvee_{u} [m|u \wedge Su = c\circ(x\circ y)]\}.$$

Suppose first that $a\cdot b = c$ and that x, y and m satisfy the conditions

$$a \perp x \wedge b \perp y \wedge c \perp x \wedge c \perp y \wedge x \perp y \wedge m|S(a\circ x) \wedge m|S(b\circ y).$$

We must show that if a and b are not both 1, then

$$\bigvee_{u} [m|u \wedge Su = (a\cdot b)\circ(x\circ y)].$$

Now because of the conditions of relative primeness, we can replace the symbol $\circ$ by $\cdot$ throughout. Hence we must check that $m|(ax + 1)$ and $m|(by + 1)$ implies that $m|(abxy - 1)$. Writing this out in terms of congruences, we have $ax \equiv -1 \pmod m$ and $by \equiv -1 \pmod m$ implies $abxy \equiv +1 \pmod m$, which certainly holds.

Conversely, suppose the right side of (2) holds and show that $a\cdot b = c$. Notice first that $c = 1$ implies $a = b = 1$, for otherwise we may take x, y, and m all equal to 1 and obtain that there exists a u such that $Su = 1$, which is impossible.

Hence consider the case when c is different from 1. Let m be prime to a and b. Choose x and y prime to a, b, and c and to each other and such that

$$ax \equiv -1 \pmod{m},$$

$$by \equiv -1 \pmod{m}.$$

This is possible since x and y are only restricted to belonging to certain residue classes mod m which are prime to m. Now since $m|S(a\circ x)$ and $m|S(b\circ y)$ and the right side of (2) holds, it follows that there is a u satisfying $m|u \wedge Su = c\circ(x\circ y)$ or in terms of congruences $cxy \equiv +1 \pmod{m}$. Hence $c \equiv ab$ for arbitrarily large values of m and thus $c = ab$.

The relation $\perp$ and the operation $\circ$ are both arithmetically definable in terms of divisibility. In fact, the following equivalences can be used as definitions:

$$a \perp b \leftrightarrow \bigwedge_x (x|a \wedge x|b \rightarrow \bigwedge_y x|y)$$

and

$$c = a\circ b \leftrightarrow \bigwedge_x (a|x \wedge b|x \leftrightarrow c|x).$$

Hence we can eliminate the symbols $\perp$ and $\circ$ from (2) and obtain a defining formula for $\cdot$ in terms of S and $|$.

We might also try to improve Theorem 1.2 by replacing divisibility by the relation of relative primeness. However I have not been able to determine whether $\cdot$ is arithmetically definable in terms of $\perp$ and S or even in terms of $\perp$ and $+$.

It is easy to see that Theorem 1.1 can be extended to the arithmetic of arbitrary (not only positive) integers and furthermore to the arithmetic of arbitrary integral domains with unity, i.e., for every integral domain addition can be defined arithmetically in terms of multiplication and the successor operation S with $Sa = a + 1$.[5] The definition of $+$ in terms of $\cdot$ and S used in the proof of Theorem 1.1 can easily be modified in order to make it apply to arbitrary integers or to the elements of arbitrary integral domains.

On the other hand, I have been unable to extend Theorem 1.2 to arbitrary integers; the difficulty in this case reduces to that of defining the notion of a positive integer in terms of $|$ and S.

2. An axiomatic problem regarding the arithmetic of positive integers. Whenever addition and multiplication can be defined in terms of other notions of the arithmetic of positive integers, it is clearly possible to formulate an axiom system for arithmetic involving these other notions as the only primitive ones. This can be done in a mechanical way by simply eliminating $+$ and $\cdot$ from any of the familiar axiom systems involving only these two notions. The axioms thus obtained are usually complicated and artificial, and the problem of finding a simple and elegant axiom system of the kind desired may present considerable difficulty. We shall consider here only one problem of this kind.

[5] This improves an analogous result for the theory of abstract fields recently published by B. A. Bernstein [1].

We start here with the familiar axiom system due to Peano. It contains four primitive notions 1, S, $\cdot$, and $+$ and consists of the following axioms:

A1. $\bigwedge_a \sim Sa = 1$

A2. $\bigwedge_{a,b} (Sa = Sb \rightarrow a = b)$

A3. $(\mathfrak{P}(1) \wedge \bigwedge_a [\mathfrak{P}(a) \rightarrow \mathfrak{P}(Sa)]) \rightarrow \bigwedge_a \mathfrak{P}(a)$

A4. $\bigwedge_a a + 1 = Sa$

A5. $\bigwedge_{a,b} a + Sb = S(a + b)$

A6. $\bigwedge_a a \cdot 1 = a$

A7. $\bigwedge_{a,b} a \cdot Sb = (a \cdot b) + a.$

Here the induction principle A3 is an axiom-schema, that is an infinite system of axioms. It is understood that the symbol $\mathfrak{P}(a)$ may be replaced by any arithmetical formula containing just one free variable a, if suitable replacements of $\mathfrak{P}(1)$ and $\mathfrak{P}(Sa)$ are also made.[6]

We put the induction principle in this form if we decide to formalize the arithmetic of positive integers entirely within the lower predicate calculus. If on the other hand we want to use set theory in developing the arithmetic of positive integers, we replace the axiom-schema A3 by the following axiom:

A3′. $\bigwedge_{\mathfrak{A}} ([1 \in \mathfrak{A} \wedge \bigwedge_a (a \in \mathfrak{A} \rightarrow Sa \in \mathfrak{A})] \rightarrow \bigwedge_a a \in \mathfrak{A}).$

In such a case, we can also replace A4—A7 by explicit set-theoretical definitions of $+$ and $\cdot$.

By our Theorem 1.1, it follows that the symbol $+$ may be eliminated from Peano's axioms. This can be done mechanically by transforming A4, A5, and A7 with the help of the formula defining $+$ in terms of S and $\cdot$ in the proof of Theorem 1.1. We thus obtained the formulations:

A4′. $\bigwedge_a S(a \cdot Sa) \cdot S(1 \cdot Sa) = S([Sa \cdot Sa] \cdot Sa)$

A5′. $\bigwedge_{a,b,c} [S(a \cdot c) \cdot S(b \cdot c) = S[(c \cdot c) \cdot S(a \cdot b)] \rightarrow S(a \cdot Sc) \cdot S(Sb \cdot Sc) = S([Sc \cdot Sc] \cdot S(a \cdot Sb))]$

A7′. $\bigwedge_{a,b} S[(a \cdot b) \cdot (a \cdot Sb)] \cdot S[a \cdot (a \cdot Sb)] = S([(a \cdot Sb) \cdot (a \cdot Sb)] \cdot S[(a \cdot b) \cdot a]).$

[6] We could consider a more general axiom schema in which $\mathfrak{P}(a)$ could be replaced by any arithmetical formula containing in addition to a also other free variables b, c, $\cdots$ (in which case the whole schema would have to be preceded by the quantifiers $\bigwedge_{b,c,\ldots}$). It is shown in Hilbert-Bernays [6], vol. I, p. 343, that this more general form of the induction principle is actually no stronger than A3.

In view of the character of the defining formula which is used, we have to add one more axiom to guarantee the operational character of addition, i.e., the uniqueness of the result of addition. This new axiom is:

$$\text{A8.} \quad \bigwedge_{a,b,c,d} \{[S(a\cdot c)\cdot S(b\cdot c) = S([c\cdot c]\cdot S(a\cdot b)) \\ S(a\cdot d)\cdot S(b\cdot d) = S([d\cdot d]\cdot S(a\cdot b))] \rightarrow c = d\}.$$

A moment's reflection suffices to see that the axiom system consisting of A1 –A3, A4′, A5′, A6, A7′, and A8 is equivalent to the original axiom system (when supplemented by the definition of $+$ in terms of $\cdot$ and S) and is adequate for the development of the arithmetic of positive integers within the lower predicate calculus. We shall refer to this axiom system as System $\mathfrak{S}$; and shall use the symbol $\mathfrak{S}'$ to denote the axiom system obtained from $\mathfrak{S}$ by replacing A3 by A3′. We do not know whether the axioms of $\mathfrak{S}$ or $\mathfrak{S}'$ are mutually independent.

We now want to consider another simpler axiom system with the same mathematical constants as $\mathfrak{S}$ and which is also possibly an adequate basis for the development of the arithmetic of positive integers. This system consists of the old axioms A1, A2, A3, A6 and the following three new axioms:

$$\text{A4}''. \quad \bigwedge_{a,b} a\cdot b = b\cdot a$$

$$\text{A5}''. \quad \bigwedge_{a,b,c} a\cdot(b\cdot c) = (a\cdot b)\cdot c$$

$$\text{A7}''. \quad \bigwedge_{a,b} Sa\cdot S(a\cdot b) = S(a\cdot S(b\cdot Sa)).$$

A4″ and A5″ are of course well-known consequences of the Peano axioms. Axiom A7″ is unfamiliar, but expresses the simple identity

$$(1 + a)\,(1 + ab) = 1 + a\,(1 + b\,(1 + a)).$$

The new axiom system will be referred to as System $\mathfrak{T}$; and by $\mathfrak{T}'$ we shall denote the system obtained from $\mathfrak{T}$ by replacing A3 by A3′. We are interested in whether Systems $\mathfrak{S}$ and $\mathfrak{T}$ are equivalent (mutually derivable) and whether consequently $\mathfrak{T}$ can actually serve as a basis for the arithmetic of integers. The question can be answered affirmatively if we replace $\mathfrak{S}$ and $\mathfrak{T}$ by $\mathfrak{S}'$ and $\mathfrak{T}'$ and permit outselves to use set-theoretical devices in derivations. In fact, we have:

THEOREM 2.1. *Systems $\mathfrak{S}'$ and $\mathfrak{T}'$ are equivalent.*

Proof. The derivation of the axioms of $\mathfrak{T}'$ from those of $\mathfrak{S}'$ presents no difficulty. By defining addition in an appropriate way, we can easily derive from $\mathfrak{S}'$ all of Peano's axioms and hence we can obtain the axioms of $\mathfrak{T}'$ by means of the ordinary recursive procedure.

To derive the axioms of $\mathfrak{S}'$ from those of $\mathfrak{T}'$ we proceed in the following way. Since A1, A2, and A3′ (i.e., "proper" Peano axioms) are available in $\mathfrak{T}'$, we introduce ordinary addition and multiplication by means of the usual recursive definitions. Then we show by induction that the multiplication operation thus defined satisfies the remaining axioms of $\mathfrak{S}'$. The only thing that we do not yet know is whether this recursive multiplication coincides with the operation $\cdot$

of the axioms of $\mathfrak{T}'$. Hence the proof will be completed if we establish the following:

LEMMA. *The only binary operation* $\cdot$ *defined on the positive integers and satisfying the following formulas for all positive integers*

(i) $a \cdot 1 = a$

(ii) $a \cdot b = b \cdot a$

(iii) $a \cdot (b \cdot c) = (a \cdot b) \cdot c$

(iv) $Sa \cdot S(a \cdot b) = S(a \cdot S(b \cdot Sa))$

is ordinary multiplication.

Proof. Let $\times$ denote ordinary multiplication, that is multiplication introduced recursively. We need to show that for every a and b, $a \cdot b = a \times b$. We proceed by induction. Clearly $a \cdot 1 = 1 \cdot a = a = 1 \times a$. Suppose that it has been shown that $m \cdot n = m \times n$ for $m \leqq a$ and for all n. We need to show that $Sa \cdot n = Sa \times n$ for all n. Let $\mathfrak{N}$ be the set of all n such that $Sa \cdot n = Sa \times n$.

We show first that the inductive hypothesis together with (i)–(iv) implies that if $b \in \mathfrak{N}$ then $S(a \times b) \in \mathfrak{N}$. Using the inductive hypothesis, we have from (iv) that

$$Sa \cdot b = Sa \times b \rightarrow Sa \cdot S(a \times b) = S(a \times S(b \times Sa)).$$

But since $\times$ also satisfies (iv), we have

$$Sa \times S(a \times b) = S(a \times S(b \times Sa)).$$

Therefore,

$$Sa \cdot b = Sa \times b \rightarrow Sa \cdot S(a \times b) = Sa \times S(a \times b),$$

and if $b \in \mathfrak{N}$ then $S(a \times b) \in \mathfrak{N}$.

Next we shall show that if $m \leqq a$ and $b \in \mathfrak{N}$, then $m \times b \in \mathfrak{N}$. Suppose $Sa \cdot b = Sa \times b$, then

$$Sa \cdot (m \times b) = Sa \cdot (m \cdot b) = (Sa \cdot b) \cdot m = (Sa \times b) \times m = Sa \times (m \times b).$$

Hence if $b \in N$, $m \times b \in \mathfrak{N}$. Here we used (ii) and (iii) as well as the inductive hypothesis.

Also for $m \leqq a$, if $m \times b \in \mathfrak{N}$, then $b \in \mathfrak{N}$. Suppose $m \leqq a$ and $Sa \cdot (m \times b) = Sa \times (m \times b)$. Then

$$(Sa \cdot b) \times m = Sa \cdot b \cdot m = Sa \cdot (m \times b) = Sa \times (m \times b) = (Sa \times b) \times m.$$

Now using the cancellation law for ordinary multiplication we have $Sa \cdot b = Sa \times b$. Therefore if $m \leqq a$ and $m \times b \in \mathfrak{N}$ then $b \in \mathfrak{N}$.

We are now ready to show by induction in b that $b \in \mathfrak{N}$. Suppose that for all $b < n$, $b \in \mathfrak{N}$, and show that $n \in \mathfrak{N}$. It is sufficient to consider $n > 1$, since $Sa \cdot 1 = Sa \times 1 = Sa$ by (i).

CASE I. n and a relatively prime. Then there are r and s such that

$$S(a \times r) = n \times s \wedge r < n \wedge s \leqq a.$$

By the inductive hypothesis $r \in \mathfrak{N}$ since $r < n$. Hence $S(a \times r) \in \mathfrak{N}$, that is $n \times s \in \mathfrak{N}$. But $s \leqq a$, so $n \in \mathfrak{N}$.

CASE II. n and a have a common factor $k > 1$. Say $n = k \times t$ with $k \leqq a$ and $t < n$. Hence by the inductive hypothesis, $t \in \mathfrak{N}$, and since $k \leqq a$ this implies $k \times t \in \mathfrak{N}$. But $k \times t$ is just n, so $n \in \mathfrak{N}$.

We have just shown that $a \cdot b = a \times b$ for every a and b. In the proof, we have used various theorems from elementary number theory but these can all be derived from Peano's axioms. The proof of our lemma and hence also of Theorem 2.1 is thus complete.

We now return to the problem of equivalence of $\mathfrak{S}$ and $\mathfrak{T}$ on the basis of the lower predicate calculus. This problem seems to be more difficult and is still open. As in the proof of Theorem 2.1 we can easily deduce the axioms of $\mathfrak{T}$ from those of $\mathfrak{S}$. Going in the opposite direction, we can easily derive A4′ and A7′ from the axioms of $\mathfrak{T}$. However I have not been able to derive from $\mathfrak{T}$ either A5′ or A8. In fact, I have not even been able to show that either the cancellation law

$$\bigwedge_{a,b,c} (a \cdot c = b \cdot c \rightarrow a = b) \tag{1}$$

or all true equalities of the form

$$\alpha \cdot \beta = \gamma \tag{2}$$

where α, β, and γ stand for arbitrary constant terms of the form 1, $S1$, $SS1$, $\cdots$ are derivable from the axioms of Systems $\mathfrak{T}$. The only result which we know in this connection is that all equalities (2) become derivable if we enrich $\mathfrak{T}$ by including the cancellation law (1). This can be shown by analyzing the proof of Theorem 2.1, more specifically the lemma formulated there.

3. Problems of definability in the arithmetic of rationals. Given any statement of the arithmetic of rational numbers with $+$ and $\cdot$, an equivalent statement of integral arithmetic with the same fundamental operations can be found by replacing each rational variable by the ratio of two integer variables, clearing of fractions, and adjoining the condition that the denominators are not zero. It is much less simple to determine whether with every statement of the arithmetic of integers we can correlate an equivalent statement in the arithmetic of rationals and whether consequently the arithmetic of rationals is adequate to express all problems of elementary number theory.

The answer to this question is an affirmative one. To show this, it clearly suffices to prove that the notion of an integer is (explicitly) arithmetically definable in the arithmetic of rationals in terms of the operations $+$ and $\cdot$.

In establishing this result, we need not refrain from using any known theorem concerning integers or rationals since, as was stated in the introduction, we are disregarding here the problem of axiomatic foundations of our discussion. In order to make the argument more easily readable, we shall use in it besides the variables capital A, B, C, $\cdots$ representing arbitrary rationals also small a, b, c, $\cdots$ which are assumed to be integers.

THEOREM 3.1. (i) *For a rational number N to be an integer it is necessary and sufficient that it satisfy the following formula*

$$\bigwedge_{A,B}(\{(\bigvee_{X,Y,Z} 2 + BZ^2 = X^2 + AY^2) \wedge \bigwedge_{M}[(\bigvee_{X,Y,Z} 2 + ABM^2 + BZ^2 = X^2 + AY^2) \rightarrow (\bigvee_{X,Y,Z} 2 + AB(M+1)^2 + BZ^2 = X^2 + AY^2)]\} \rightarrow (\bigvee_{X,Y,Z} 2 + ABN^2 + BZ^2 = X^2 + AY^2)).$$

(ii) *Hence the notion of an integer and that of a positive integer is arithmetically definable in terms of the notion of a rational and the operations of addition and multiplication on rationals.*

Proof. (i) Let $\phi(A, B, K)$ stand for

$$\bigvee_{X,Y,Z} 2 + ABK^2 + BZ^2 = X^2 + AY^2.$$

Then we can rewrite the formula given in (i) as follows:

$$(1) \quad \bigwedge_{A,B}\{(\phi(A, B, 0) \wedge \bigwedge_{M}[\phi(A, B, M) \rightarrow \phi(A, B, M+1)]) \rightarrow \phi(A, B, N)\}.$$

It may be noticed that our formula is closely related to the formula

$$\bigwedge_{\mathfrak{A}}\{[0 \in \mathfrak{A} \wedge \bigwedge_{M}(M \in \mathfrak{A} \rightarrow M + 1 \in \mathfrak{A})] \rightarrow N \in \mathfrak{A}\},$$

which defines the notion of a non-negative integer set-theoretically.

We first show that any given integer N satisfies (1). In fact, suppose A and B satisfy the hypothesis of (1),

$$(2) \quad \phi(A, B, 0) \wedge \bigwedge_{M}[\phi(A, B, M) \rightarrow \phi(A, B, M+1)].$$

If now N is a positive integer, then by induction it satisfies the conclusion of (1), i.e., $\phi(A, B, N)$. On the other hand, since N occurs in $\phi(A, B, N)$ only to an even power, it is clear that

$$\phi(A, B, -N) \leftrightarrow \phi(A, B, N).$$

Thus if N is any integer and A and B satisfy (2), then $\phi(A, B, N)$ holds; in other words, N satisfies (1).

It is much harder to show that every rational number N which satisfies (1) is an integer. We shall need several lemmas. The first two are special cases of a general theorem of Hasse [5] which gives necessary and sufficient conditions for rational representation of a rational number by a given quadratic form in any number of variables.[7] The symbol (k/p) is the familiar Legendre symbol giving the quadratic character of $k \pmod p$.

LEMMA 1. *If p is a prime $\equiv 3 \pmod 4$ then $X^2 + Y^2 - pZ^2$ represents a non-zero rational number M, if and only if M is not of the form*

$$p \cdot k \cdot S^2 \quad \text{with } (k/p) = 1$$

$$\text{or} \quad k \cdot S^2 \quad \text{with } k \equiv p \pmod 8.$$

[7] A forthcoming book by Gordon Pall, ***The arithmetical theory of quadratic forms***, will give an elementary account of the theory.

LEMMA 2. *If p and q are odd primes with $p \equiv 1 \pmod 4$ and $(q/p) = -1$, then $X^2 + qY^2 - pZ^2$ represents a non-zero rational number M if and only if M is not of the form*

$$p \cdot k \cdot S^2 \quad \text{with } (k/p) = -1$$

$$\text{or} \quad q \cdot k \cdot S^2 \quad \text{with } (k/q) = -1.$$

LEMMA 3. *If p is a prime $\equiv 3 \pmod 4$ then*

$$2 + pM^2 + pZ^2 = X^2 + Y^2$$

has a solution for X, Y, and Z if and only if the denominator of M in lowest terms is odd and prime to p.

Proof. Let $M = n/d$ in lowest terms. Put $m = 2d^2 + pn^2$. It is sufficient to determine when m can be represented rationally by the form $X^2 + Y^2 - pZ^2$. Suppose that d is odd and prime to p. Then m is prime to p, so m is not of the form $p \cdot k \cdot S^2$. Also $m \equiv 1, 2 \pmod 4$, so it is not of the form $k \cdot S^2$ with $k \equiv p \pmod 8$ since $p \equiv 3 \pmod 4$. Hence by Lemma 1, m can be represented.

Suppose $p|d$ and put $d = p \cdot r$. Then $m = p \cdot k$ where $k = 2pr^2 + n^2$ is prime to p, since we assumed that n/d is in lowest terms, so $(k/p) = (n^2/p) = 1$. Thus, m is of the form $p \cdot k \cdot S^2$ with $(k/p) = 1$. Therefore by Lemma 1, m is not represented by $X^2 + Y^2 - pZ^2$.

Suppose $2|d$ and put $d = 2s$. Then $m = 8s^2 + pn^2$. But n is odd, so $m \equiv p \pmod 8$ and hence is not represented by the forms $X^2 + Y^2 - pZ^2$.

LEMMA 4. *If p and q are odd primes with $p \equiv 1 \pmod 4$ and such that $(q/p) = -1$, then*

$$2 + pqM^2 + pZ^2 = X^2 + qY^2$$

has a solution for X, Y, Z if and only if the denominator of M in lowest terms is prime to p and q.

Proof. Let $M = n/d$ in lowest terms and put $m = 2d^2 + pqn^2$. It is sufficient to check that m is represented by the form $X^2 + qY^2 - pZ^2$ if and only if d is prime to p and q.

Suppose that d is prime to p and q, then m is also prime to p and q. Hence by Lemma 2, m is represented by the form $X^2 + qY^2 - pZ^2$.

Suppose that $p|d$ and put $d = p \cdot r$, then $m = p \cdot k$ where $k = 2pr^2 + qn^2$. Since qn^2 is prime to p, the quadratic character $(k/p) = (qn^2/p) = (q/p) = -1$. Hence m is not represented by $X^2 + qY^2 - pZ^2$.

Similarly, suppose $q|d$ and put $d = q \cdot s$. Then $m = qk$ where $k = 2qr^2 + pn^2$ and $(k/q) = (pn^2/q) = (p/q) = (q/p) = -1$. Hence m is not represented by the given form.

LEMMA 5. *If p is a prime $\equiv 1 \pmod 4$, there is an odd prime q such that $(q/p) = -1$.*

Proof. Let s be any non-residue of p. Then either s or $s + p$ is odd and an odd non-residue of p must have an odd prime factor which is also a non-residue of p. Let this be q.

We are now ready to proceed with the proof of (i). We wish to show that if N satisfies (1), then N is an integer.

Consider first the case when $A = 1$ and $B = p$ where p is any prime $\equiv 3 \pmod 4$. Lemma 3 states that $\phi(1, p, M)$ if and only if the denominator of M in lowest terms is not divisible by 2 or p. Hence $A = 1$ and $B = p$ satisfy (2) since M and $M + 1$ have the same denominator and the denominator of 0 in lowest terms is ± 1. Therefore, if N satisfies (1), we must have $\phi(1, p, N)$. Hence the denominator of N is not divisible by 2 or p. But this holds for any prime $\equiv 3 \pmod 4$, hence the denominator of N is not divisible by 2 or by any prime $\equiv 3 \pmod 4$.

Next let p be any prime $\equiv 1 \pmod 4$. Choose q by Lemma 5 to be an odd prime such that $(q/p) = -1$. Then, Lemma 4 states that $\phi(q, p, M)$ if and only if the denominator of M in lowest terms is not divisible by p or q. Hence, as before, $A = q$ and $B = p$ satisfy the condition (2) so that if N satisfies (1) we must have $\phi(q, p, N)$. Hence the denominator of N in lowest terms is not divisible by any prime $\equiv 1 \pmod 4$.

Combining these results, we see that the denominator of N is not divisible by any prime, and therefore must be ± 1. Hence N is an integer.

(ii) From the formula stated in (i) we can easily eliminate the symbols 1 and 2 and replace X^2 by $X \cdot X$ (cf. the proof of the second part of Theorem 1.1). Hence the definability of integers in terms of the notion of a rational and the operations of addition and multiplication follows at once.

To extend this result to the notion of a positive integer it is sufficient to recall that the latter notion is definable in terms of that of an arbitrary integer and the operations $+$ and $\cdot$; in fact, using the symbolic expression $\mathrm{Int}(A)$ to express the fact that A is an arbitrary integer, the following formula holds if and only if A is a positive integer:

$$\mathrm{Int}(A) \wedge \sim A = 0 \wedge \bigvee_{X,Y,Z,W} A = X^2 + Y^2 + Z^2 + W^2.$$

Another defining formula with fewer quantifiers which may serve the same purpose was suggested by R. M. Robinson:

$$\mathrm{Int}(A) \wedge \sim A = 0 \wedge \bigvee_{X,Y} [\mathrm{Int}(X) \wedge \sim X = 0 \wedge (A = X^2 \vee X^2 = 1 + A Y^2)].$$

As an obvious consequence of Theorem 3.1, we obtain:

THEOREM 3.2. *Let n be any fixed positive integer and let R be an n-ary relation between rational numbers. Let R' be the relation which holds between $2n$ integers, $p_1, p_2, \cdots, p_n; q_1, \cdots, q_n$ if and only if $q_1 \neq 0, \cdots, q_n \neq 0$, and R holds between $p_1/q_1, \cdots, p_n/q_n$. Then R is arithmetically definable in terms of $+$ and $\cdot$ on rationals if (and only if) R' is arithmetically definable in terms of $+$ and $\cdot$ on integers.*

This consequence of our discussion is interesting because of a result of Gödel [4] which shows that the variety of relations between integers (and operations on integers) which are arithmetically definable in terms of addition and multiplication of integers is very great. For instance from Theorem 3.2 and Gödel's result, we can conclude that the relation which holds between three rationals A, B, and N if and only if N is a positive integer and $A = B^N$ is definable in the arithmetic of rationals.

4. Applications to the decision problem in arithmetic. From the results obtained in Sections 1 and 3 various consequences can be derived concerning the decision problem in the arithmetic of integers and rationals. In deriving these consequences, we make use of some unpublished results of Tarski and Mostowski. Hence we start with a brief account of these results.

The following remarks apply to mathematical theories which are assumed to be formalized within the lower predicate calculus (with identity and without variable predicates). We assume that in all these theories the same logical symbols, the same logical axioms and axiom-schemata, and the same rules of inference are used. Thus two such theories differ from each other only by the range of their variables, their specific mathematical constants (primitive symbols) and their specific mathematical axioms.

In each theory, we define in the usual way what we understand by a formula; in particular, all axioms turn out to be formulas and any application of rules of inference to given formulas yields a new formula. A formula which can be obtained from logical and mathematical axioms by applying rules of inference is referred to as a provable formula. A theory $\mathfrak{T}$ is called *consistent* if not every formula in it is provable; this amounts to saying that no two formulas one of which is the negation of the other are both provable.

A theory $\mathfrak{T}'$ is called an *extension* of the theory $\mathfrak{T}$ if every provable formula in $\mathfrak{T}$ is also provable in $\mathfrak{T}'$. A set of formulas is called *decidable* if a method exists which permits us in each particular case to decide in a finite number of steps if a given formula belongs to the set;[8] otherwise, it is called *undecidable*. A theory is decidable if the set of its provable formulas is decidable. A theory $\mathfrak{T}$ is said to be *essentially undecidable*[9] if it is consistent and if no consistent theory $\mathfrak{T}'$ which is an extension of $\mathfrak{T}$ is decidable.

As an example of the theories discussed, we may consider the arithmetic of positive integers with $+$ and $\cdot$ as the only mathematical constants; however, for our purpose it is convenient to introduce in this theory the symbol Pos to denote the notion of a positive integer. The mathematical axioms are essentially Peano's axioms listed in Section 2. We modify them slightly in order to eliminate the symbols S and 1; in formulating these axioms, we use the symbolic expression $\mathfrak{U}(c)$ (to mean $c = 1$) as an abbreviation of the formula

$$\mathrm{Pos}(c) \wedge \bigwedge_{x,y} [\mathrm{Pos}(x) \wedge \mathrm{Pos}(y) \rightarrow \sim(x + y = c)].$$

The resulting axioms are:

B1. $\bigvee_{c} \mathfrak{U}(c)$

B2. $\bigwedge_{a,b,c} ([\mathrm{Pos}(a) \wedge \mathrm{Pos}(b) \wedge \mathfrak{U}(c) \wedge a + c = b + c] \rightarrow a = b)$

B3. $\bigwedge_{a,b,c} \{[\mathrm{Pos}(a) \wedge \mathrm{Pos}(b) \wedge \mathfrak{U}(c)] \rightarrow a + (b + c) = (a + b) + c\}$

[8] Using more technical terminology, a set of formulas is decidable if the set of integers correlated with the formulas is general recursive.

[9] This notion was introduced by Tarski.

B4. $\bigwedge_{a,c} [\{\mathrm{Pos}(a) \wedge \mathfrak{U}(c)\} \rightarrow a \cdot c = a]$

B5. $\bigwedge_{a,b,c} \{[\mathrm{Pos}(a) \wedge \mathrm{Pos}(b) \wedge \mathfrak{U}(c)] \rightarrow a \cdot (b + c) = (a \cdot b) + a\}$

B6. $\bigwedge_{c} \{[\mathfrak{U}(c) \wedge \mathfrak{P}(c) \wedge \bigwedge_{a} ([\mathrm{Pos}(a) \wedge \mathfrak{P}(a)] \rightarrow \mathfrak{P}(a + c))] \rightarrow \bigwedge_{a} (\mathrm{Pos}(a) \rightarrow \mathfrak{P}(a))\}.$

We shall call the theory based on these axioms $\mathfrak{P}$. The same remarks that were made in Section 2 about A6 apply to the induction principle B6.

It was shown by Church [2] using essentially the method of Gödel [4] that the theory $\mathfrak{P}$ based upon the above axioms is undecidable. Rosser [9] showed that this theory is even essentially undecidable.

It is well known that the following formulas are provable in Theory $\mathfrak{P}$:

B7. $\bigwedge_{a,b,c} [(\mathrm{Pos}(a) \wedge \mathrm{Pos}(b) \wedge \mathrm{Pos}(c) \wedge a + c = b + c) \rightarrow a = b]$

B8. $\bigwedge_{a,b} [(\mathrm{Pos}(a) \wedge \mathrm{Pos}(b)) \rightarrow a + b = b + a]$

B9. $\bigwedge_{a,b,c} [(\mathrm{Pos}(a) \wedge \mathrm{Pos}(b) \wedge \mathrm{Pos}(c)) \rightarrow a + (b + c) = (a + b) + c]$

B10. $\bigwedge_{a,b} [(\mathrm{Pos}(a) \wedge \mathrm{Pos}(b) \wedge \sim a = b) \rightarrow \bigvee_{c} (\mathrm{Pos}(c) \wedge [a = b + c \vee b = a + c])]$

B11. $\bigwedge_{a,b,c} [(\mathrm{Pos}(a) \wedge \mathrm{Pos}(b) \wedge \mathrm{Pos}(c)) \rightarrow a \cdot (b + c) = (a \cdot b) + (a \cdot c)].$

It is also clear that if we replace B2, B3, and B5 by B7–B11 in the axiom system of the theory $\mathfrak{P}$ we obtain an equivalent axiom system. Hence the results of Church and Rosser previously mentioned apply equally well to the new axiom system. In this connection, however, Mostowski and Tarski have recently obtained a stronger result:

I. *The theory $\mathfrak{P}'$ with primitive mathematical terms* $+$, $\cdot$, *and* Pos *and with the mathematical axioms* B1, B4, B7–B11 *is essentially undecidable.*

The method of proof is similar to that used by earlier authors.

As is easily seen, an important difference between $\mathfrak{P}$ and $\mathfrak{P}'$ is that $\mathfrak{P}'$ does not have the induction principle and hence has only a finite number of mathematical axioms. In consequence, as we shall see, Theorem I has a much wider range of applications than the older results in this direction, i.e., it enables us to establish the undecidability of a much greater variety of mathematical theories.

The applications of Theorem I are based on the following general method developed by Tarski. Let $\mathfrak{T}_1$ be a theory (of the type considered) with the (specific) mathematical constants $O_1, \cdots, O_n$ and $\mathfrak{T}_2$ be another theory with the mathematical constants $Q_1, \cdots, Q_m$. We shall speak of a possible definition of one of the symbols O_i in terms of $Q_1, \cdots, Q_m$. To fix the idea, assume for example that O_i is the symbol for a binary operation. Then by a possible definition of O_i in terms of $Q_1, \cdots, Q_m$ we understand any equivalence of the form

$$\bigwedge_{a,b,c} [aO_ib = c \leftrightarrow \phi]$$

where ϕ stands for any formula containing only three free variables a, b, and c and containing no mathematical constants other than $Q_1, \cdots, Q_m$. We now say that Theory $\mathfrak{T}_1$ is *consistently interpretable* in Theory $\mathfrak{T}_2$ if there is a consistent theory $\mathfrak{T}$ satisfying the following conditions: (i) $\mathfrak{T}$ is an extension of both $\mathfrak{T}_1$ and $\mathfrak{T}_2$, i.e., both $O_1, \cdots, O_n$ and $Q_1, \cdots, Q_m$ are mathematical constants of $\mathfrak{T}$ and all axioms of both $\mathfrak{T}_1$ and $\mathfrak{T}_2$ are axioms (or at least provable formulas) of $\mathfrak{T}$. (ii) For each of the symbols O_i $(i = 1, \cdots, n)$ which does not occur in the sequence $Q_1, \cdots, Q_m$, there is an axiom (or provable formula) in $\mathfrak{T}$ which is a possible definition of O_i in terms $Q_1, \cdots, Q_m$.

Using this terminology Tarski stated the following general principle:

II. *If a theory $\mathfrak{T}_1$ has only a finite number of mathematical axioms and is essentially undecidable, then every theory $\mathfrak{T}_2$ in which $\mathfrak{T}_1$ is consistently interpretable is undecidable (although not necessarily essentially undecidable).*

By applying II to two theories $\mathfrak{T}_1$ and $\mathfrak{T}_2$ with the same mathematical constants, we obtain the following formulation:

III. *Let $\mathfrak{T}_1$ and $\mathfrak{T}_2$ be two theories with the same mathematical constants. If $\mathfrak{T}_1$ has only a finite number of mathematical axioms and is essentially undecidable, and if the theory $\mathfrak{T}$ which has the same mathematical constants as $\mathfrak{T}_1$ and $\mathfrak{T}_2$ and whose axiom system is the union of those of $\mathfrak{T}_1$ and $\mathfrak{T}_2$ is consistent, then $\mathfrak{T}_2$ is undecidable.*

From I–III various general results regarding the decision problem have been derived. Thus, I and III imply at once the following corollary:

IV. *Every theory $\mathfrak{T}$ with mathematical symbols* Pos, $+$, *and* $\cdot$ *is undecidable provided only that all the axioms of $\mathfrak{T}$ are true formulas of the arithmetic of positive integers; or at least that all the axioms of $\mathfrak{T}$ are compatible with those of Theory $\mathfrak{P}'$ of Theorem I (i.e., the theory based on the union of the two axiom systems is consistent).*

This result comprehends two particular cases which are known from the literature: the case when all true sentences are regarded as axioms of $\mathfrak{T}$; and the case when $\mathfrak{T}$ has no mathematical axioms at all, so that $\mathfrak{T}$ reduces to a purely logical theory whose undecidability amounts to the undecidability of the lower predicate calculus which was established by Church [3].

By using II instead of III, Theorem IV can be extended to the arithmetic of arbitrary integers. Since among the true formulas of the arithmetic of arbitrary integers involving $+$ and $\cdot$, we find those which serve as postulates defining the notion of an abstract ring, this result implies the following interesting corollary:

V. *The general (arithmetical) theory of abstract rings is undecidable.*

Finally, by means of I and II Tarski has established the undecidability of the general theories of lattices and groups.

New theorems in this domain can be obtained by combining I–III with the results of the earlier sections of this paper. In fact we obtain:

THEOREM 4.1. *Every theory $\mathfrak{T}$ whose mathematical constants are* Pos *(or* Int*), S, and $\cdot$ is undecidable provided only that the axioms are true formulas in the arithmetic of positive integers (or of arbitrary integers). The result (in its application*

to positive integers) remains valid if the multiplication symbol : *is replaced by the divisibility symbol* |.[10]

THEOREM 4.2. *Every theory* $\mathfrak{T}$ *whose mathematical constants are* Rt *(to denote the notion of a rational number),* $+$, *and* $\cdot$ *is undecidable provided only that the axioms of* $\mathfrak{T}$ *are true formulas in the arithmetic of rationals.*

The proofs of these two theorems are entirely analogous. We want to outline briefly the proof 4.2 in order to clarify the use of I–III.

Given the theories $\mathfrak{P}'$ of Theorem I and the theory $\mathfrak{T}$ satisfying the hypothesis of 4.2, we construct a new theory $\mathfrak{T}'$ in the following way. The mathematical constants of $\mathfrak{T}'$ are Rt, Pos, $+$, and $\cdot$. The axiom system of $\mathfrak{T}'$ consists: (i) of all axioms of $\mathfrak{P}'$ listed in I; (ii) of all axioms of $\mathfrak{T}$; and (iii) of an equivalence which is a possible definition of Pos in terms of Rt, $+$, and $\cdot$ and which results from Theorem 3.1. The theory $\mathfrak{T}'$ thus obtained is obviously consistent since all its axioms are true formulas in the arithmetic of rational numbers. Hence according to the definition of consistent interpretability, $\mathfrak{P}'$ is consistently interpretable in $\mathfrak{T}$; and therefore, by I and II, $\mathfrak{T}$ is undecidable.

It may be noticed that the symbol $+$ in 4.2 can be replaced by S; for the addition of rationals, like that of integers, is definable in terms of S and

Since among the formulas involving $+$ and $\cdot$ which are true in the arithmetic of rationals, we find those which are used as postulates to define the notion of an abstract field, we obtain as a particular case of 4.2:

THEOREM 4.3. *The general (arithmetical) theory of abstract fields is undecidable.*[11, 12]

It should be emphasized that the general theory of abstract fields is by no means essentially undecidable, for extensions of this theory are known which are decidable. In fact, as it was stated by Tarski [11], the arithmetical theory of real closed fields and that of algebraically closed fields (thus in particular the arithmetic of algebraic numbers, real algebraic numbers, real numbers, and that of complex numbers with $+$ and $\cdot$) are decidable. Hence many further problems are suggested which are still open.

In particular, we can ask whether the arithmetical theory of various algebraic extensions of the field of rational numbers are decidable. This applies to both finite and infinite extensions.

A specially interesting case, in view of its application to the decision problem for geometry, is that of the field of all constructible numbers, i.e., numbers which can be obtained from 1 by means of rational operations and extracting square roots.

We can also look for purely mathematical characterization of those fields

[10] The problem of the undecidability of the system of integers with multiplication and less-than was proposed by Mostowski.

[11] The decision problem for fields was proposed by Tarski.

[12] Using the results formulated in theorems 4.1–4.3, Tarski has recently shown that the general (arithmetical) theory of modular lattices and that of projective geometry are also undecidable. This improves his earlier result regarding the undecidability of the general lattice theory.

whose theory is decidable or undecidable. Regarding those fields with characteristic 0, parallel problems arise if, instead of fields whose theories are undecidable, we consider those in which the notion of an integer is arithmetically definable. We do not know at present whether these two series of problems are equivalent; if the notion of integer is arithmetically definable in a field then the arithmetical theory of this field is undecidable, but the problem of whether the converse holds (for fields of characteristic zero) is still open.

References

[1] Bernstein, B. A., *Weak definitions of a field*, **Duke mathematical journal**, vol. 14 (1947), pp. 475–482.

[2] Church, Alonzo, *An unsolvable problem of elementary number theory*, **American journal of mathematics**, vol. 58(1936), pp. 345–363.

[3] Church, Alonzo, *A note on the Entscheidungsproblem*, this Journal, vol. 1(1936), pp. 40–41, 101–102.

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

[5] Hasse, H., *Über die Darstellbarkeit von Zahlen durch quadratische Formen im Körper der rationalen Zahlen*, **Journal für die reine und angewandte Mathematik**, vol. 152 (1923), pp. 129–148.

[6] Hilbert, D., and Bernays, P., **Grundlagen der Mathematik.**

[7] Padoa, A., *Un nouveau système irréductible de postulats pour l'algèbre*, **Comptes rendus du 2-e Congrès International des Mathématiciens**, 1902, pp. 249–256.

[8] Presburger, M., *Über die Vollstandigkeit eines gewissen Systems der Arithmetik*, **Comptes rendus du I Congrés des Pays Slaves**, Warsaw 1929.

[9] Rosser, B., *Extensions of some theorems of Gödel and Church*, this Journal, vol. 1(1936), pp. 87–91.

[10] Tarski, A., *Der Wahrheitsbegriff in den formalisierten Sprachen*, **Studia philosophica**, vol. 1(1935), pp. 261–405.

[11] Tarski, A., *New investigations on the completeness of deductive theories* (abstract), this Journal, vol. 4(1939), p. 176. [Added in proof: A detailed account has since appeared in A. Tarski, ***A decision method for elementary algebra and geometry***, Project RAND, publication R-109, August 1948.]

UNIVERSITY OF CALIFORNIA