PROJECT RAND

A DECISION METHOD FOR ELEMENTARY ALGEBRA AND GEOMETRY

ALFRED TARSKI

Prepared for Publication by J. C. C. McKinsey

This report, although published by the RAND Corporation, was written while the Project was a part of Douglas Aircraft Co., Inc.

August 1, 1948

(Revised May, 1951)

R-109

The RAND Corporation
1700 MAIN ST. • SANTA MONICA • CALIFORNIA

Second Edition, 1957

CONTENTS

A DECISION METHOD FOR ELEMENTARY ALGEBRA AND GEOMETRY

INTRODUCTION

By a *decision method* for a class K of sentences (or other expressions) is meant a method by means of which, given any sentence θ, one can always decide in a finite number of steps whether θ is in K; by a *decision problem* for a class K we mean the problem of finding a decision method for K. A decision method must be like a recipe, which tells one what to do at each step so that no intelligence is required to follow it; and the method can be applied by anyone so long as he is able to read and follow directions.

The importance of the decision problem for the whole of mathematics (and for various special mathematical theories) was stressed by Hilbert, who considered this as the main task of a new field of mathematical research for which he suggested the term "metamathematics". The most important kind of decision problems is that in which K is defined to be the class of true sentences of a certain theory. When we say that there is a decision method for a certain theory, we mean that there is a decision method for the class of true sentences of the theory(1). (All superscripts in round brackets refer to Notes, pp. 47ff.)

Some decision methods have been known for a very long time. For example, Euclid's algorithm provides (among other things) a decision method for the class of all true sentences of the form "p and q are relatively prime," where p and q are integers (or polynomials with constant coefficients). And Sturm's theorem enables one to decide how many roots a given polynomial has and thus to decide on the truth of sentences of the form, "the polynomial p has exactly k roots."

Other decision methods are of more recent date. Löwenheim (1915) gave a decision method for the class of correct formulas of the lower predicate calculus involving only one variable. Post (1921) gave an exact proof of the validity of the familiar decision method (the so-called "truth-table method") for ordinary sentential calculus. Langford (1927) gave a decision method for an elementary theory of linear order. Presburger (1930) gave a decision method for the part of the arithmetic of integers which involves only the operation of addition. Tarski (1940) found a decision method for the elementary theory of Boolean algebra. McKinsey (1943) gave a decision method for the class of true universal sentences of elementary lattice theory. Mrs. Szmielew has recently found a decision method for the elementary theory of Abelian groups(2).

There are also some important negative results in this connection. From the fundamental results of Gödel (1930) and subsequent improvements of them obtained by Church (1936) and Rosser (1936), it follows that there does not exist a decision method for any theory to which belong all the sentences of elementary number theory (i.e., the arithmetic of integers with addition and multiplication) — and hence no decision method for the whole of mathematics is possible. A similar result has been obtained recently by Mrs. Robinson for theories to which belong all the sentences of the arithmetic of rationals. It is also known that there do not exist decision methods for various parts of modern algebra — in fact, for the elementary theory of rings (Mostowski and Tarski), the elementary theories of groups and lattices (Tarski), and the elementary theory of fields (Mrs. Robinson)[3].

In this monograph we present a method (found in 1930 but previously unpublished)[4] for deciding on the truth of sentences of the elementary algebra of real numbers — and hence also of elementary geometry.

By elementary algebra we understand that part of the general theory of real numbers in which one uses exclusively variables representing real numbers, constants denoting individual numbers, like "0" and "1", symbols denoting elementary operations on and elementary relations between real numbers, like "+", ".", "–", "<", ">", and "=", and expressions of elementary logic such as "and", "or", "not", "for some *x*", and "for all *x*". Among formulas of elementary algebra we find algebraic equations and inequalities; and by combining equations and inequalities by means of the logical expressions listed above, we obtain arbitrary sentences of elementary algebra. Thus, for example, the following are sentences of elementary algebra:

$0 > (1 + 1) + (1 + 1)$;

For every a, b, c, and d, where $a \neq 0$, there exists an x such that

$ax^3 + bx^2 + cx + d = 0$.

The first sentence is false, and the second is true.

On the other hand, in elementary algebra we do not use variables standing for arbitrary sets or sequences of real numbers, for arbitrary functions of real numbers, and the like. (When in this monograph we attach the qualifier "elementary" to the name of a theory, we refer to this abstention from the use of set-theoretical notions.) Hence those algebraic concepts whose definitions in terms of the fundamental notions listed above would require some set-theoretical devices cannot be represented in our system of elementary algebra. This applies, for instance, to the general notion of a polynomial, to the notion of solvability of an equation by means of radicals, and the like. For this reason it is not possible, for example, to consider as a sentence of elementary algebra the sentence:

Every polynomial has at least one root.

On the other hand, one can formulate in elementary algebra the sentences:

Every polynomial of degree 1 has a root;
Every polynomial of degree 2 has a root;
Every polynomial of degree 3 has a root;

and so on. Since we are dealing with real — not complex — algebra, the above sentences are true for odd degree but false for even degree.

It should be emphasized that the general notion of an integer (as well as that of a rational, or of an algebraic number) also belongs to those notions which cannot be represented in our system of elementary algebra — and this in spite of the fact that each individual integer can easily be represented (e.g., 2 as 1 + 1, 3 as 1 + 1 + 1, etc.)[5]. The variables in elementary algebra always stand for arbitrary real numbers and cannot be supposed to assume only integers as values. For such a supposition would imply that the class of all sentences of elementary algebra contains all sentences of elementary number theory; and, by results mentioned above, there could be no universal method for deciding on the truth of sentences of such a class. Thus, the following is not a sentence of elementary algebra:

> The equation
>
> $$x^3 + y^3 = z^3$$
>
> has no solution in positive integral x, y, z.

This gives, we hope, an adequate idea of what is understood here by a sentence of elementary algebra. Turning now to geometry, we can say roughly that by a sentence of elementary geometry we understand one which can be translated into a sentence of elementary algebra by fixing a coördinate system. It is well known that most sentences of elementary geometry in the traditional meaning are of this kind. There are, however, exceptions. These are, for instance, statements which involve explicitly or implicitly the general notion of a natural number: for instance, statements regarding polygons with an arbitrary number of sides — such as, that in every polygon each side is shorter than the sum of the remaining sides. It goes without saying that statements which involve the general notion of a point set — of an arbitrary geometrical figure — are also not elementary in our sense, but they would hardly be regarded as elementary in the everyday understanding of the term.

On the other hand, there are sentences which are elementary according to our definition but which are not ordinarily so considered. Most sentences of analytic geometry concerning algebraic curves of any definite degree belong here: for example, the theorem that any two ellipses intersect in at most four points.

It is important to realize that only the nature of the concepts involved, and not the character of the means of proof, determines whether a geometrical theorem is a sentence of elementary geometry. For instance, the statement that every angle can be divided into three congruent angles is an elementary sentence in our sense, and of course a true elementary sentence — despite the fact that the usual proofs of this statement make essential use of the axiom of continuity. On the other hand, the general notion of constructibility by rule and compass cannot be defined in elementary geometry, and therefore the statement that an angle in general cannot be trisected by by rule and compass is not an elementary sentence — although we can express in elementary gecmetry the facts that, say, an angle of 30° cannot be trisected by 1, 2,..., or in general any fixed number n of applications of rule and compass.

If we now compare the theories treated in this monograph (i.e., elementary algebra and geometry) with the other theories mentioned above for which decision methods have been found, we see at once that although the logical structure in both cases is indeed equally elementary, the theories investigated here have a considerably richer mathematical content. It would be possible to mention numerous problems which can be formulated in these theories, and which played in the past an important role in the development of mathematics. In the solution of these problems, and in general in the development of the theories considered, a great variety of modes of inference have been applied — some of them of a rather intricate nature (to mention only one example: the proof of the theorem that a triangle is isosceles if the bisectors of two of its angles are congruent). Thus the fact that there exists a universal decision method for elementary algebra and geometry could hardly have been regarded as a foregone conclusion.

In the light of these remarks one should not expect that the mathematical basis for the decision method to be discussed will be of a quite obvious and trivial nature. In fact by analyzing this decision method the reader will easily see that in its mathematical content it is very closely related to a classical algebraic result — namely, the theorem of Sturm previously mentioned — and it even provides an extension of this theorem to arbitrary systems of equations and inequalities in many unknowns.

Since a decision method, by its very nature, requires no intelligence for its application, it is clear that, whenever one can give a decision method for a class K of sentences, one can also devise a machine to decide whether an arbitrary sentence belongs to K. It often happens in mathematical research, both pure and applied, that problems arise as to the truth of complicated sentences of elementary algebra or geometry. The decision method presented in this work gives the mathematician the assurance that he will be able to solve every such problem by working at it long enough. Once the machine is devised, his task will reduce to explaining the problem to the machine — or to its operator. It may be instructive to illustrate, by means of an example, the more specific ways in which a decision machine could prove helpful in the study of unsolved problems.

As is well known, any two polygons of equal area, P and Q, can be decomposed into the same finite number n of non-overlapping triangles in such a way that each triangle in P is congruent to the corresponding triangle in Q. We are interested in determining the smallest number for which such a decomposition is possible. We assume in the following that P is the unit square and Q is a rectangle of unit area whose base has x units. Now the smallest number n depends exclusively on x and is denoted by $d(x)$; our problem reduces to describing the behavior of the function d for all positive values of x.

In particular, given any x_0, we can ask what the value of $d(x_0)$ is. In most cases, even the answer to this simple question presents difficulty; e.g., it is not easily seen whether or not $d(7/2) = 8$. However, we can easily establish, by means of a direct geometrical argument, an upper bound for $d(x_0)$; in fact, if $1 \leq x_0 \leq n$, where n is an integer, we have $d(x_0) \leq 2n$. Consequently, just one of the sentences "$d(x_0) = 1$", "$d(x_0) = 2$", ..., "$d(x_0) = 2n$" is true. If, moreover, x_0 is an algebraic number, all these sentences prove to be expressible in elementary geometry. Hence, by setting the machine in motion at most $2n$ times, we could check which of the sentences is true and thus find the value of $d(x_0)$.

In turn we may consider hypotheses regarding the behavior of the function d in some intervals. For instance, offhand, it seems plausible that $5 \leq d(x) \leq 6$ whenever

$2 < x \leq 3$. This hypothesis is still expressible in elementary geometry, and hence could be confirmed or rejected by means of a machine. The situation changes when we consider hypotheses of a more general character concerning the behavior of the function in its whole domain, e.g., the following one: for any real x and integral n, if $x > n$, then $d(x) > 2n$. This hypothesis has not yet been confirmed even for small values of n. In its general form, the hypothesis cannot be formulated in elementary geometry, and hence cannot be tested by means of the machine suggested here. However, the machine would permit us to test the hypothesis for any special value of n. We could carry out such tests for a sequence of consecutive values, $n = 2, 3, \ldots,$ up to, say, $n = 100$. If the result of at least one test were negative, the hypothesis would prove to be false; otherwise, our confidence in the hypothesis would increase, and we should feel encouraged to attempt establishing the hypothesis (by means of a normal mathematical proof), instead of trying to construct a counterexample.

As is seen from the last remarks, the machine envisaged may prove useful in connection with certain problems which cannot be formulated in elementary algebra (or geometry). The most typical in this class of problems are those of the form "Is it the case that, for every integer n, the condition C_n holds?" where C_n is expressible in elementary algebra for each fixed value of n. The machine could be used to solve mechanically this sort of problem for a series of consecutive values of n; in consequence, either we would learn that the solution of the problem in its general form is negative or else the plausibility of a positive solution would increase. Many important and difficult problems belong to this class, and the applicability of the machine to such problems may greatly enhance its value for mathematical research. (The results of this work have further implications, independent of the use of the machine, for the class of problems discussed; see Supplementary Note 7.)

It will be seen later, from the detailed description of the decision method, that the machine could serve some further purposes. We are often concerned, not with a sentence of elementary algebra, but with a condition involving parameters $a, b, c, \ldots,$ and formulated in terms of elementary algebra; the condition may be very involved, and we are interested in simplifying it — and, in fact, in reducing it to a standard form, in which it appears as a combination of algebraic equations and inequalities in $a, b, c, \ldots$. To give an example, consider the condition satisfied by the numbers a, b, and c if and only if there are exactly two (real) solutions of the equation:

$$ax^2 + bx + c = 0 .$$

In this case, the reduction is very simple and is well known from high-school algebra; the condition can be given the standard form:

$$a \neq 0 \text{ and } b^2 - 4ac > 0 .$$

The decision method developed below will give the assurance that such a reduction is always possible; and the decision machine would perform the reduction mechanically.

This monograph is divided into three sections. The first section contains a description of the system of algebra to which the decision method applies. In Section 2, the decision method itself is developed in a detailed way. In Section 3, some extensions of the results obtained as well as some related open problems are discussed. The notes at the end of the monograph contain, in addition to historical and bibliographical references, the discussion of various points of theoretical interest which are not directly related to the question of constructing a decision machine. A short bibliography following the notes lists the works which are referred to in the monograph[6].

SECTION 1.

THE SYSTEM OF ELEMENTARY ALGEBRA

In this section we want to describe a formal system of elementary algebra — and in particular to define in a precise way the class of sentences of this system[7].

By a *variable* we shall mean any one of the following symbols:

$$x,\ x_1,\ x_2, \ldots;\ y,\ y_1,\ y_2, \ldots;\ z,\ z_1,\ z_2, \ldots\ .$$

We suppose that there are infinitely many variables and that they are arranged in a sequence, so that we can speak of the variable occupying the 1st, 2nd,..., nth place in the sequence. These variables are to be thought of intuitively as ranging over the set of real numbers.

By an *algebraic constant* we shall mean one of the following three symbols:

$$1,\ 0,\ -1\ .$$

By an *algebraic operation-sign* we shall mean one of the following two symbols:

$$+,\ \cdot\ .$$

The first is called the *addition sign*, and the second the *multiplication sign*.

By an *algebraic term* we understand any meaningful expression built up from variables and algebraic constants by means of the elementary operation-signs. Thus, for example,

$$x, \qquad x_1 + y,\ -1\cdot x, \qquad \left[\left(x_1 \ \cdot\ -1\right)\cdot x_1\right] + x_2$$

are algebraic terms. But

$$x + , \qquad \sqrt{2}\ + x$$

are not algebraic terms: the first, because it is meaningless; the second, because it involves the sign " $\sqrt{2}$ ", which is neither a variable nor an algebraic constant (in the restricted meaning we have given to the latter term).

If one wants a precise definition of algebraic terms, they can be defined recursively as follows: An algebraic term of first order is simply a variable or one of the three algebraic constants. If α and β are algebraic terms of order at most k, and if the maximum of the orders of α and β is k, then $(\alpha\cdot\beta)$ and $(\alpha + \beta)$ are algebraic terms of order $k + 1$. An expression is called an algebraic term if, for some k, it is an algebraic term of order k.

According to the above definition, one should inclose in parentheses the results of performing operations on terms. Thus one should write, for example, always

$$(x + y) \text{ and } (x\cdot y)$$

instead of simply

$$x + y \text{ and } x \cdot y \ .$$

We shall often omit these parentheses, however, when no ambiguity will result from doing so; we shall use, in general, the ordinary conventions as to omitting parentheses in writing algebraic terms. Thus, we write

$$x + y \cdot z$$

instead of

$$[x + (y \cdot z)] \ .$$

It is convenient to introduce the operation of *subtraction* as follows[8]: if α and β are any terms, then we set

$$(\alpha - \beta) \equiv [\alpha + (-1 \cdot \beta)] \ .$$

We have used here the symbol "≡" to indicate that two formulas are identically the same — in the present case by definition. We shall use this symbol throughout the rest of this report. When we write

$$\alpha \equiv \beta$$

we mean that α and β are composed of exactly the same symbols, written in exactly the same order. Thus, for example, it is true that

$$0 \equiv 0 \ ,$$

and that

$$(0 = 1) \equiv (0 = 1) \ ,$$

but not that

$$(0 + 0) \equiv 0 \ ,$$

nor that

$$(0 = 1) \equiv (1 = 0) \ .$$

It is also convenient to introduce notation for sums and products of arbitrary finite length. Let $\alpha_1, \alpha_2, \ldots$ be a sequence of terms. Then we set

$$\sum_{i=1}^{1} \alpha_i \equiv \alpha_1$$

$$\sum_{i=1}^{k+1} \alpha_i \equiv \left(\sum_{i=1}^{k} \alpha_i + \alpha_{k+1} \right) ,$$

and similarly,

$$\prod_{i=1}^{1} \alpha_i \equiv \alpha_1$$

$$\prod_{i=1}^{k+1} \alpha_i \equiv \left(\prod_{i=1}^{k} \alpha_i \cdot \alpha_{k+1} \right) .$$

Instead of

$$\sum_{i=1}^{n} \alpha_i$$

we shall also sometimes use the notation

$$\alpha_1 + \alpha_2 +\ldots+ \alpha_n ,$$

or simply,

$$\alpha_1 +\ldots+ \alpha_n ;$$

and instead of

$$\prod_{i=1}^{n} \alpha_i ,$$

we shall sometimes write

$$\alpha_1 \cdot \alpha_2 \cdot \ldots \cdot \alpha_n$$

or

$$\alpha_1 \cdot \ldots \cdot \alpha_n .$$

If $\alpha_1,\ldots, \alpha_n$ are all the same, and equal, say, to α, then instead of

$$\prod_{i=1}^{n} \alpha_i$$

we sometimes write simply

$$\alpha^n .$$

Thus, for example,

$$\xi^3$$

has the same meaning as

$$[(\xi\cdot\xi)\cdot\xi] .$$

Moreover, we shall sometimes write α^0 for 1.

By an *algebraic relation-symbol* we shall mean one of the two symbols:

$$= , > ,$$

called, respectively, the *equality sign* and the *greater-than sign*[8].

By an *atomic formula* we shall mean an expression of one of the forms

$$(\alpha = \beta) , (\alpha > \beta)$$

where α and β stand for arbitrary algebraic terms; according to our previous remarks, parentheses will sometimes be omitted. The first kind of expression is called an *equality*, and the second an *inequality*. Thus, for example, the following are atomic formulas:

$$1 = 1 + 1$$

$$0 + x = x$$

$$x \cdot (y + z) = 0$$

$$[x \cdot (1 + 1)] + (y \cdot y) > 0$$

$$x > (y \cdot y) + x \ .$$

By a *sentential connective* we shall mean one of the following three symbols:

$$\sim , \wedge , \vee \ .$$

The first is called the *negation sign* (and is to be read "not"), the second is called the *conjunction sign* (and is to be read "and"), and the third is called the *disjunction sign* (and is to be read "or" — in the nonexclusive sense).

By the *(existential) quantifier* we understand the symbol "E". If ξ is any variable, then $(E\xi)$ is called a *quantifier expression*. The expression $(E\xi)$ is to be read "there exists a ξ such that ."

By a *formula* we shall mean an expression built up from atomic formulas by use of sentential connectives and quantifiers. Thus, for example, the following are formulas:

$$0 = 0$$

$$(Ex)(x = 0) \ ,$$

$$(x = 0) \vee (Ey)(x > y) \ ,$$

$$(Ex) \sim (Ey) \sim [(x = y) \vee (x > 1 + y)] \ ,$$

$$\sim (x > 1) \wedge (Ey)(x = y \cdot y) \ .$$

If one wants a precise definition of formulas, they can be defined recursively as follows: A formula of first order is simply an atomic formula. If θ is a formula of order k, then $\sim \theta$ is a formula of order $k + 1$. If θ is a formula of order k and ξ is any variable, then $(E\xi)\ \theta$ is a formula of order $k + 1$. If θ and Φ are formulas of order at most k, and one of them is of order k, then $(\theta \wedge \Phi)$ and $(\theta \vee \Phi)$ are formulas of order $k + 1$. An expression is a formula, if, for some n, it is a formula of order n.

Among the variables occuring in a formula, it is for some purposes convenient to distinguish the so-called "free" variables. We define this notion recursively in the following way: If Φ is an atomic formula, then ξ is *free* in Φ if and only if ξ occurs in Φ; ξ is *free* in $(E\eta)\ \theta$ if and only if η is not the same variable as

ξ, and ξ is free in θ; ξ is free in $\sim\theta$ if and only if ξ is free in θ; ξ is free in $(\theta \wedge \Phi)$, and in $(\theta \vee \Phi)$, if and only if ξ is free in at least one of the two formulas θ and Φ. Thus, for example, x is free in the formulas

$$x = 1$$

$$x = x$$

$$(Ey)(y = x)$$

$$(x = 1) \vee (Ex)(x = 2)$$

but not in the formulas

$$y = 1$$

$$(Ex)(x = x)$$

$$(Ex)(Ey)(y = x) \ .$$

(For certain purposes a more subtle notion is needed: that of a variable's being free, or not free, at a certain occurrence in a formula. Thus, for instance, in the formula

$$(Ey)(y = x) \wedge (Ex)[x + y = x \cdot w] \ ,$$

the variable x is free at its first occurrence — reading from left to right — but not in its other occurrences. This notion is not necessary for our discussion, however, so we shall not give a more exact explanation of it.)

It is convenient to introduce some abbreviated notation[8]. If θ and Φ are any formulas, then we regard

$$(\theta \longrightarrow \Phi)$$

as an abbreviation for

$$(\sim\theta \vee \Phi) \ ,$$

and

$$(\theta \longleftrightarrow \Phi)$$

as an abbreviation for

The sign $\longrightarrow$ is called the *implication sign*, and the sign $\longleftrightarrow$ is called the *equivalence sign*. If θ and Φ are any formulas, then the formula $\theta \longrightarrow \Phi$ is called an *implication*; we call θ the *antecedent* or *hypothesis* and Φ the *consequent* or *conclusion* of this implication.

If θ is any formula, and ξ is any variable, then

$$(A\xi)\theta$$

is an abbreviation for

$$\sim(E\xi)\sim\theta \ .$$

We also introduce notation to represent disjunctions and conjunctions of arbitrarily many formulas. In the simplest case the formulas in question are arranged in a finite sequence $\theta_1, \theta_2, \ldots, \theta_n$; we then denote the disjunction of the formulas by

$$\bigvee_{1 \leq i \leq n} \theta_i$$

or

$$\theta_1 \vee \theta_2 \vee \ldots \vee \theta_n$$

and their conjunction by

$$\bigwedge_{1 \leq i \leq n} \theta_i$$

or

$$\theta_1 \wedge \theta_2 \wedge \ldots \wedge \theta_n \, .$$

A recursive definition of these symbolic expressions hardly needs to be formulated explicitly here. Sometimes we are confronted with more involved cases: for instance, we may have a finite set S of ordered couples (n,p), a formula $\theta_{n,p}$ being correlated with each member (n,p) of S. To denote the disjunction and conjunction of all such formulas $\theta_{n,p}$ we use the symbolic expressions

$$\bigvee_{(n,p) \text{ in } S} \theta_{n,p}$$

and

$$\bigwedge_{(n,p) \text{ in } S} \theta_{n,p}$$

(where "(n,p) *in* S" may be replaced by formulas defining the set S). To ascribe to these symbolic expressions an unambiguous meaning we have of course to specify the order in which the formulas $\theta_{n,p}$ are taken in forming the disjunction or conjunction. The way in which this order is specified is immaterial for our purposes; we can, if we wish, specify once and for all that the formulas are taken in lexicographical order of their indices; thus, for instance, the symbolic expression

$$\bigvee_{\substack{n+p \leq 4 \\ 1 \leq n,p}} \theta_{n,p}$$

will denote the disjunction

$$\left(\left[\left\{\left[\left(\theta_{1,1} \vee \theta_{1,2}\right) \vee \theta_{1,3}\right] \vee \theta_{2,1}\right\} \vee \theta_{2,2}\right] \vee \theta_{3,1}\right).$$

Analogous notations are used for disjunctions and conjunctions of finite systems of formulas which are correlated, not with couples, but with triples, quadruples,..., or even arbitrary finite sequences, of integers.

We also need a symbolism to denote arbitrarily long sequences of quantifier expressions. For this purpose we shall use exclusively the "three-dot" notation:

$$\left(E\xi_1\right)\ldots\left(E\xi_n\right)\theta$$

and

$$\left(A\xi_1\right)\ldots\left(A\xi_n\right)\theta\ ,$$

where $\xi_1,\ldots,\ \xi_n$ are arbitrary variables, and θ is an arbitrary formula.

A formula is called a *sentence,* if it contains no free variables. Thus, for example, the following are sentences:

$$0 = 0$$

$$0 = 1$$

$$(0 = 0) \wedge (1 = 1)$$

$$(Ex)(0 = 0)$$

$$(Ex)(x = 0) \wedge (Ey) \sim (y = 0)$$

$$(Ex)(Ey)(y > x)\ .$$

On the other hand, the following are not sentences since they contain free variables:

$$x > 0$$

$$(Ey)(x > 0)$$

$$(Ex)\Big(x > \left[(x + 1) + (y\cdot y)\right]\Big).$$

It should be noticed that while a sentence is either true or false, this is not the case for a formula with free variables, which in general will be satisfied by some values of the free variables and not satisfied by others.

The notion of the truth of a sentence will play a fundamental role in our further discussion. It will occur either explicitly or, more often, implicitly; in fact, in terms of the notion of truth we shall define that of the equivalence of two formulas, and the latter notion will be involved in numerous theorems of Section 2, which are essential for establishing the decision method. We shall use the notion of truth intuitively, without defining it in a formal way. We hope, however, that the correctness of the theorems involving the notion of truth will be apparent to anyone who grasps the mathematical content of our arguments. No one will doubt, for instance, that a sentence of elementary algebra like

$$(Ax)(Ay)\left[(x + y) = (y + x)\right]$$

is true, and that the sentence

$$(Ax)(Ay)\left[(x - y) = (y - x)\right]$$

is false[9].

As examples of general laws involving the notion of truth, we give the following:

If θ is a sentence, then $\sim \theta$ is true if and only if θ is not true. If θ and Φ are sentences, then $(\theta \wedge \Phi)$ is true if and only if θ and Φ are both true. If θ and Φ are sentences, then $(\theta \vee \Phi)$ is true if and only if at least one of the sentences θ and Φ is true; $\theta \longrightarrow \Phi$ is true if and only if either θ is not true, or Φ is true; and $\theta \longleftrightarrow \Phi$ is true if and only if θ and Φ are either both true or both false.

Let θ and Φ be any formulas, and let ξ_1, $\xi_2, \ldots, \xi_n$ be the totality of free variables that occur in θ or Φ or both.

Then if the sentence

$$\left(A\xi_1\right)\ldots\left(A\xi_n\right)(\theta \longleftrightarrow \Phi)$$

is true, we say that θ and Φ are *equivalent*.

Thus, for example, the following two formulas are equivalent:

$$(x > 0) \vee (x = 0)\ , \quad (Ey)(x = y \cdot y)\ .$$

(Notice that neither of these formulas is equivalent to

$$(z > 0) \vee (z = 0)$$

since the latter contains "z" instead of "x".)

We now have some simple but very useful theorems regarding this notion of equivalence; they will be used in the subsequent discussion without explicit references.

A. *The relation of equivalence is symmetric, reflexive, and transitive.*

B. *Let θ_1 and θ_2 be equivalent formulas, and suppose that the formula Ψ_2 arises from the formula Ψ_1 by replacing θ_1 by θ_2 at one or more places. Then Ψ_1 is equivalent to Ψ_2.*

The proof of A and B presents no difficulty; in establishing B we apply induction with respect to the order of Ψ_1.

It is also convenient to define an equivalence relation for terms. Let α and β be any terms, and let ξ_1, $\xi_2, \ldots$, ξ_n be the variables which occur in α or β or both. Then if the sentence

$$\left(A\xi_1\right)\ldots\left(A\xi_n\right)(\alpha = \beta)$$

is true, we say that α and β are *equivalent*.

The fundamental theorems regarding the equivalence of terms are analogous to those concerning the equivalence of formulas. In fact we have:

C. *The relation of equivalence of terms is symmetric, reflexive, and transitive.*

D. *If α_1 and α_2 are equivalent terms, and if the term β_2 arises from the term β_1 by replacing α_1 by α_2 at one or more places, then β_1 is equivalent to β_2.*

E. *If α_1 and α_2 are equivalent terms, and if the formula Ψ_2 arises from the formula Ψ_1 by replacing α_1 by α_2 at one or more places, then Ψ_1 is equivalent to Ψ_2.*

SECTION 2.

DECISION METHOD FOR ELEMENTARY ALGEBRA

The decision method for elementary algebra which will be explained in this section can be properly characterized as the "method of eliminating quantifiers"[10],[11]. It falls naturally into two parts. The first, essential, part consists in a procedure by means of which, given any formula θ, one can always find in a mechanical way an equivalent formula which involves no quantifiers, and no free variables besides those already occurring in θ; in particular, this procedure enables us, given any sentence, to find an equivalent sentence without quantifiers. Mathematically, this part of the decision method coincides with the extension of Sturm's theorem mentioned in the Introduction. The second part consists in a procedure by means of which, given any sentence θ without quantifiers, one can always decide in a mechanical way whether θ is true. It is obvious that these two procedures together provide the desired decision method.

In order to establish the first half of the decision method, we proceed by induction on the order of a formula. As is easily seen (using the elementary properties of equivalence of formulas mentioned in Section 1) it suffices to describe a procedure by means of which, given a formula $(E\xi)\ \theta$, where θ contains no quantifiers, one can always find an equivalent formula Φ, without quantifiers, and such that every variable in Φ is free in $(E\xi)\ \theta$; i.e., to give a method of eliminating the quantifier from $(E\xi)\ \theta$. Actually, it turns out to be convenient to do slightly more: i.e., to give a method of eliminating the quantifier from $(\underset{k}{E}\xi)\ \theta$, where the prefix "$(\underset{k}{E}x)$" is to be read "there exist exactly k values of x such that."

DEFINITION 1. *Let* $\alpha_0, \alpha_1, \ldots, \alpha_n$ *be terms which do not involve* ξ. *Then the term*

$$\alpha_0 + \alpha_1 \cdot \xi + \ldots + \alpha_n \cdot \xi^n$$

is called a polynomial *in* ξ. *We say that the* degree *of this polynomial is n, and that* $\alpha_0, \ldots, \alpha_n$ *are its* coefficients: α_n *is called the* leading coefficient.

REMARK. Our definition of the degree of polynomials differs slightly from the one usually given in algebra, in that we do not require that the leading coefficient be different from zero. Thus, we call

$$1 + (1 + 1)\,x + (1 - 1)\,x^2$$

a polynomial of the second degree, not of the first degree.

DEFINITION 2. *Let* α *and* β *be polynomials in* ξ *of degrees m and n respectively: i.e., let*

$$\alpha \equiv \alpha_0 + \alpha_1 \cdot \xi + \ldots + \alpha_m \cdot \xi^m$$

$$\beta \equiv \beta_0 + \beta_1 \cdot \xi + \ldots + \beta_n \cdot \xi^n \ ,$$

where $\alpha_0, \ldots, \alpha_m$ *and* $\beta_0, \ldots, \beta_n$ *are terms which do not involve* ξ. *Let* r *be the minimum of the integers* m *and* n, *and let* s *be their maximum. Let*

$$\gamma_i \equiv \alpha_i + \beta_i \text{ for } i \leq r \ .$$

If $m < n$, *let*

$$\gamma_i \equiv \beta_i \text{ for } r < i \leq s \ .$$

If $m > n$, *let*

$$\gamma_i \equiv \alpha_i \text{ for } r < i \leq s \ .$$

Then we set

$$\alpha +_\xi \beta \equiv \gamma_0 + \gamma_1 \cdot \xi + \ldots + \gamma_s \cdot \xi^s \ .$$

DEFINITION 3. *Let*

$$\alpha \equiv \alpha_0 + \alpha_1 \cdot \xi + \ldots + \alpha_m \cdot \xi^m$$

be a polynomial in ξ. *Then by the* first reductum *(or, simply, the reductum) of* α *we mean the polynomial obtained by leaving off the term* $\alpha_m \cdot \xi^m$*: i.e., we set*

$$Rd_\xi(\alpha) \equiv \alpha_0 + \alpha_1 \cdot \xi + \ldots + \alpha_{m-1} \cdot \xi^{m-1} \ ;$$

if $m = 0$ *(so that* α *does not involve* ξ *at all) we set*

$$Rd_\xi(\alpha) \equiv 0 \ .$$

We define reducta of all orders recursively, by setting

$$Rd_\xi^0(\alpha) \equiv \alpha$$

$$Rd_\xi^{k+1}(\alpha) \equiv Rd_\xi\left[Rd_\xi^k(\alpha)\right] \ .$$

The following theorem is easily established by an induction on the degree of α.

THEOREM 4. *If* α *is a polynomial in* ξ, *then* $Rd_\xi(\alpha)$ *is also a polynomial in* ξ *(whose coefficients, of course, are the same as certain of the coefficients of* α — *and hence contain no variables except those occurring in the coefficients of* α*). If* α *is of a degree* $m > 0$, *then* $Rd_\xi(\alpha)$ *is of degree* $m - 1$.

We make use of Theorem 4 in defining recursively the product of two polynomials:

DEFINITION 5. *Let*

$$\alpha \equiv \alpha_0 + \alpha_1 \cdot \xi + \ldots + \alpha_m \cdot \xi^m$$

$$\beta \equiv \beta_0 + \beta_1 \cdot \xi + \ldots + \beta_n \cdot \xi^n$$

be polynomials in ξ of degrees m and n respectively. If $m = 0$, then we set

$$\alpha \cdot_\xi \beta \equiv \left(\alpha\cdot\beta_0\right) + \left(\alpha\cdot\beta_1\right)\xi + \ldots + \left(\alpha\cdot\beta_n\right)\xi^n \ .$$

If $m > 0$, let

$$\begin{aligned} \gamma_i &\equiv 0 \text{ for } i < m \\ \gamma_m &\equiv \alpha_m \cdot \beta_0 \\ \gamma_{m+1} &\equiv \alpha_m \cdot \beta_1 \\ &\vdots \\ \gamma_{m+n} &\equiv \alpha_m \cdot \beta_n \ , \end{aligned}$$

and we set

$$\alpha \cdot_\xi \beta \equiv \left[Rd_\xi(\alpha) \cdot_\xi \beta\right] +_\xi \left(\gamma_0 + \gamma_1 \cdot \xi + \ldots + \gamma_{m+n} \cdot \xi^{m+n}\right).$$

Definition 6. *If α and β are polynomials in ξ, then we set*

$$\alpha -_\xi \beta \equiv \alpha +_\xi \left[(-1) \cdot_\xi \beta\right] \ .$$

Theorem 7. *If α and β are polynomials in ξ, then $\alpha +_\xi \beta$, $\alpha \cdot_\xi \beta$, and $\alpha -_\xi \beta$ are polynomials in ξ.*

Proof. Obvious from the definitions.

Definition 8. *If $\alpha \equiv \xi$, then we set*

$$P_\xi(\alpha) \equiv 0 + 1 \cdot \xi \ .$$

If α is a constant (0, 1, or -1), or a variable different from ξ, then we set

$$P_\xi(\alpha) \equiv \alpha \ .$$

If α and β are arbitrary terms, then we set

$$\begin{aligned} P_\xi(\alpha + \beta) &\equiv P_\xi(\alpha) +_\xi P_\xi(\beta) \\ P_\xi(\alpha\cdot\beta) &\equiv P_\xi(\alpha) \cdot_\xi P_\xi(\beta) \ . \end{aligned}$$

Theorem 9. *If α is any term, and ξ is any variable, then $P_\xi(\alpha)$ is a polynomial in ξ, and is equivalent to α.*

Proof. By an induction on the order of α, making use of Theorem 7.

Remark. It will be seen that if α is any term, then $P_\xi(\alpha)$ is the polynomial which results from "multiplying out" and "arranging in increasing powers of ξ." It is convenient to extend the definition of P_ξ so that it will be defined not only for all terms but for all formulas without quantifiers. This is done in our next definition. The intuitive significance of $P_\xi(\theta)$, when θ is a formula, will become clear in Theorem 11.

Definition 10. *For all terms α and β, and for all formulas θ and Φ, we set*

(i) $P_\xi(\alpha = \beta) \equiv P_\xi(\alpha - \beta) = 0$

(ii) $P_\xi(\alpha > \beta) \equiv P_\xi(\alpha - \beta) > 0$

(iii) $P_\xi[\sim(\alpha = \beta)] \equiv [P_\xi(\alpha > \beta) \vee P_\xi(\beta > \alpha)]$

(iv) $P_\xi[\sim(\alpha > \beta)] \equiv [P_\xi(\alpha = \beta) \vee P_\xi(\beta > \alpha)]$

(v) $P_\xi(\theta \vee \Phi) \equiv [P_\xi(\theta) \vee P_\xi(\Phi)]$

(vi) $P_\xi(\theta \wedge \Phi) \equiv [P_\xi(\theta) \wedge P_\xi(\Phi)]$

(vii) $P_\xi[\sim(\theta \vee \Phi)] \equiv P_\xi(\sim\theta) \wedge P_\xi(\sim\Phi)$

(viii) $P_\xi[\sim(\theta \wedge \Phi)] \equiv P_\xi(\sim\theta) \vee P_\xi(\sim\Phi)$

(ix) $P_\xi(\sim\sim\theta) \equiv P_\xi(\theta)$.

Theorem 11. *Let θ be any formula without quantifiers, and let ξ be any variable. Then $P_\xi(\theta)$ is equivalent to θ. Moreover, $P_\xi(\theta)$ is a formula built up by means of conjunction and disjunction signs (but without using negation signs) from atomic formulas of the form*

$$\alpha = 0$$

and

$$\alpha > 0 ,$$

where α is a polynomial in ξ.

Proof. We prove that $P_\xi(\theta)$ is equivalent to θ by an induction on the order of θ. If θ is of first order, the theorem is obvious by 10 (i), 10 (ii), 9, and the following facts: $\alpha = \beta$ is equivalent to $\alpha - \beta = 0$; and $\alpha > \beta$ is equivalent to $\alpha - \beta > 0$. In order to carry out the recursive step, we make use of the facts: that $\sim(\alpha = \beta)$ is equivalent to $(\alpha > \beta) \vee (\beta > \alpha)$; that $\sim(\alpha > \beta)$ is equivalent to $(\alpha = \beta) \vee (\beta > \alpha)$; that $\sim(\theta \vee \Phi)$ is equivalent to $\sim\theta \wedge \sim\Phi$; that $\sim(\theta \wedge \Phi)$ is equivalent to $\sim\theta \vee \sim\Phi$; and that $\sim\sim\theta$ is equivalent to θ.

The second part of the theorem can also be proved by an induction on the order of θ, making use of Theorem 9.

Given any formula θ without quantifiers, we have thus obtained an equivalent formula $\Psi \equiv P_{\xi}(\theta)$ which contains no quantifiers and no negation signs. We are now going to define an operator Q which subjects any formula Ψ of this kind to further transformations by applying mainly the distributive law of sentential calculus, so as to bring Ψ to the so-called "disjunctive normal form."

Definition 12. *If Φ is an atomic formula, then we set*

$$Q(\Phi) \equiv \Phi \, .$$

If

$$Q(\Phi_1) \equiv \bigvee_{i \leq m} \; \bigwedge_{j \leq m_i} \Psi_{i,j} \; ,$$

and

$$Q(\Phi_2) \equiv \bigvee_{m < i \leq m+n} \; \bigwedge_{j \leq m_i} \Psi_{i,j}$$

where $\psi_{i,j}$ (for $i \leq m + n$ and $j \leq m_i$) *is an atomic formula, then we set*

$$Q(\Phi_1 \vee \Phi_2) \equiv \bigvee_{i \leq m+n} \; \bigwedge_{j \leq m_i} \Psi_{i,j}$$

and

$$Q(\Phi_1 \wedge \Phi_2) \equiv \bigvee_{\substack{i \leq m \\ m < j \leq m+n}} \left(\Psi_{i,1} \wedge \ldots \wedge \Psi_{i,m_i} \wedge \Psi_{j,1} \wedge \ldots \wedge \Psi_{j,m_j} \right) \, .$$

Theorem 13. *If Φ is any formula which involves no negation signs or quantifiers, then $Q(\Phi)$ is a disjunction of conjunctions of atomic formulas. Moreover, $Q(\Phi)$ is equivalent to Φ.*

Proof. By induction on the order of Φ, making use of the following fact: for any formulas Φ, θ, and Ψ, the formulas $\Phi \wedge (\theta \vee \Psi)$ and $(\Phi \wedge \theta) \vee (\Phi \wedge \Psi)$ are equivalent, as are also the formulas $\Phi \wedge (\theta \wedge \Psi)$ and $(\Phi \wedge \theta) \wedge \Psi$, as well as the formulas $\Phi \vee (\theta \vee \Psi)$ and $(\Phi \vee \theta) \vee \Psi$.

THEOREM 14. *Let Φ be any formula without quantifiers, and let ξ be any variable. Then $QP_{\xi}(\Phi)$ is a disjunction of conjunctions of atomic formulas — each of the atomic formulas in question having a polynomial in ξ for its left member and 0 for its right member. Moreover, $QP_{\xi}(\Phi)$ is equivalent to Φ.*

PROOF. By Theorems 11 and 13; $QP_{\xi}(\Phi)$ is of course used here to mean $Q[P_{\xi}(\Phi)]$.

We now introduce the notion of a derivative (with respect to a given variable).

DEFINITION 15. *If*

$$\alpha \equiv \alpha_0 + \alpha_1 \cdot \xi + \ldots + \alpha_n \cdot \xi^n$$

is a polynomial in ξ, of degree $n > 0$, then we put (writing "2" for "1 + 1", etc.)

$$D_{\xi}(\alpha) \equiv \alpha_1 + (2 \cdot \alpha_2) \cdot \xi + \ldots + (n \cdot \alpha_n) \xi^{n-1} .$$

If α is of degree zero in ξ, we set

$$D_{\xi}(\alpha) \equiv 0 .$$

REMARK. The notion of a derivative can of course be extended to arbitrary terms which are not formally polynomials in ξ according to Definition 1 by putting

$$D_{\xi}(\alpha) \equiv D_{\xi} P_{\xi}(\alpha) .$$

THEOREM 16. *If α is a polynomial in ξ, so is $D_{\xi}(\alpha)$.*

PROOF. By Definitions 1 and 15.

We also define derivatives of arbitrary order as follows:

DEFINITION 17. *If α is any term, and ξ is any variable, we set*

$$D_{\xi}^{0}(\alpha) \equiv \alpha$$

$$D_{\xi}^{k+1}(\alpha) \equiv D_{\xi}\left[D_{\xi}^{k}(\alpha)\right] .$$

THEOREM 18. *If α is a polynomial in ξ, and k is a non-negative integer, then $D_{\xi}^{k}(\alpha)$ is a polynomial in α.*

PROOF. By Theorem 16 and Definition 17.

The operator M which will be introduced next correlates, with every polynomial α, every variable ξ, and every non-negative integer n, a formula $M_{\xi}^{n}(\alpha)$, which in intuitive interpretation means that ξ is a root of α of order n. In case $n = 0$, this formula means simply that ξ is not a root of α. In this connection the formula $M_{\xi}^{n}(\alpha)$ will be read "the number ξ is of order n in the polynomial α," independent of whether n is positive or equal to zero.

Definition 19. *Let α be any polynomial in ξ. If n is any positive integer, we set*

$$M^n_\xi(\alpha) \equiv \left\{\left(\bigwedge_{1 \le i \le n} \left[D^{i-1}_\xi(\alpha) = 0\right]\right) \wedge \sim \left[D^n_\xi(\alpha) = 0\right]\right\}.$$

We set, in addition,

$$M^0_\xi(\alpha) \equiv \sim(\alpha = 0) \;.$$

We now introduce by definition a new kind of existential quantifier, which may be called the *numerical* existential quantifier. If n is any non-negative integer, ξ any variable, and Φ any formula, then $(\underset{n}{E}\xi)\Phi$ is to be interpreted intuitively as meaning that there exist exactly n values of ξ which make Φ true.

Definition 20. *Let ξ be any variable, and let Φ be any formula. We set*

$$(\underset{0}{E}\xi)\Phi \equiv (A\xi)\sim\Phi \;.$$

Let n be any positive integer, and let $\eta_1, \ldots, \eta_n$ be the first n variables (in the sequence of all variables) which do not occur in Φ and are different from ξ. Then we set

$$(\underset{n}{E}\xi)\Phi \equiv \left\{(E\eta_1)\ldots(E\eta_n)\left(\bigwedge_{1 \le i < j \le n} \sim(\eta_i = \eta_j) \wedge (A\xi)\left[\Phi \longleftrightarrow \bigvee_{1 \le i \le n} (\eta_i = \xi)\right]\right)\right\}.$$

We next introduce an operator F with a more complicated and technical interpretation. If n is an integer, ξ a variable, and α and β any polynomials, then $F^n_\xi(\alpha,\beta)$ is a formula to be intuitively interpreted as meaning that there are exactly n numbers ξ which satisfy the following conditions: (1) ξ is a root of higher order of α than of β, and the difference between these two orders is an odd integer; (2) there exists an open interval, whose right end-point is ξ, within which α and β have the same sign. The exact form of the symbolic expression used to define $F^n_\xi(\alpha,\beta)$ will probably seem strange at first glance even to those who are acquainted with logical symbolism; we have chosen this form so as to avoid the necessity of introducing a notation to indicate the result of replacing one variable by another in a given term. (An analogous remark applies to some other symbolic formulations given elsewhere in this work — in particular, in Note 9.) It will be noticed that the variable ξ is not free in $F_\xi^n(\alpha,\beta)$.

DEFINITION 21. *Let α be a polynomial of degree p in ξ, and let β be a polynomial of degree q in ξ. Let η_1 and η_2 be the first two variables which are different from ξ and which do not occur in α or β. Then we set*

$$F_\xi^n(\alpha,\ \beta) \equiv \underset{n}{(E\xi)} \left\{ \bigvee_{\substack{0 \leq k \leq q \\ 0 \leq 2m \leq p-k-1}} \left[M_\xi^{k+2m+1}(\alpha) \wedge M_\xi^k(\beta)\right] \wedge \right.$$

$$\left. (E\eta_1)(E\eta_2) \left[(\eta_1 = \xi) \wedge (\xi > \eta_2) \wedge (A\xi)\left\{\left[(\xi > \eta_2) \wedge (\eta_1 > \xi)\right] \longrightarrow (\alpha \cdot \beta > 0)\right\}\right] \right\}$$

The operator G which will now be defined is closely related to the operator F. In fact, α and β being polynomials in ξ, $G_\xi^n(\alpha,\beta)$ has the following meaning: if n_1 is the integer for which $F_\xi^{n_1}(\alpha,\beta)$ holds and n_2 is the integer for which $F_\xi^{n_2}(\alpha,\beta')$ holds (where β' is the negative of β — i.e., the polynomial obtained by multiplying β by -1), then $n = n_1 - n_2$; the integer n may be positive, zero, or negative. Remembering the intuitive meaning of $F_\xi^n(\alpha,\beta)$, the intuitive meaning of $G_\xi^n(\alpha,\beta)$ now becomes clear.

DEFINITION 22. *Let n be any integer (positive, negative, or zero), and let α and β be any polynomials in ξ. Let k be the maximum of the degrees of α and β. Then we set*

$$G_\xi^n(\alpha,\beta) \equiv \bigvee_{\substack{0 \leq m \leq k \\ 0 \leq m+n \leq k}} \left[F_\xi^{n+m}(\alpha,\beta) \wedge F_\xi^m(\alpha,(-1)\cdot_\xi\beta)\right] .$$

We need also the notion of the *remainder* obtained by dividing one polynomial by another. For our purposes, however, it turns out to be slightly more convenient to introduce a notation for the *negative of the remainder*.

DEFINITION 23. *Let ξ be a variable. Let α be a polynomial of degree m in ξ, whose leading coefficient is α_m. Let β be a polynomial of degree n in ξ, whose leading coefficient is β_n. If $m < n$, we set*

$$R_\xi(\alpha,\beta) \equiv (-1)\cdot_\xi\alpha .$$

If $m = n$, we set

$$R_\xi(\alpha,\beta) \equiv Rd_\xi P_\xi\left(\alpha_m\cdot\beta_n\cdot\beta - \beta_n^2\cdot\alpha\right) \quad .$$

If $m > n$, we set

$$R_\xi(\alpha,\beta) \equiv R_\xi\left\{ Rd_\xi P_\xi\left(\beta_n^2\cdot\alpha - \alpha_m\cdot\beta_n\cdot\xi^{m-n}\cdot\beta\right),\ \beta \right\} .$$

THEOREM 24. *If α and β are two polynomials in a variable ξ, then $R_\xi(\alpha,\beta)$ is again a polynomial in ξ whose coefficients contain no variables except those occurring in the coefficients of α and β. If β is a polynomial of degree $n > 0$, then $R_\xi(\alpha,\beta)$ is of degree less than n. If β is of degree zero, then $R_\xi(\alpha,\beta) \equiv 0$.*

It should be noticed that our definition of the negative of the remainder diverges somewhat from that which would normally be given in a textbook of algebra. According to the usual definition of the remainder, the negative of the remainder obtained by dividing a polynomial α of degree m by a polynomial β of degree n — both in the variable ξ — is a polynomial δ of a degree lower than n, such that, for some polynomial γ, the equation

$$\alpha = \beta\cdot\gamma - \delta$$

is satisfied identically. The coefficients of γ and δ can be obtained from those of α and β by means of the four rational operations, division included. We have modified this definition so as to eliminate division, which, as we know, is not available in our system. In consequence, we cannot construct for the negative remainder in our sense a polynomial γ which satisfies the above equation. We have instead:

THEOREM 25. *Let α and β be any polynomials in a variable ξ, of degrees m and n, respectively, and let β_n be the leading coefficient of β. We set $q = 0$ in case $m < n$, and $q = m - n + 1$ in case $m \geq n$. Then there is a polynomial γ in ξ, whose coefficients contain no variables except those occurring in the coefficients of α and β, and for which $\alpha\cdot\beta_n^{2q}$ and $\beta\cdot\gamma - R_\xi(\alpha,\beta)$ are equivalent.*

PROOF. By induction on the difference of the degrees of α and β.

One rather undesirable consequence of our modification of the notion of a negative remainder is that, in case the leading coefficient β_n of β is 0, all the coefficients of $R_\xi(\alpha,\beta)$ prove to be terms equivalent to 0. No difficulty will arise from this fact, however, since we shall never use $R_\xi(\alpha,\beta)$ except when conjoined with the hypothesis $\sim\left(\beta_n = 0\right)$.

It should be pointed out that our negative remainder $R_\xi(\alpha,\beta)$ is still a polynomial of lower degree than β — except when β is of degree zero, in which case $R_\xi(\alpha,\beta) \equiv 0$. This circumstance, together with the analogous property of the reductum of a polynomial (see Theorem 4) will be the basis for some recursive definitions given in our later discussion.

The following three definitions (26, 28, and 30) and the theorems which follow them (27, 29, and 31) are of crucial importance for the decision method under discussion. In these definitions we introduce three operators S, T, and U which correlate, with certain formulas Φ, new formulas $S(\Phi)$, $T(\Phi)$, and $U(\Phi)$ containing no quantifiers; and in the subsequent theorems we show that the correlated formulas are always equivalent to the original ones. The operator S is defined only for rather special formulas — in fact, for those of the form $G^k_\xi(\alpha,\beta)$. The operator T, which is constructed with the help of S, is defined for a rather extensive class of formulas, which contains formulas like

$$(\underset{k}{E}\xi)(\alpha = 0), \qquad (\underset{k}{E}\xi)[(\alpha = 0) \wedge (\beta > 0)]$$

(where α and β are any polynomials in ξ), and some related but more complicated types of formulas. The operator U, finally, constructed in terms of T, is defined for all possible formulas; hence Theorem 31, which establishes the equivalence of Φ and $U(\Phi)$, provides us with a universal method of eliminating quantifiers. It may be pointed out that the operator U, though constructed with the help of T, and thus indirectly of S, is not an extension of either of these operators; thus, if Φ is a formula for which S is defined, then $S(\Phi)$ and $U(\Phi)$ are in general formally different, though equivalent, formulas.

Definition 26. *Let k be an integer, and let α and β be polynomials in a variable ξ of degrees m and n respectively and having leading coefficients α_m and β_n; and let*

$$\Phi \equiv G^k_\xi(\alpha,\beta) \quad .$$

(i) *If α or β is the polynomial 0, we set*

$$S(\Phi) \equiv (0 = 0), \qquad \text{for } k = 0$$

and

$$S(\Phi) \equiv (0 = 1), \qquad \text{for } k \neq 0 \quad .$$

(ii) *If neither α nor β is the polynomial 0, and if $m + n$ is even, we set*

$$S(\Phi) \equiv \Big\{ \Big[\big(\alpha_m = 0\big) \wedge SG^k_\xi\big(Rd_\xi(\alpha),\beta\big)\Big] \vee \\ \Big[\big(\beta_n = 0\big) \wedge SG^k_\xi\big(\alpha, Rd_\xi(\beta)\big)\Big] \vee \Big[\sim\big(\alpha_m \cdot \beta_n = 0\big) \wedge SG^k_\xi\big(\beta, R_\xi(\alpha,\beta)\big)\Big] \Big\} \ .$$

(iii) *If neither α nor β is the polynomial 0, and $m + n$ is odd, we set*

$$S(\Phi) \equiv \Big\{ \Big[\big(\alpha_m = 0\big) \wedge SG^k_\xi\big(Rd_\xi(\alpha),\beta\big)\Big] \vee \Big[\big(\beta_n = 0\big) \wedge SG^k_\xi\big(\alpha, Rd_\xi(\beta)\big)\Big] \vee \\ \Big[\big(\alpha_m \cdot \beta_n > 0\big) \wedge SG^{k+1}_\xi\big(\beta, R_\xi(\alpha,\beta)\big)\Big] \vee \Big[\big(0 > \alpha_m \cdot \beta_n\big) \wedge SG^{k-1}_\xi\big(\beta, R_\xi(\alpha,\beta)\big)\Big] \Big\} .$$

Theorem 27. *Let Φ be one of the formulas for which the operator S is defined (by 26). Then $S(\Phi)$ is a formula which contains no quantifiers, and no variables except those that occur free in Φ. Moreover, Φ is equivalent to $S(\Phi)$.*

PROOF. The first part follows immediately from Definition 26.

To show the second part we consider the recursive definition for S given in 26. In view of this definition, we easily see that it suffices to establish what follows (for arbitrary polynomials α and β of degrees m and n respectively in a variable ξ, with leading coefficients α_m and β_n, and for an arbitrary integer k):

(1) if α or β is the polynomial 0, then $G^k_\xi(\alpha,\beta)$ is equivalent to $(0 = 0)$ for $k = 0$, and to $(0 = 1)$ for $k \neq 0$;

(2) if $m + n$ is even, then $G^k_\xi(\alpha,\beta)$ is equivalent to

$$\Big\{\Big[\big(\alpha_m = 0\big) \wedge G^k_\xi\big(Rd_\xi(\alpha),\beta\big)\Big] \vee \Big[\big(\beta_n = 0\big) \wedge G^k_\xi\big(\alpha, Rd_\xi(\beta)\big)\Big] \vee \Big[\sim\big(\alpha_m \cdot \beta_n = 0\big) \wedge G^k_\xi\big(\beta, R_\xi(\alpha,\beta)\big)\Big]\Big\};$$

(3) if $m + n$ is odd, then $G^k_\xi(\alpha,\beta)$ is equivalent to

$$\Big\{\Big[\big(\alpha_m = 0\big) \wedge G^k_\xi\big(Rd_\xi(\alpha),\beta\big)\Big] \vee \Big[\big(\beta_n = 0\big) \wedge G^k_\xi\big(\alpha, Rd_\xi(\beta)\big)\Big] \vee \Big[\big(\alpha_m \cdot \beta_n > 0\big) \wedge G^{k+1}_\xi\big(\beta, R_\xi(\alpha,\beta)\big)\Big] \vee \Big[\big(0 > \alpha_m \cdot \beta_n\big) \wedge G^{k-1}_\xi\big(\beta, R_\xi(\alpha,\beta)\big)\Big]\Big\}.$$

Let $\xi_1, \ldots, \xi_s$ be all the variables which occur in the coefficients of α or β or both.

It is easily seen that the proof of (1) reduces to showing that, in case $\alpha \equiv 0$ or $\beta \equiv 0$, the following sentences are true:

$$\big(A\xi_1\big) \ldots \big(A\xi_s\big) G^k_\xi(\alpha,\beta), \text{ for } k = 0;$$

$$\big(A\xi_1\big) \ldots \big(A\xi_s\big) \sim G^k_\xi(\alpha,\beta), \text{ for } k \neq 0.$$

Now, we notice by Definition 15 that, for every non-negative integer p, $D^p_\xi(0) \equiv 0$. Hence we conclude by Definition 19 that, in case $\alpha \equiv 0$ or $\beta \equiv 0$, the formula $F^k_\xi(\alpha,\beta)$ is satisfied by all values of $\xi_1, \ldots, \xi_s$ if $k = 0$, and by no such values if $k \neq 0$. From Definition 22 we then easily see that the same applies to the formula $G^k_\xi(\alpha,\beta)$; and this is just what we wanted to show.

Analogously, by means of easy transformations, we see that the proof of (2) and (3) reduces to showing that the following sentences are true:

$$(4)\quad (A\xi_1)\dots(A\xi_s)\left\{\sim\left(\alpha_m\cdot\beta_n = 0\right)\longrightarrow\left[G^k_\xi(\alpha,\beta)\longleftrightarrow G^k_\xi\left(\beta,R_\xi(\alpha,\beta)\right)\right]\right\}, \text{ for } m+n \text{ even;}$$

$$(5)\quad (A\xi_1)\dots(A\xi_s)\left\{\left(\alpha_m\cdot\beta_n > 0\right)\longrightarrow\left[G^k_\xi(\alpha,\beta)\longleftrightarrow G^{k+1}_\xi\left(\beta,R_\xi(\alpha,\beta)\right)\right]\right\}, \text{ for } m+n \text{ odd:}$$

$$(6)\quad (A\xi_1)\dots(A\xi_s)\left\{\left(0 > \alpha_m\cdot\beta_n\right)\longrightarrow\left[G^k_\xi(\alpha,\beta)\longleftrightarrow G^{k-1}_\xi\left(\beta,R_\xi(\alpha,\beta)\right)\right]\right\}, \text{ also for } m+n \text{ odd.}$$

Actually it turns out to be more convenient to establish, instead of (4), (5) and (6), certain stronger statements. For this purpose we introduce the formula $H^p_\xi(\alpha,\beta)$ expressing the fact that there are just p numbers ξ such that the difference between the order of ξ in α and the order of ξ in β is an odd integer, not necessarily positive. A precise formal definition of $H^p_\xi(\alpha,\beta)$ hardly needs to be given here. The sentences whose truth we want to establish can now be formulated as follows (letting γ and δ be arbitrary polynomials in ξ, whose coefficients involve no variables except $\xi_1, \dots, \xi_s$, and letting p and q be arbitrary non-negative integers):

$$(7)\quad (A\xi_1)\dots(A\xi_s)\left\{\left[H^p_\xi(\alpha,\beta)\wedge(A\xi)\left(\alpha\cdot\beta_n^{2q} = \beta\cdot\gamma - \delta\right)\wedge\sim\left(\alpha_m\cdot\beta_n = 0\right)\right]\longrightarrow\left[G^k_\xi(\alpha,\beta)\longleftrightarrow G^k_\xi(\beta,\delta)\right]\right\}, \text{ for } p \text{ even;}$$

$$(8)\quad (A\xi_1)\dots(A\xi_s)\left\{\left[H^p_\xi(\alpha,\beta)\wedge(A\xi)\left(\alpha\cdot\beta_n^{2q} = \beta\cdot\gamma - \delta\right)\wedge\left(\alpha_m\cdot\beta_n > 0\right)\right]\longrightarrow\left[G^k_\xi(\alpha,\beta)\longleftrightarrow G^{k+1}_\xi(\beta,\delta)\right]\right\}, \text{ for } p \text{ odd;}$$

$$(9)\quad (A\xi_1)\dots(A\xi_s)\left\{\left[H^p_\xi(\alpha,\beta)\wedge(A\xi)\left(\alpha\cdot\beta_n^{2q} = \beta\cdot\gamma - \delta\right)\wedge\left(0 > \alpha_m\cdot\beta_n\right)\right]\longrightarrow\left[G^k_\xi(\alpha,\beta)\longleftrightarrow G^{k-1}_\xi(\beta,\delta)\right]\right\}, \text{ also for } p \text{ odd.}$$

It is easily seen that the truth of (7), (8), and (9) implies that of (4), (5), and (6) respectively. We shall sketch the proof of this for the cases (7) and (4). Thus, assume (7) to be true and $m + n$ to be even. Consider any fixed but arbitrary set of values of $\xi_1, \dots, \xi_s$ and suppose the hypothesis of (4) to be satisfied. Let p be the (uniquely determined) integer for which $H^p_\xi(\alpha,\beta)$ is satisfied (by the given values of $\xi_1, \dots, \xi_s$). An elementary algebraic argument shows that p is congruent to $m + n$ modulo two; therefore p is even, and (7) may be applied. We now set $q = 0$ if $m < n$, and $q = m - n + 1$ otherwise; and we construct a polynomial γ in ξ, with coefficients involving no variables except those occurring in the coefficients of α or β, and such that

$$\alpha\cdot\beta_n^{2q} = \beta\cdot\gamma - R_\xi(\alpha,\beta)$$

holds for every value of ξ. (Regarding the possibility of constructing such a γ, see Theorem 25.) We then see that the hypothesis of (7) is satisfied with δ replaced by $R_\xi(\alpha,\beta)$. Hence the conclusion of (7) is also satisfied. This conclusion, however, with the indicated replacement, coincides with the conclusion of (4). The proof now reduces to establishing the truth of (7), (8), and (9). It is convenient in this part of proof to avail ourselves of customary mathematical language and symbolism. Also, we shall not be too meticulous in trying to avoid possible confusions between mathematical and metamathematical formulations.

Given a polynomial α and a number λ, we shall denote by $f(\lambda,\alpha)$ the order of λ in α: i.e., the uniquely determined non-negative integer r such that $M_{\lambda}^{r}(\alpha)$ holds. The function f is thus defined for every number λ, and for every polynomial α which does not vanish identically.

Similarly, for any given polynomials α and β in ξ we denote by $g(\alpha,\beta)$ the integer k for which $G_{\xi}^{k}(\alpha,\beta)$ holds. From the definition of $G_{\xi}^{k}(\alpha,\beta)$ (see Definition 22) it follows that such an integer always exists and is uniquely determined. It can be computed in the following way. We consider all these numbers λ for which $f(\lambda,\alpha) - f(\lambda,\beta)$ is positive and odd, and we divide them into two sets, P and N; λ belongs to P (or N) if there is an open interval whose right-hand end-point is λ, within which the values of α and β have always the same sign (or always different signs). Both sets P and N are clearly finite, and the difference between the number of elements in P and the number of elements in N is just $g(\alpha,\beta)$. Thus $g(\alpha,\beta)$ can be positive, negative, or zero; in case α or β vanishes identically, $g(\alpha,\beta) = 0$.

Finally we introduce the symbol $h(\alpha,\beta)$ to denote the integer p for which $H_{\xi}^{p}(\alpha,\beta)$ holds; in other words, $h(\alpha,\beta)$ is the number of all those numbers λ for which $f(\lambda,\alpha) - f(\lambda,\beta)$ is odd — though not necessarily positive.

For later use we state here without proof (which would be quite elementary) the following property of the function f defined above:

(10) Let α, β, γ, and δ be polynomials in ξ, such that

$$\alpha\cdot\beta_{n}^{2q} = \gamma\cdot\beta - \delta$$

holds for every value of ξ, β_{n} being the (nonvanishing) leading coefficient of β and q some integer. If, for any given number λ, $f(\lambda,\beta) > f(\lambda,\alpha)$ — so that α, as well as β, does not vanish identically — then $f(\lambda,\alpha) = f(\lambda,\delta)$ (so that δ does not vanish identically either). Similarly, if $f(\lambda,\beta) > f(\lambda,\delta)$, then $f(\lambda,\alpha) = f(\lambda,\delta)$.

We now take up the proof of (7), (8), and (9), which will be done by a simultaneous induction on $h(\alpha,\beta) = p$. The reader can easily verify that (7), (8), and (9) hold in case the polynomial δ vanishes identically; therefore we shall assume henceforth that δ does not vanish identically.

Assume first that $h(\alpha,\beta) = 0$. Thus there are no numbers λ such that $f(\lambda,\alpha) - f(\lambda,\beta)$ is odd. *A fortiori* there are no numbers λ such that $f(\lambda,\alpha) - f(\lambda,\beta)$ is positive and odd; and hence $g(\alpha,\beta) = 0$. Furthermore, there are no numbers λ such that $f(\lambda,\beta) - f(\lambda,\delta)$ is positive and odd; for if such a number λ existed, we should have $f(\lambda,\alpha) =$

$f(\lambda,\delta)$ by (10), and hence $f(\lambda,\alpha) - f(\lambda,\beta)$ would be odd. Consequently, $g(\beta,\delta) = 0$ and therefore $g(\alpha,\beta) = g(\beta,\delta)$. Thus in this case (7) proves to hold, while (8) and (9) are of course vacuously satisfied.

Assume now that (7), (8), and (9) have been established for arbitrary polynomials α and β with $h(\alpha,\beta) = p$ (p any given integer). Consider any polynomials α and β in ξ with nonvanishing coefficients α_m and β_n, and with

(11) $$h(\alpha,\beta) = p + 1 \ ,$$

as well as two further polynomials γ and δ in ξ such that

(12) $\alpha\cdot\beta_n^{2q} = \gamma\cdot\beta - \delta$ holds identically for some non-negative integer q .

Two cases can be distinguished here, according as $\alpha_m\cdot\beta_n > 0$ or $0 > \alpha_m\cdot\beta_n$; since the arguments are entirely analogous in both cases, however, we restrict ourselves to the case

(13) $$\alpha_m\cdot\beta_n > 0 \ .$$

Our assumption (11) implies that there are exactly $p + 1$ numbers λ for which $f(\lambda,\alpha) - f(\lambda,\beta)$ is odd. Let

(14) λ_0 = the largest λ such that $f(\lambda,\alpha) - f(\lambda,\beta)$ is odd.

Condition (13) implies that for sufficiently large numbers $\xi > \lambda_0$ the values of α and β are of the same sign. This can be extended to every number $\xi > \lambda_0$ (not a root of α or β), since, by (14), there is no number $\xi > \lambda_0$ for which $f(\xi,\alpha) - f(\xi,\beta)$ is odd (and therefore at which one of the polynomials α and β changes sign while the other does not). Hence, and from the fact that $f(\lambda_0,\alpha) - f(\lambda_0,\beta)$ is odd, we conclude:

(15) There is an open interval whose right-hand end-point is λ_0, within which the values of α and β are everywhere of different signs.

We now introduce three new polynomials α', γ', and δ' by stipulating that the equations

(16) $$\alpha' = \alpha\cdot(\lambda_0 - \xi), \qquad \gamma' = \gamma\cdot(\lambda_0 - \xi), \qquad \delta' = \delta\cdot(\lambda_0 - \xi)$$

hold identically. By (12), (13), and (16) we obviously have:

(17) $\alpha'\cdot\beta_n^{2q} = \gamma'\cdot\beta - \delta'$ holds identically for some non-negative integer q ;

(18) $\alpha'_{m+1}\cdot\beta_n < 0$, where α'_{m+1} is the leading coefficient of α' ;

(19) $f(\lambda_0,\alpha') = f(\lambda_0,\alpha) + 1$, and also $f(\lambda_0,\delta') = f(\lambda_0,\delta) + 1$ (since δ and δ' do not vanish identically);

(20) $f(\xi,\alpha') = f(\xi,\alpha)$ for every $\xi \neq \lambda_0$, and similarly $f(\xi,\delta') = f(\xi,\delta)$ for every $\xi \neq \lambda_0$ (since δ and δ' do not vanish identically).

From (19) and (20) we conclude that the set of numbers λ such that $f(\lambda,\alpha') - f(\lambda,\beta)$ is odd differs from the analogous set for α and β only by the absence of λ_0; thus, using also (11),

$$h(\alpha',\beta) = h(\alpha\ ,\beta) - 1 = p\ .$$

Consequently, our inductive premise applies to the polynomials α' and β: i.e., sentences (7), (8), and (9) are true if α is replaced by α'. Remembering the meaning of $g(\alpha,\beta)$, and taking account of (17) and (18), we conclude:

(21) $$g(\alpha',\beta) = g(\beta,\delta') \text{ in case } p \text{ is even;}$$

(22) $$g(\alpha',\beta) = g(\beta,\delta') + 1 \text{ in case } p \text{ is odd.}$$

We now want to show that

(23) $$g(\alpha,\beta) - g(\beta,\delta) = g(\alpha',\beta) - g(\beta,\delta') - 1\ .$$

To do this, we first notice that by (16):

(24) The values of α and α' are of the same sign for every $\xi < \lambda_0$ (not a root of α); similarly for the values of δ and δ'.

We also observe that:

(25) There is no $\xi > \lambda_0$ such that $f(\xi,\beta) - f(\xi,\delta)$ is positive and odd; similarly for β and δ'.

For, if $f(\xi,\beta) - f(\xi,\delta)$ were positive and odd for some $\xi > \lambda_0$, then, by (10) and (12), $f(\xi,\alpha) - f(\xi,\beta)$ would be odd for the same $\xi > \lambda_0$, and this would contradict (14). The argument for β and δ'. is analogous; instead of (12) we use (17), and when stating the final contradiction we refer to (14) combined with the first part of (20), instead of merely to (14).

We now distinguish two cases, dependent on the sign of $f(\lambda_0,\alpha) - f(\lambda_0,\beta)$. In view of (20), (24), and (25), the only number which can cause a difference in the values of $g(\alpha,\beta)$ and $g(\alpha',\beta)$, or in the values of $g(\beta,\delta)$ and $g(\beta,\delta')$, is the number λ_0. If now

(A) $$f\big(\lambda_0,\alpha\big) - f\big(\lambda_0,\beta\big) > 0\ ,$$

then by (14) and (15) the number λ_0 effects a decrease of $g(\alpha,\beta)$ by 1; while, as a result of (19), it has no effect on the value of $g(\alpha',\beta)$. Hence

(26) $$g(\alpha,\beta) = g(\alpha',\beta) - 1\ .$$

Furthermore, in the case (A) considered, $f(\lambda_0,\beta) - f(\lambda_0,\delta)$ cannot be positive by (10); and therefore $f(\lambda_0,\beta) - f(\lambda_0,\delta')$ cannot *a fortiori* be positive by (19). Thus in this case the number λ_0 proves to have no effect on the values of $g(\beta,\delta)$ and $g(\beta,\delta')$; and consequently

$$(27) \qquad g(\beta,\delta) = g(\beta,\delta') \ .$$

Equations (26) and (27) at once imply (23).

Turning to the case

$$(\text{B}) \qquad f(\lambda_0,\alpha) - f(\lambda_0,\beta) < 0 \ ,$$

we first notice that under this assumption λ_0 does not affect the value of $g(\alpha,\beta)$. Nor does it affect the value of $g(\alpha',\beta)$, since, by (14) and (19), $f(\lambda_0,\alpha') - f(\lambda_0,\beta)$ is even. Therefore,

$$(28) \qquad g(\alpha,\beta) = g(\alpha',\beta) \ .$$

Moreover, in the case (B) under consideration, we see from (10) that $f(\lambda_0,\alpha) = f(\lambda_0,\delta)$, and hence, using (14), that

$$(29) \qquad f(\lambda_0,\beta) - f(\lambda_0,\delta) \text{ is positive and odd.}$$

Let

$$f(\lambda_0,\alpha) = f(\lambda_0,\delta) = r \ .$$

Thus λ_0 is of order r in α and δ, and of a higher order in β. Consequently there are three polynomials α'', β'', and δ'' such that the equations

$$(30) \qquad \alpha = \alpha''\cdot(\lambda_0-\xi)^r, \qquad \beta = \beta''\cdot(\lambda_0-\xi)^r, \qquad \delta = \delta''\cdot(\lambda_0-\xi)^r$$

hold identically; λ_0 is a root of β'', but not of α'' or δ''. We obtain from (12) and (30):

$$\alpha''\cdot\beta_n^{2q} = \gamma\cdot\beta'' - \delta'' \ .$$

Consequently, the values of α'' and δ'', for $\xi = \lambda_0$, have different signs. Therefore there is an open interval, whose right-hand end-point is λ_0, within which the values of α'' and δ'' have different signs; and, by (30), this applies also to α and δ. By comparing this result with (15), we conclude that there is an open interval whose right-hand end-point is λ_0, within which the values of β and δ have the same sign. Hence, and by (29), λ_0 contributes to the increase of $g(\beta,\delta)$ by 1. On the other hand, by (19) and (29), $f(\lambda_0,\beta) - f(\lambda_0,\delta')$ is even, so that λ_0 has no effect on the value of $g(\beta,\delta')$. Thus, finally,

$$(31) \qquad g(\beta,\delta) = g(\beta,\delta') + 1 \ .$$

Equations (28) and (31) again imply (23). Hence (23) holds in both the cases (A) and (B).

From (21), (22), and (23) we obtain at once:

$$g(\alpha,\beta) = g(\beta,\delta) \text{ in case } p + 1 \text{ is even ;}$$

$$g(\alpha\ \beta) = g(\beta,\delta) - 1 \text{ in case } p + 1 \text{ is odd .}$$

Thus we have shown that (7), (8), and (9) hold for polynomials α and β with $h(\alpha,\beta) = p + 1$; and hence by induction they hold for arbitrary polynomials α and β. This completes the proof.

DEFINITION 28. *Let*

$$\begin{aligned} \alpha &\equiv \alpha_0 + \alpha_1\xi + \ldots + \alpha_m\xi^m \\ \beta &\equiv \beta_0 + \beta_1\xi + \ldots + \beta_n\xi^n \\ \gamma_1 &\equiv \gamma_{1,0} + \gamma_{1,1}\xi + \ldots + \gamma_{1,n_1}\xi^{n_1} \\ &\ \vdots \\ \gamma_r &\equiv \gamma_{r,0} + \gamma_{r,1}\xi + \ldots + \gamma_{r,n_r}\xi^{n_r} \end{aligned}$$

be arbitrary polynomials in ξ. We define the function T as follows:

(i) *If Φ is a formula of the form*

$$(\underset{k}{E}\xi)\,[\alpha = 0]\ ,$$

then we set

$$T(\Phi) \equiv \left[\sim\left(\alpha_0 = 0\right) \vee \ldots \vee \sim\left(\alpha_m = 0\right)\right] \wedge SG_\xi^{-k}\left(\alpha, D_\xi(\alpha)\right)\ .$$

(ii) *If Φ is a formula of the form*

$$\left[\sim\left(\alpha_0 = 0\right) \vee \ldots \vee \sim\left(\alpha_m = 0\right)\right] \wedge (\underset{k}{E}\xi)\left[(\alpha = 0) \wedge (\beta > 0)\right]\ ,$$

then we set

$$T(\Phi) \equiv \left\{ \left[\sim\left(\alpha_0 = 0\right) \vee \ldots \vee \sim\left(\alpha_m = 0\right)\ \right] \wedge \bigvee_{\substack{2k = r_1 - r_2 + r_3 \\ 0 \leq r_1,\, r_2 \leq m \\ -m \leq r_3 \leq m}} \left(SG_\xi^{-r_1}\left[\alpha, D_\xi(\alpha)\right] \wedge SG_\xi^{-r_2}\left[P_\xi(\alpha^2 + \beta^2), D_\xi P_\xi(\alpha^2 + \beta^2)\right] \wedge SG_\xi^{-r_3}\left[\alpha, D_\xi(\alpha) \cdot_\xi \beta\right]\right) \right\}\ .$$

(iii) *If Φ is a formula of the form*

$$\left[\sim\left(\alpha_0 = 0\right) \vee \ldots \vee \sim\left(\alpha_m = 0\right)\right] \wedge (\underset{k}{E}\xi)\left[(\alpha = 0) \wedge \left(\gamma_1 > 0\right) \wedge \ldots \wedge \left(\gamma_r > 0\right)\right]\ ,$$

where $r \geq 2$, *then we set*

$$T(\Phi) \equiv \bigvee_{\substack{2k = r_1 + r_2 - r_3 \\ 0 \leq r_1, r_2, r_3 \leq m}} \left\{ T\left(\Phi_1\right) \wedge T\left(\Phi_2\right) \wedge T\left(\Phi_3\right) \right\} ,$$

where

$$\Phi_1 \equiv \left\{ \left[\sim \left(\alpha_0 = 0\right) \vee \ldots \vee \sim \left(\alpha_m = 0\right) \right] \wedge \right.$$
$$\left. \underset{r_1}{(E\xi)} \left[\left(\alpha = 0\right) \wedge \left(\gamma_1 > 0\right) \wedge \ldots \wedge \left(\gamma_{r-2} > 0\right) \wedge P_\xi\left(\gamma_{r-1} \cdot \gamma_r^2\right) > 0 \right] \right\} ,$$

$$\Phi_2 \equiv \left\{ \left[\sim \left(\alpha_0 = 0\right) \vee \ldots \vee \sim \left(\alpha_m = 0\right) \right] \wedge \right.$$
$$\left. \underset{r_2}{(E\xi)} \left[\left(\alpha = 0\right) \wedge \left(\gamma_1 > 0\right) \wedge \ldots \wedge \left(\gamma_{r-2} > 0\right) \wedge P_\xi\left(\gamma_{r-1}^2 \cdot \gamma_r\right) > 0 \right] \right\} ,$$

$$\Phi_3 \equiv \left\{ \left[\sim \left(\alpha_0 = 0\right) \vee \ldots \vee \sim \left(\alpha_m = 0\right) \right] \wedge \right.$$
$$\left. \underset{r_3}{(E\xi)} \left(\left(\alpha = 0\right) \wedge \left(\gamma_1 > 0\right) \wedge \ldots \wedge \left(\gamma_{r-2} > 0\right) \wedge P_\xi \left[(-1) \cdot \gamma_{r-1} \cdot \gamma_r \right] > 0 \right) \right\} ;$$

in the case $r = 2$ *we omit the expression*

$$\left(\gamma_1 > 0\right) \wedge \ldots \wedge \left(\gamma_{r-2} > 0\right) \wedge$$

from the formulas defining Φ_1, Φ_2, *and* Φ_3.

(iv) *If* Φ *is a formula of the form*

$$\sim \left(\alpha_m = 0\right) \wedge \underset{k}{(E\xi)} \left[\left(\alpha = 0\right) \wedge \left(\gamma_1 > 0\right) \wedge \ldots \wedge \left(\gamma_r > 0\right) \right] ,$$

then we set

$$T(\Phi) \equiv \left(\sim \left(\alpha_m = 0\right) \wedge T \left\{ \left[\sim \left(\alpha_0 = 0\right) \vee \ldots \vee \sim \left(\alpha_m = 0\right) \right] \wedge \right. \right.$$
$$\left. \left. \underset{k}{(E\xi)} \left[\left(\alpha = 0\right) \wedge \left(\gamma_1 > 0\right) \wedge \ldots \wedge \left(\gamma_r > 0\right) \right] \right\} \right) .$$

(v) *If* Φ *is a formula of the form*

$$\left[\sim \left(\gamma_{1,n_1} = 0\right) \wedge \sim \left(\gamma_{2,n_2} = 0\right) \wedge \ldots \wedge \sim \left(\gamma_{r,n_r} = 0\right) \right] \wedge \underset{k}{(E\xi)} \left[\left(\gamma_1 > 0\right) \wedge \ldots \wedge \left(\gamma_r > 0\right) \right] ,$$

then, if $k > 0$, we set

$$T(\Phi) \equiv (0 = 1) \;;$$

while if $k = 0$ and $n_1 + \cdots + n_r = 0$, we set

$$T(\Phi) \equiv \Big\{ \big[\sim(\gamma_{1,0} = 0) \wedge \ldots \wedge \sim(\gamma_{r,0} = 0)\big] \wedge \big[(0 > \gamma_{1,0}) \vee \ldots \vee (0 > \gamma_{r,0})\big] \Big\} \;;$$

and if $k = 0$ and $n_1 + \ldots + n_r > 0$, we set

$$\begin{aligned} T(\Phi) \equiv & \Big\{ \sim\left(\gamma_{1,n_1} = 0\right) \wedge \ldots \wedge \sim\left(\gamma_{r,n_r} = 0\right) \;\wedge \Big[\left(0 > \gamma_{1,n_1}\right) \vee \ldots \vee \left(0 > \gamma_{r,n_r}\right) \Big] \Big\} \;\wedge \\ & \Big\{ \left[0 > (-1)^{n_1} \cdot \gamma_{1,n_1}\right] \vee \ldots \vee \left[0 > (-1)^{n_r} \cdot \gamma_{r,n_r}\right] \Big\} \;\wedge \\ & T \Big\{ \sim(\delta = 0) \wedge (\underset{0}{E}\,\xi) \Big(\Big[D_\xi P_\xi(\gamma_1 \cdot \ldots \cdot \gamma_r) = 0 \Big] \wedge (\gamma_1 > 0) \;\wedge \ldots \wedge (\gamma_r > 0) \Big) \Big\} \end{aligned}$$

where δ is the leading coefficient of $D_\xi P_\xi(\gamma_1 \cdot \ldots \cdot \gamma_r)$.

(vi) *If Φ is a formula of the form*

$$(\underset{k}{E}\,\xi)\, \big[(\gamma_1 > 0) \wedge \ldots \wedge (\gamma_r > 0)\big] \;,$$

and if $k \neq 0$, we set

$$T(\Phi) \equiv (0 = 1) \;;$$

while if $k = 0$, we set

$$\begin{aligned} T(\Phi) \equiv & \Big\{ \Big[(\gamma_{1,0} = 0) \wedge \ldots \wedge (\gamma_{1,n_1} = 0) \Big] \vee \ldots \vee \Big[(\gamma_{r,0} = 0) \wedge \ldots \wedge (\gamma_{r,n_r} = 0) \Big] \Big\} \;\vee \\ & \bigvee_{(s_1,\ldots,s_r) \text{ in } S} \Big\{ \Psi_{1,s_1} \wedge \ldots \wedge \Psi_{r,s_r} \wedge T\Big(\Big[\sim(\gamma_{1,s_1} = 0) \wedge \ldots \wedge \sim(\gamma_{r,s_r} = 0) \Big] \;\wedge \\ & \qquad (\underset{0}{E}\,\xi) \;\Big[\left(Rd_\xi^{n_1 - s_1}(\gamma_1) > 0\right) \wedge \ldots \wedge \left(Rd_\xi^{n_r - s_r}(\gamma_r) > 0\right) \Big] \Big) \Big\} \;. \end{aligned}$$

where S is the set of all ordered r-tuples $(s_1, \ldots, s_r)$ with $0 \le s_1 \le n_1, \ldots, 0 \le s_r \le n_r$,

$\Psi_{k,l} \equiv \big[(\gamma_{k,l+1} = 0) \wedge \ldots \wedge (\gamma_{k,n_k} = 0)\big]$ for $0 \le l < n_k$, and $\Psi_{k,l} \equiv (0 = 0)$ for $l = n_k$.

(vii) *If Φ is a formula of the form*

$$(\underset{k}{E}\xi)\ \left[(\alpha = 0)\wedge(\gamma_1 > 0)\wedge\ldots\wedge(\gamma_r > 0)\right]$$

then we set

$$T(\Phi) \equiv T\left\{\left[\sim(\alpha_0 = 0)\vee\ldots\vee\sim(\alpha_m = 0)\right]\wedge\Phi\right\} \vee$$

$$\left(\left[(\alpha_0 = 0)\wedge\ldots\wedge(\alpha_m = 0)\right]\wedge T\left\{(\underset{k}{E}\xi)\ \left[(\gamma_1 > 0)\wedge\ldots\wedge(\gamma_r > 0)\right]\right\}\right).$$

(viii) *If Φ is a formula of the form*

$$(\underset{k}{E}\xi)\left[(\gamma_1 = 0)\wedge\ldots\wedge(\gamma_r = 0)\right] ,$$

then we set

$$T(\Phi) \equiv T\left\{(\underset{k}{E}\xi)\left[P_\xi\left(\gamma_1^2+\ldots+\gamma_r^2\right) = 0\right]\right\} .$$

(ix) *If Φ is a formula of the form*

$$(\underset{k}{E}\xi)\left[(\gamma_1 = 0)\wedge\ldots\wedge(\gamma_s = 0)\wedge(\gamma_{s+1} > 0)\wedge\ldots\wedge(\gamma_r > 0)\right]$$

where $1 < s < r$, then we set

$$T(\Phi) \equiv T\left\{(\underset{k}{E}\xi)\left[P_\xi\left(\gamma_1^2+\ldots+\gamma_s^2\right) = 0\wedge(\gamma_{s+1} > 0)\wedge\ldots\wedge(\gamma_r > 0)\right]\right\}.$$

(x) *If Φ is a formula, not of any of the previous forms, but such that*

$$\Phi \equiv (\underset{k}{E}\xi)\left(\Phi_1\wedge\Phi_2\wedge\ldots\wedge\Phi_r\right),$$

where each Φ_i is of one of the forms $\gamma_i = 0$ or $\gamma_i > 0$, and if $j_1,\ldots,j_u$ are the values of i (in increasing order) for which $\Phi_i \equiv (\gamma_i = 0)$; and if $j_{u+1},\ldots,j_r$ are the values of i (in increasing order) for which $\Phi_i \equiv (\gamma_i > 0)$, then we set

$$T(\Phi) \equiv T(\underset{k}{E}\xi)\left(\Phi_{j_1}\wedge\ldots\wedge\Phi_{j_r}\right)$$

THEOREM 29. *Let ξ be any variable, and let Φ be any formula such that $T(\Phi)$ is defined (by Definition 28). Then $T(\Phi)$ is a formula which contains no quantifiers, and no variables except those that occur free in Φ. Moreover, Φ is equivalent to $T(\Phi)$.*

PROOF. The first part follows immediately from Theorem 27 and Definition 28.

We shall prove the second part by considering separately the ten possible forms Φ can have according to Definition 28. As in the proof of Theorem 27, we shall use here partially ordinary mathematical modes of expression, without taking any great pains to distinguish sharply mathematical from metamathematical notions.

Suppose first, then, that Φ is of the form 28 (i): i.e., that $\Phi \equiv (\underset{k}{E}\xi)\,(\alpha = 0)$, where α is a polynomial in ξ. We are to show that Φ is equivalent to the formula

$$\left[\sim\left(\alpha_0 = 0\right) \vee \ldots \vee \sim\left(\alpha_m = 0\right)\right] \wedge SG_{\xi}^{-k}\left(\alpha, D_{\xi}(\alpha)\right) ,$$

where $\alpha_0, \ldots, \alpha_m$ are the coefficients of α. Since by Theorem 27 the latter formula is equivalent to

$$\left[\sim\left(\alpha_0 = 0\right) \vee \ldots \vee \sim\left(\alpha_m = 0\right)\right] \wedge G_{\xi}^{-k}\left(\alpha, D_{\xi}(\alpha)\right) ,$$

we see that our task reduces to establishing the following: if α is any polynomial in ξ which is not identically zero, then α has k distinct roots if and only if $G_{\xi}^{-k}\left(\alpha, D_{\xi}(\alpha)\right)$ holds. Let s_1 be the number of numbers ξ such that: (1) the order of ξ in α is by a positive odd integer higher than its order in $D_{\xi}(\alpha)$; (2) there exists an open interval whose right-hand end-point is ξ, within which the values of α and $D_{\xi}(\alpha)$ have the same sign. Let s_2 be the number of numbers ξ which satisfy condition (1) above and moreover the condition: (3) there exists an open interval whose right-hand end-point is ξ, within which the values of α and $D_{\xi}(\alpha)$ have different signs. By the remark preceding Definition 22, we see that $G_{\xi}^{-k}(\alpha, D_{\xi}(\alpha))$ is true if and only if $-k = s_1 - s_2$. Moreover, it is readily seen that $s_1 = 0$, and that s_2 is simply the number of distinct roots of α. Thus $G_{\xi}^{-k}(\alpha, D_{\xi}(\alpha))$ holds if and only if k is the number of distinct roots of α, as was to be shown.

In order to treat the case where Φ is of the form 28 (ii), it is convenient first to establish the following: Let α and β be polynomials in ξ, let t_1, be the number of roots of α at which β is positive, and let t_2 be the number of roots of α at which β is negative; then $SG_{\xi}^{-c}(\alpha, D_{\xi}(\alpha) \cdot_{\xi} \beta)$ is true if and only if $c = t_1 - t_2$. This can easily be done by the sort of argument applied in the preceding paragraph — making use of Theorem 27 and the remark preceding Definition 22. We notice also that, since we are dealing with the algebra of real numbers, the common roots of two polynomials α and β coincide with the roots of $\alpha^2 + \beta^2$. Now let Φ be a formula of the form given in 28 (ii). To show that Φ is equivalent to $T(\Phi)$, it suffices to show that, if k is a non-negative integer, and α and β are polynomials, where α is of degree m and not identically zero, then the following conditions are equivalent: (1) there are exactly k roots of α at which β is positive; (2) there are integers r_1, r_2, and r_3 satisfying $2k = r_1 - r_2 + r_3$, $0 \leq r_1 \leq m$, $0 \leq r_2 \leq m$, $-m \leq r_3 \leq m$, such that r_1 is the number of roots of α, r_2 is the number of roots common to α and β, and r_3 is the difference between the number of roots of α at which β is positive and the number of roots of α at which β is negative. Now α has at most m roots; hence, if r_1, r_2, and r_3 have the meanings indicated in (2) — i.e., if r_1 is the number of roots of α, etc. — we obviously have

$$0 \leq r_1 \leq m,\ 0 \leq r_2 \leq m, \text{ and } -m \leq r_3 \leq m .$$

Let k be the number of roots of α at which β is positive, and let r_4 be the number of roots of α at which β is negative. We see immediately from the definitions of r_1, r_2, r_3, k, and r_4 that

$$r_1 - r_2 = k + r_4$$

$$r_3 = k - r_4$$

Eliminating r_4 between these two equations, we obtain

$$2k = r_1 - r_2 + r_3 \ .$$

Thus (1) implies (2); the proof in the opposite direction is almost obvious.

To prove our theorem for formulas of the form 28 (iii), it suffices to show that if α is a polynomial of degree m, and not identically zero, and if $\gamma_1, \ldots, \gamma_r$ are any polynomials, then the following conditions are equivalent: (1) there are exactly k roots of α at which $\gamma_1, \ldots, \gamma_r$ are all positive; and (2) there are three integers r_1, r_2, r_3 satisfying $2k = r_1 + r_2 - r_3$, $0 \leq r_1, r_2, r_3 \leq m$, such that r_1 is the number of roots of α at which $\gamma_1, \ldots, \gamma_{r-2}$, and $\gamma_{r-1} \cdot \gamma_r^2$ are all positive, r_2 is the number of roots of α at which $\gamma_1, \ldots, \gamma_{r-2}$, and $\gamma_{r-1}^2 \cdot \gamma_r$ are all positive, and r_3 is the number of roots of α at which $\gamma_1, \ldots, \gamma_{r-2}$, and $-1 \cdot \gamma_{r-1} \cdot \gamma_r$ are all positive. In fact, if r_1, r_2, and r_3 have the meanings just indicated, we obviously have

$$0 \leq r_1, r_2, r_3 \leq m \ .$$

Let r_4 be the number of roots of α at which $\gamma_1, \ldots, \gamma_{r-2}, \gamma_{r-1}$ are all positive, and γ_r is negative. Let r_5 be the number of roots of α at which $\gamma_1, \ldots, \gamma_{r-2}$ and γ_r are all positive, and γ_{r-1} is negative. Let k be the number of roots of α at which $\gamma_1, \ldots, \gamma_r$ are all positive. From the definitions of r_1, r_2, r_3, r_4, r_5 and k we see that

$$k + r_4 = r_1$$

$$k + r_5 = r_2$$

$$r_4 + r_5 = r_3$$

Eliminating r_4 and r_5 from these equations, we obtain

$$2k = r_1 + r_2 - r_3 \ ,$$

which completes this part of the proof.

To prove our theorem for formulas of the form 28 (iv), we need only notice that the formula

$$\sim\!\left(\alpha_m = 0\right) \wedge \left[\sim\!\left(\alpha_0 = 0\right) \vee \ldots \vee \sim\!\left(\alpha_m = 0\right)\right]$$

is equivalent to

$$\sim\!\left(\alpha_m = 0\right) \ .$$

Now suppose that Φ is of the form 28 (v): i.e., that Φ is

$$\left[\sim\left(\gamma_{1,n_1} = 0\right)\wedge\ldots\wedge\sim\left(\gamma_{r,n_r} = 0\right)\right] \wedge \underset{k}{(E\xi)} \left[\left(\gamma_1 > 0\right)\wedge\ldots\wedge\left(\gamma_r > 0\right)\right] .$$

We notice first that if $k > 0$, then the formula

$$\underset{k}{(E\xi)} \left[\left(\gamma_1 > 0\right)\wedge\ldots\wedge\left(\gamma_r > 0\right)\right]$$

is never satisfied (i.e., is satisfied by no values of the free variables occurring in it), so that Φ is never satisfied either — and hence is equivalent to $(0 = 1)$. If $k = 0$, and $n_1 +\ldots+ n_r = 0$, then $n_1 = n_2 =\ldots= n_r = 0$, and hence Φ reduces to

$$\left[\sim\left(\gamma_{1,0} = 0\right)\wedge\ldots\wedge\sim\left(\gamma_{r,0} = 0\right)\right] \wedge \underset{0}{(E\xi)} \left[\left(\gamma_{1,0} > 0\right)\wedge\ldots\wedge\left(\gamma_{r,0} > 0\right)\right] ,$$

where $\gamma_{1,0}, \ldots, \gamma_{r,0}$ are terms which do not involve ξ; since

$$\underset{0}{(E\xi)} \left[\left(\gamma_{1,0} > 0\right)\wedge\ldots\wedge\left(\gamma_{r,0} > 0\right)\right]$$

is then equivalent to

$$\sim\left[\left(\gamma_{1,0} > 0\right)\wedge\ldots\wedge\left(\gamma_{r,0} > 0\right)\right] ,$$

we see that Φ is equivalent to $T(\Phi)$, as was to be shown.

Thus we are left with the case that Φ is of the form 28 (v) where $k = 0$ and $n_1 +\ldots+ n_r > 0$. To establish in this case that Φ is equivalent to $T(\Phi)$, it suffices to prove: If $\gamma_1, \ldots, \gamma_r$ are polynomials in ξ not all of which are of degree zero, and whose leading coefficients are all different from zero, then a necessary and sufficient condition that there exist no value of ξ which makes all these polynomials positive is that the following three conditions hold: (1) at least one of the polynomials have a negative leading coefficient; (2) at least one of the polynomials satisfy $(-1)^{n_i}\gamma_{i,ni} < 0$ (where n_i is the degree of the polynomial, and $\gamma_{i,ni}$ its leading coefficient); (3) there exist no value of ξ which is a root of the derivative of the product of the polynomials, and which makes them all positive. To see that the condition is necessary, suppose that $\gamma_1, \ldots, \gamma_r$ are polynomials which are never all positive for the same value of ξ; then it is immediately apparent that (3) is satisfied; to see that (1) is satisfied, we remember that, if the leading coefficient of a polynomial is positive, then we can find a number μ such that the polynomial is positive for all values of the variable ξ greater than μ; the proof of (2) is similar, by considering large negative values of the variable. Now suppose, if possible, that the condition is not sufficient: i.e., suppose that (1), (2), and (3) are satisfied, and that there exists some ξ which makes all the polynomials positive. Let λ be a value of ξ at which $\gamma_1 > 0, \ldots, \gamma_r > 0$. Then we see that, for $\xi = \lambda$,

$$\gamma_1 \cdot \gamma_2 \cdot \ldots \cdot \gamma_r > 0 .$$

On the other hand, since (1) is true, there exists an i such that γ_i has a negative leading coefficient. Hence we can find a λ' which is larger than λ and sufficiently large that γ_i is negative at λ'. Then γ_i is positive at λ and negative at λ' and hence has a root between these numbers. Since every root of γ_i is also a root of $\gamma_1 \cdot \gamma_2 \cdot \ldots \cdot \gamma_r$, we conclude that $\gamma_1 \cdot \gamma_2 \cdot \ldots \cdot \gamma_r$ has a root to the right of λ. Similarly, making use of (2), we see that $\gamma_1 \cdot \gamma_2 \cdot \ldots \cdot \gamma_r$ has a root to the left of λ. Now let μ_1 be the largest root of $\gamma_1 \cdot \gamma_2 \cdot \ldots \cdot \gamma_r$ to the left of λ and let μ_2 be the smallest root of $\gamma_1 \cdot \gamma_2 \cdot \ldots \cdot \gamma_r$ to the right of λ. Then $\gamma_1 \cdot \gamma_2 \cdot \ldots \cdot \gamma_r$ is positive in the open interval (μ_1, μ_2) and zero at its end-points. We see that no γ_i can have a root within the open interval (μ_1, μ_2); since each γ_i is positive at λ, which lies within this interval, we conclude that each γ_i is positive throughout the whole open interval. On the other hand, since $\gamma_1 \cdot \gamma_2 \cdot \ldots \cdot \gamma_r$ is zero at μ_1 and at μ_2, we see by Rolle's theorem that there is a point ν within (μ_1, μ_2) at which the derivative of $\gamma_1 \cdot \gamma_2 \cdot \ldots \cdot \gamma_r$ vanishes. Since this contradicts (3), we conclude that the condition is also sufficient.

Now suppose that $\bar{\Phi}$ is of the form 28 (vi). If $k \neq 0$, it is obvious that $\bar{\Phi}$ is equivalent to $T(\bar{\Phi})$. Hence suppose that $k = 0$. Two cases are logically possible: either one of the polynomials $\gamma_1, \ldots, \gamma_r$ vanishes identically, or none of them does. In the first case, $\bar{\Phi}$ obviously holds. In the second case, let s_i, for $i = 1, \ldots, r$, be the largest index j such that $\gamma_{i,j}$ (i.e., the j^{th} coefficient of γ_i) does not vanish. Then $\bar{\Phi}$ is obviously equivalent to the formula

$$\psi \equiv \Big[\sim\!\big(\gamma_{1,s_1} = 0\big) \wedge \ldots \wedge \sim\!\big(\gamma_{r,s_r} = 0\big)\Big] \wedge (\underset{0}{E}\xi)\Big(\Big[Rd_\xi^{n_1 - s_1}(\gamma_1) > 0\Big] \wedge \ldots \wedge \Big[Rd_\xi^{n_r - s_r}(\gamma_r) > 0\Big]\Big).$$

However $\bar{\Psi}$ is of the form 28 (v), and hence, as we have shown above, is equivalent to $T(\bar{\Psi})$. In view of these remarks, by looking at the formula defining $T(\bar{\Phi})$ in 28 (vi), we see at once that $\bar{\Phi}$ and $T(\bar{\Phi})$ are equivalent.

If $\bar{\Phi}$ is of the form 28 (vii), our theorem follows from the obvious fact that $\bar{\Phi}$ is equivalent to

$$\Big\{\Big[\sim\!\big(\alpha_0 = 0\big) \vee \ldots \vee \sim\!\big(\alpha_m = 0\big)\Big] \wedge \bar{\Phi}\Big\} \vee \Big\{\Big[\big(\alpha_0 = 0\big) \wedge \ldots \wedge \big(\alpha_m = 0\big)\Big] \wedge \bar{\Phi}\Big\}.$$

If $\bar{\Phi}$ is of the form 28 (viii), or of the form 28 (ix), our theorem follows from the fact — which was already used in discussing 28 (ii) — that the common roots of r polynomials $\gamma_1, \ldots, \gamma_r$ coincide with the roots of $\gamma_1^2 + \ldots + \gamma_r^2$.

If $\bar{\Phi}$ is of the form 28 (x), our theorem follows from the associative and commutative laws for conjunction, familiar from elementary logic.

DEFINITION 30. *Let $\bar{\Phi}$, $\bar{\Psi}$, and Θ be any formulas, and ξ any variable.*

(i) *If $\bar{\Phi}$ is an atomic formula, we set*

$$U(\bar{\Phi}) \equiv \bar{\Phi}.$$

(ii) *If $\bar{\Phi} \equiv (\bar{\Psi} \vee \Theta)$, then we set*

$$U(\bar{\Phi}) \equiv \Big[U(\bar{\Psi}) \vee U(\Theta)\Big].$$

(iii) *If* $\Phi \equiv (\Psi \wedge \Theta)$, *then we set*

$$U(\Phi) \equiv \left[U(\Psi) \wedge U(\Theta) \right] .$$

(iv) *If* $\Phi \equiv \sim \Psi$, *then we set*

$$U(\Phi) \equiv \sim U(\Psi) .$$

(v) *If* $\Phi \equiv (E\xi)\,\Psi$, *and*

$$QP_{\xi}\, U(\Psi) \equiv \Psi_1 \vee \Psi_2 \vee \ldots \vee \Psi_n \;,$$

where Ψ_i, *for* $i = 1, \ldots, n$, *is a conjunction of atomic formulas, then we set*

$$U(\Phi) \equiv \sim T\left[\underset{0}{(E\xi)}\, \Psi_1 \right] \vee \sim T\left[\underset{0}{(E\xi)}\, \Psi_2 \right] \vee \ldots \vee \sim T\left[\underset{0}{(E\xi)}\, \Psi_n \right] .$$

Theorem 31. *If* Φ *is any formula, then* $U(\Phi)$ *is a formula which contains no quantifiers, and no free variables except variables which occur free in* Φ. *Moreover,* Φ *is equivalent to* $U(\Phi)$.

Proof. By induction on the order of Φ, making use of Theorems 14 and 29.

Corollary 32. *If* Φ *is any sentence, then* $U(\Phi)$ *is an equivalent sentence without any variables or quantifiers.*

The first part of our task as outlined at the beginning of this section has thus been completed. We have established a general procedure which permits us to transform every formula (and in particular every sentence) into an equivalent formula (or sentence) without quantifiers[12], [13]. Before continuing the discussion, we should like to give a few relatively simple examples in which such a transformation has actually been carried out. The equivalent transformations $U'(\Phi)$ which are given below for some formulas Φ do not coincide with $U(\Phi)$ but can be obtained from the latter by means of elementary simplifications.

Let ξ be any variable, and α_0, α_1, α_2, α_3, β_0, β_1, and β_2 any terms which do not involve ξ. If

$$\Phi \equiv (E\xi)\left[\alpha_0 + \alpha_1 \cdot \xi + \alpha_2 \cdot \xi^2 + \alpha_3 \cdot \xi^3 = 0 \right]$$

we obtain an equivalent formula by setting

$$U'(\Phi) \equiv \Big\{ (\alpha_0 = 0) \vee \left[\sim(\alpha_1 = 0) \wedge (\alpha_2 = 0) \right] \vee \left[\sim(\alpha_2 = 0) \wedge \sim\left(4 \cdot \alpha_0 \cdot \alpha_2 > \alpha_1^2\right) \right] \vee \sim(\alpha_3 = 0) \Big\}$$

(where, as can easily be guessed, 4 stands for 1 + 1 + 1 + 1). If

$$\Phi \equiv (E\xi)\left[\alpha_0 + \alpha_1\cdot\xi + \alpha_2\cdot\xi^2 + \alpha_3\cdot\xi^3 > 0\right],$$

we can put

$$U'(\Phi) \equiv \left\{(\alpha_0 > 0) \vee (\alpha_1^2 > 4\cdot\alpha_0\cdot\alpha_2) \vee (\alpha_2 > 0) \vee \sim(\alpha_3 = 0)\right\}.$$

If, finally,

$$\Phi \equiv (E\xi)\left[(\alpha_0 + \alpha_1\cdot\xi + \alpha_2\cdot\xi^2 = 0) \wedge (\beta_0 + \beta_1\cdot\xi + \beta_2\cdot\xi^2 > 0)\right],$$

we can put

$$\begin{aligned} U'(\Phi) \equiv \Big\{ & \left[(\alpha_0 = 0) \wedge (\alpha_1 = 0) \wedge (\alpha_2 = 0) \wedge \left((\beta_0 > 0) \vee (\beta_1^2 > 4\cdot\beta_0\cdot\beta_2) \vee (\beta_2 > 0)\right)\right] \vee \\ & \left[\sim(\alpha_1 = 0) \wedge (\alpha_2 = 0) \wedge (\alpha_0^2\cdot\beta_2 + \alpha_1^2\cdot\beta_0 > \alpha_0\cdot\alpha_1\cdot\beta_1)\right] \vee \\ & \left[\sim(\alpha_2 = 0) \wedge \sim(4\cdot\alpha_0\cdot\alpha_2 > \alpha_1^2) \wedge (\alpha_1^2\cdot\beta_2 + 2\cdot\alpha_2^2\cdot\beta_0 > 2\cdot\alpha_0\cdot\alpha_2\cdot\beta_2 + \alpha_1\cdot\alpha_2\cdot\beta_1)\right] \vee \\ & \Big[\sim(\alpha_2 = 0) \wedge (\alpha_1^2 > 4\alpha_0\cdot\alpha_2) \wedge \\ & \quad (\alpha_0^2\cdot\beta_2^2 + \alpha_0\cdot\alpha_2\cdot\beta_1^2 + \alpha_1^2\cdot\beta_0\cdot\beta_2 + \alpha_2^2\cdot\beta_0^2 > \alpha_0\cdot\alpha_1\cdot\beta_1\cdot\beta_2 + 2\cdot\alpha_0\cdot\alpha_2\cdot\beta_0\cdot\beta_2 + \alpha_1\cdot\alpha_2\cdot\beta_0\cdot\beta_1)\Big]\Big\}. \end{aligned}$$

We now turn to the second part of our task. We want to correlate, with every sentence Φ which contains no variables or quantifiers, an equivalent sentence of a very special form: in fact, one of the two sentences

$$0 = 0$$

and

$$0 = 1.$$

We first consider terms which occur in such sentences. As is easily seen, every such term is obtained from the algebraic constants 0, 1, and −1 by combining them by means of addition and multiplication. Hence we can correlate with every such term α an integer $n(\alpha)$ in the following way.

DEFINITION 33. *We set*

$$n(1) = 1,$$

$$n(-1) = -1,$$

$$n(0) = 0.$$

If $\alpha \equiv (\beta + \gamma)$, *then we set*

$$n(\alpha) = n(\beta) + n(\gamma).$$

If $\alpha \equiv (\beta\cdot\gamma)$, *then we set*

$$n(\alpha) = n(\beta)\cdot n(\gamma).$$

Remark. It should be emphasized that the above definition correlates integers, not expressions, with terms. It is for this reason that we have written, for example,

$$n(1) = 1,$$

instead of

$$n(1) \equiv 1;$$

$n(1)$ is the integer 1, not a name of that integer. In the equation

$$n(\alpha) = n(\beta) + n(\gamma)$$

the addition sign indicates the sum of the two integers $n(\beta)$ and $n(\gamma)$. $n(\alpha)$ is what would ordinarily be called the "value" of the expression α; thus, if

$$\alpha \equiv 1 + (1 + 1)\cdot(1 + 1), \text{ then } n(\alpha) = 5.$$

On the other hand, we could use for our purposes, instead of integers, certain expressions of our formal system of algebra — in fact one of the terms of the following sequence

$$\ldots, \quad (-1) + (-1), \quad -1, \quad 0, \quad 1, \quad 1 + 1, \ldots .$$

We can use these special terms since they can obviously be put in one-to-one correspondence with arbitrary integers. As a result of this modification, however, Definition 33 and the subsequent Definition 34 would assume a more complicated form.

Definition 34. *Let α and β be terms, and Φ, Ψ, and θ formulas, none of which contain any variables.*

(i) *If $\Phi \equiv (\alpha = \beta)$, we set*

$$W(\Phi) \equiv (0 = 0)$$

in case $n(\alpha) = n(\beta)$, and otherwise

$$W(\Phi) \equiv (0 = 1) .$$

(ii) *If $\Phi \equiv (\alpha > \beta)$, we set*

$$W(\Phi) \equiv (0 = 0)$$

in case $n(\alpha) > n(\beta)$, and otherwise

$$W(\Phi) \equiv (0 = 1) .$$

(iii) *If $\Phi \equiv (\Psi \vee \theta)$, we set*

$$W(\Phi) \equiv (0 = 0)$$

in case either $W(\Psi) \equiv (0 = 0)$ or $W(\theta) \equiv (0 = 0)$, and otherwise

$$W(\Phi) \equiv (0 = 1) .$$

(iv) *If $\Phi \equiv (\Psi \wedge \Theta)$, we set*

$$W(\Phi) \equiv (0 = 0)$$

in case both $W(\Psi) \equiv (0 = 0)$ and $W(\Theta) \equiv (0 = 0)$, and otherwise

$$W(\Phi) \equiv (0 = 1) .$$

(v) *If $\Phi \equiv \sim \Psi$, we set*

$$W(\Phi) \equiv (0 = 0)$$

in case $W(\Psi) \equiv (0 = 1)$, and otherwise

$$W(\Phi) \equiv (0 = 1) .$$

THEOREM 35. *If Φ is any sentence which involves no quantifiers or variables, then $W(\Phi)$ is one or the other of the two sentences $0 = 0$ and $0 = 1$. Moreover, Φ is equivalent to $W(\Phi)$.*

PROOF. By induction on the order of Φ.

THEOREM 36. *If Φ is any sentence, then $WU(\Phi)$ is one or the other of the two sentences $0 = 0$ and $0 = 1$. Moreover, Φ is equivalent to $WU(\Phi)$.*

PROOF. By 32 and 35.

Now by analyzing the definitions of W, U, and the preceding functions, we notice that for any given sentence Φ we can actually find the value of $WU(\Phi)$ in a finite number of steps(14). By combining this with the result stated in Theorem 36, we obtain

THEOREM 37. *There is a decision method for the class of all true sentences of elementary algebra*(15).

In concluding this section we should like to remark that the minimum number of steps which are necessary for the evaluation of $WU(\Phi)$ is of course a function of the form of Φ — in particular, this number depends on the length of Φ, on the number of quantifiers occurring in it, and so on. The problem of estimating the order of increase of this function is of primary importance in connection with the question of the feasibility of constructing a decision machine for elementary algebra.

SECTION 3.

EXTENSIONS TO RELATED SYSTEMS

In this section we shall discuss some applications to other systems of the resu'lts obtained in Section 2, as well as some problems that are still open.

The decision method found for the algebra of real numbers can be extended to various algebraic systems built upon real numbers — thus to the elementary algebra of complex numbers, that of quaternions, and that of n-dimensional vectors. We can think of the elementary algebra of complex numbers, for example, as a formal system very closely related to that described in Section 1: variables are now thought of as representing arbitrary complex numbers; the logical and mathematical constants remain unchanged; but now the greater-than relation is thought of as holding exclusively between real numbers — thus we can define real numbers within the system by saying that x is real if, for some y, $x > y$. If one wishes, one can enrich the system by a new predicate $Rl(x)$, agreeing that $Rl(x)$ will mean that x is real(16).

The results obtained can furthermore be extended to the elementary systems of n-dimensional Euclidean geometry. Since the methods of extending the results to the algebraic systems and the geometric systems are essentially the same, we shall consider a little more closely the case of 2-dimensional Euclidean geometry.

We first give a sketchy description of the formal system of 2-dimensional Euclidean geometry. We use infinitely many *variables,* which are to be thought of as representing arbitrary points of the Euclidean plane. We use three constants denoting relations between points: the binary relation of *identity*, symbolized by "="; the ternary relation of *betweenness*, symbolized by "B", so that "$B(x, y, z)$" is to be read "y is between x and z" (i.e., y lies between x and z on the straight line connecting them; it is not necessary that the three points all be distinct; $B(x, y, z)$ is always true if $x = y$ or if $y = z$; but we cannot have $x = z$ unless $x = y = z$); and the quaternary *equidistance* relation, symbolized by "D", so that "$D(x,y; x',y')$" is to be read "x is just as far from y as x' is from y'" (or, "the distance from x to y equals the distance from x' to y'")(17). The only *terms* of this system are variables. An *atomic formula* is an expression of one of the forms

$$\xi = \eta, \qquad B(\xi_1,\xi_2,\xi_3), \qquad D(\xi,\eta;\xi',\eta'),$$

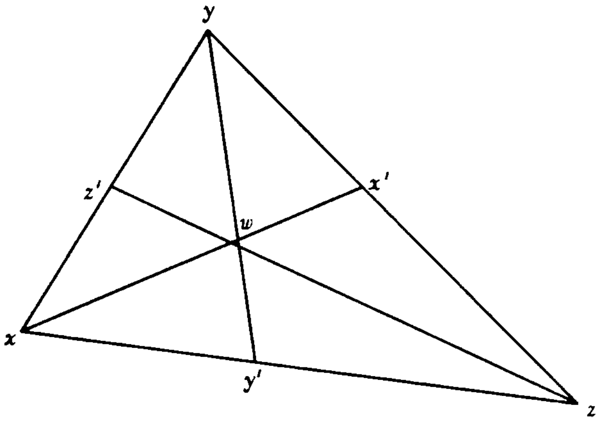
where

$$\xi,\eta,\xi_1,\xi_2,\xi_3,\xi', \text{ and } \eta'$$

are arbitrary variables. As in the formal system of elementary algebra we build up *formulas,* from atomic formulas by means of negation, conjunction, disjunction, and the application of quantifiers; we also introduce here as abbreviations the symbols $\rightarrow$ and $\leftrightarrow$.

Sentences of elementary geometry, in our formulation, express certain facts about points and relation between them. On the other hand, most theorems which one finds in high-school textbooks on this subject involve also such notions as triangle, plane, circle, line, and the like. It is easy, however, to convince oneself that a considerable part of these notions can be translated into the language of our system. Thus, for example, the theorem that the medians of a triangle are concurrent can be expressed as follows (cf. the figure immediately following the formula):

$$
\begin{aligned}
(Ax)(Ay)(Az)(Ax')(Ay')(Az')\Big\{\Big[&\sim B(x,y,z)\wedge\sim B(y,z,x)\wedge\sim B(z,x,y)\wedge B(x,y',z)\wedge\\
&B(y,z',x)\wedge B(z,x',y)\wedge D(x,z';z',y)\wedge\\
&D(y,x';x',z)\wedge D(z,y';y',x)\Big]\longrightarrow\\
&(Ew)\Big[B(x,w,x')\wedge B(y,w,y')\wedge B(z,w,z')\Big]\Big\}.
\end{aligned}
$$



On the other hand, it would not be difficult to enrich our system of geometry so as to enable us to refer to these elementary figures directly. Regarding more essential limitations of our system, see the remarks in the Introduction.

In order to obtain a decision procedure for elementary geometry, we correlate with every sentence Φ of elementary geometry a sentence Φ^* of elementary algebra in the sense of Section 1. The construction of Φ^* can be roughly described in the following way. With every (geometric) variable ξ in Φ we correlate two different (algebraic) variables $\bar{\xi}$ and $\bar{\bar{\xi}}$, in such a way that if ξ and η are two different variables in Φ, then $\bar{\xi}$, $\bar{\bar{\xi}}$, $\bar{\eta}$, and $\bar{\bar{\eta}}$ are all distinct. Next we replace in Φ every quantifier expression $(E\xi)$ by $(E\bar{\xi})(E\bar{\bar{\xi}})$; every partial formula $\xi = \eta$ by $(\bar{\xi} = \bar{\eta}) \wedge (\bar{\bar{\xi}} = \bar{\bar{\eta}})$; every formula $B(\xi,\eta,\mu)$ by

$$
\begin{aligned}
\Big[(\bar{\bar{\eta}}-\bar{\bar{\xi}})\cdot(\bar{\mu}-\bar{\eta}) = (\bar{\bar{\mu}}-\bar{\bar{\eta}})\cdot(\bar{\eta}-\bar{\xi})\Big]\wedge\Big[&((\bar{\xi}-\bar{\eta})\cdot(\bar{\eta}-\bar{\mu}) > 0)\vee((\bar{\xi}-\bar{\eta})\cdot(\bar{\eta}-\bar{\mu}) = 0)\Big]\wedge\\
\Big[&((\bar{\bar{\xi}}-\bar{\bar{\eta}})\cdot(\bar{\bar{\eta}}-\bar{\bar{\mu}}) > 0)\vee((\bar{\bar{\xi}}-\bar{\bar{\eta}})\cdot(\bar{\bar{\eta}}-\bar{\bar{\mu}}) = 0)\Big];
\end{aligned}
$$

and every partial formula $D(\xi,\eta;\mu,\nu)$ by

$$(\bar{\xi}-\bar{\eta})^2 + (\bar{\bar{\xi}}-\bar{\bar{\eta}})^2 = (\bar{\mu}-\bar{\nu})^2 + (\bar{\bar{\mu}}-\bar{\bar{\nu}})^2.$$

It is now obvious to anyone familiar with the elements of analytic geometry that whenever Φ is true then Φ^* is true, and conversely. And since we can always decide in a mechanical way about the truth of Φ^*, we can also do this for Φ.

The decision method just outlined applies with obvious changes to Euclidean geometry of any number of dimensions[18]. And, since it depends exclusively on the possibility of introducing into geometry a system of real coordinates, it will apply as well to various systems of non-Euclidean and projective geometry[19].

We can attempt to extend the results concerning elementary algebra in still another way: in fact, by introducing into the system of algebra new mathematical terms which cannot be defined by means of those occurring in the original system. The new terms may denote certain properties of numbers, certain relations between numbers, or certain operations on numbers (in particular, unary operations — i.e., functions of one real variable). In consequence of any such extension of the original system we are presented with a new decision problem. In some cases, from the results known in the literature it easily follows that the solution of the problem is negative — i.e., that no decision method for the enlarged system can ever be found, and that no decision machine can be constructed. In view of the Gödel-Church-Rosser result mentioned in the Introduction, this applies, for instance, if we introduce into the system of real algebra the predicate *In*, to denote the property of being an integer (so that $In(x)$ is read: "x in an integer"); and, by the result of Mrs. Robinson, the same applies to the predicate *Rt*, denoting the property of being rational. The situation is still the same if we introduce a symbol for some periodic function, for instance, *sine*; this is seen if only from the fact that the notion of an integer and of a rational number can easily be defined in terms of *sine* and the notions of our original system; thus we can say that x is a rational if and only if it satisfies the formula

$$(Ey)(Ez)\left[(x\cdot y = z)\wedge\sim(y = 0)\wedge(\sin y = 0)\wedge(\sin z = 0)\right].$$

In other cases, by introducing a new symbol we arrive at a system for which the decision problem is open. This applies, for instance, to the system obtained by introducing the operation of exponentiation (of course restricted to the cases where it yields a definite real result), or — what amounts essentially to the same thing — the symbol *Exp* to denote an exponential with a fixed base, for example, 2[20]. The decision problem for the system just mentioned is of a great theoretical and practical interest. But its solution seems to present considerable difficulties. These difficulties appear, however, to be of a purely mathematical (not logical) nature: they arise from the fact that our knowledge of conditions for the solvability of equations and inequalities in the enlarged system is far from adequate[21].

In this connection it may be worth while to mention that by introducing the operation of exponentiation into the system of elementary complex algebra, we arrive at a system for which the solution of the decision problem is negative. In fact it is well known that the exponential function in the complex domain is periodic, and hence, like the function *sine* in the real domain, it allows us to define the notion of an integer.

NOTES

1. When dealing with theories presented as formal axiomatized systems, one often uses the term "decision method" for a theory in a different sense, by referring it to the class, not of all true sentences, but of all theorems of the theory: i.e., of all sentences of the theory which can be derived from the axioms by means of certain prescribed rules of inference.

2. See Löwenheim [11], Post [14], Langford [10], Presburger [15], and McKinsey [12]. (The numbers in square brackets refer to items in the Bibliography following these Notes.) The results of Tarski and Mrs. Szmielew are unpublished.

3. See Gödel [4], Church [3], and Rosser [16]. The results of Mostowski, Tarski, and Mrs. Robinson are unpublished.

4. This result was mentioned, though in an implicit form and without proof, in Tarski [19], pp.233 and 234; see also Tarski [22]. Some partial results tending in the same direction — e.g., decision methods for elementary algebra with addition as the only operation, and for the geometry of the straight line — are still older, and were obtained by Tarski and presented in his university lectures in the years 1926-1928; cf. Presburger [15], p.95, footnote 4, and Tarski [21], p.324, footnote 53.

5. In this connection A. Mostowski has pointed out the following. Although the general concept of an integer is lacking in our system of elementary algebra, yet it can easily be shown that a "general arithmetic" in the sense of Carnap [2], p.206, is "contained" in this system. Since the language in question is consistent and decidable (again in the sense of Carnap [2], pp.207 and 209), it provides an example against Carnap's assertion that "every consistent language which contains a general arithmetic is irresoluble" (*ibid.*, p.210). Carnap's definition of the phrase "contains a general arithmetic" is therefore certainly too wide.

6. Among the works listed in the Bibliography, Hilbert-Bernays [7] may be consulted for various logical and metamathematical notions and results involved in our discussion, and van der Waerden [23] will provide necessary information in the domain of algebra.

7. In this monograph we establish certain results concerning various mathematical theories, such as elementary algebra and elementary geometry. Hence our discussion belongs to the general theory of mathematical theories: i.e., to what is called "metamathematics". To give our discussion a precise form we have to use various metamathematical symbols and notions. Since, however, we do not want to create any special difficulties for the reader, we apply the following method: when referring to individual symbols of the mathematical theory being discussed, or to expressions involving these symbols, we use the symbols and expressions themselves. We could thus say that the symbols and expressions play in our discussion the role of metamathematical constants. On the other

hand, when referring to arbitrary symbols and expressions, or to arbitrary expressions of a certain form, we use special metamathematical variables. In fact, small Greek letters, as for instance "α", "β", "γ", are used to represent arbitrary terms, and in particular the letters "ξ", "η", "λ", "μ", "ν", will be used to represent arbitrary variables; on the other hand, Greek capitals "Φ", "Θ", "Ψ" will be used to represent arbitrary formulas and sentences. With these exceptions we do not introduce any special metamathematical symbolism. Various metamathematical notions whose intuitive meaning is clear will be used without any explanation; this applies, for instance, to such a phrase as "the variable ξ occurs in the formula Φ." Also, we do not consider it necessary to set up an axiomatic foundation for our metamathematical discussion, and we avoid a strictly formal exposition of metamathematical arguments. We assume that we can avail ourselves in metamathematics of elementary number theory; we use variables "m", "n", "p", and so on to represent arbitrary integers; and we employ the ordinary notation for individual integers, arithmetical relations between integers, and operations on them.

The reader who is interested in the deductive foundations, and a precise development, of metamathematical discussion, may be referred to Carnap [2] (part II, pp.55 ff.), Gödel [4], Tarski [21] (Section 2, pp.279 ff., in particular p.289), and Tarski [20] (especially p.100).

8. In choosing symbols for the formalized system of algebra, we have been interested in presenting the metamathematical results in the simplest possible form. For this reason we have not introduced into the system various mathematical and logical symbols which are ordinarily used in expressing mathematical theorems: such as the subtraction symbol "-", the symbol "<", the implication sign "$\rightarrow$", the equivalence sign "$\leftrightarrow$", and the universal quantifier "A". Nevertheless, some of these symbols are made available for our use, since they are introduced as metamathematical abbreviations. If we wished, we could reduce the number of symbols still further; we could, for instance, dispense with the ">" sign, by treating

$$x > y$$

merely as an abbreviation for

$$(Ez)\left[\sim(z = 0) \wedge (x = y + z^2)\right].$$

In an analogous way we could dispense with the symbols 0, 1, and -1, and with one of the two logical connectives $\vee$ and $\wedge$. But such a reduction in the number of symbols would hardly be advantageous from our point of view.

It should be pointed out that, in order to increase the efficiency of the decision machine which may be constructed on the basis of this monograph, it might very well turn out to be useful to enrich the symbolism of our system, even if this carried with it certain complications in the description of the decision method.

9. A formal definition of truth can be found in Tarski [21]. It should be pointed out that we can eliminate the notion of truth from our whole discussion by subjecting the system of elementary algebra to the process of axiomatization. For this purpose, we single out certain sentences of our system which

we call "axioms". They are divided into logical and algebraic axioms. The logical axioms (or rather, axiom schemata) are those of the sentential calculus and the lower predicate calculus with identity; they can be found, for instance, in Hilbert-Bernays [7] (see sections 3, 4 and 5 in vol.1, and supplement 1 in vol.2). Among algebraic axioms we find, in the first place, those which characterize the set of real numbers as a commutative ordered field with the operations + and · and the relation >, and which single out in a familiar way the three special elements 0, 1, and -1. These axioms are supplemented by one additional axiom schema comprehending all sentences of the form

$$\text{(i)}\qquad (A\xi_1)\ldots(A\xi_n)(A\eta)(A\zeta)\Big\{\Big[(\eta > \zeta) \wedge (E\xi)\big((\xi = \eta) \wedge (\alpha > 0)\big) \wedge (E\xi)\big((\xi = \zeta) \wedge (0 > \alpha)\big)\Big] \rightarrow (E\xi)\big((\eta > \xi) \wedge (\xi > \zeta) \wedge (\alpha = 0)\big)\Big\}.$$

where $\xi_1, \ldots, \xi_n$, η, ζ are arbitrary variables, ξ is any variable different from η and ζ, and α is any term — which, in the non-trivial cases, of course involves the variable ξ. Intuitively speaking, this axiom schema expresses the fact that every function which is represented by a term of our symbolism (i.e., every rational integral function) and which is positive at one point and negative at another, vanishes at some point in between.

From what can be found in the literature (see van der Waerden [23], in particular pp. 235 f.), it is seen that this axiom schema can be equivalently replaced by the combination of an axiom expressing the fact that every positive number has a square root, with an axiom schema comprehending all sentences to the effect that every polynomial of odd degree has a zero: i.e., all sentences of the form

$$\text{(ii)}\qquad (A\eta_0)(A\eta_1)\ldots(A\eta_{2n+1})\Big[\sim(\eta_{2n+1} = 0) \rightarrow (E\xi)\big(\eta_0 + \eta_1\xi + \ldots + \eta_{2n+1}\xi^{2n+1} = 0\big)\Big],$$

where η_0, $\eta_1, \ldots, \eta_{2n+1}$ are arbitrary variables, and ξ is any variable different from all of them. It is also possible to use, instead of (ii), a schema comprehending all sentences to the effect that every polynomial of degree at least three has a quadratic factor. Finally, it turns out to be possible to replace equivalently schema (i) by the seemingly much stronger axiom schema comprehending all those particular cases of the continuity axiom which can be expressed in our symbolism. (By the continuity axiom we may understand the statement that every set of real numbers which is bounded above has a least upper bound; when expressing particular cases of this axiom in our symbolism, we speak, not of elements of a set, but of numbers satisfying a given formula.) The possibility of this last replacement, however, is a rather deep result, which is a by-product of other results presented in this work: in fact, of those discussed below in Note 15.

After having selected the axioms, we describe the operations by means of which new sentences can be derived from given ones. These operations are expressed in the so-called "rules of inference" familiar from mathematical logic. A sentence which can be derived from axioms by repeated applications of the rules of inference is called a provable sentence. In our further discussion — in particular, in defining the notions of equivalence of terms and equivalence of formulas — we replace everywhere the notion of a true sentence by that of a provable one. Hence, when establishing certain of the results given later — in particular, the theorems about equivalent formulas — we have to show that the sentences involved are formally derivable from the selected axioms (and not that they are true in any intuitive sense); otherwise the discussion does not differ from that in the text.

10. We use the term "decision method" here in an intuitive sense, without giving a formal definition. Such a procedure is possible because our result is of a positive character: we are actually going to establish a decision method, and no one who understands our discussion will be likely to have any doubt that this method enables us to decide in a finite number of steps whether any given sentence of elementary algebra is true. The situation changes radically, however, if one intends to obtain a result of a negative character — i.e., to show for a given theory that no decision method can be found; a precise definition of a decision method then becomes indispensable. The way in which such a definition is to be given is of course known from the contemporary literature. Using one of the familiar methods — for instance the method due to Gödel — one establishes a one-to-one correspondence between expressions of the system and positive integers, and one agrees to treat the phrase "there exists a decision method for the class A of expressions" as equivalent with the phrase "the set of numbers correlated with the expressions of A is general recursive." (When the set of numbers correlated with a class A of sentences is general recursive, we sometimes say simply that A is general recursive.) For a discussion of the notion of general recursiveness, see Hilbert-Bernays [7] and Kleene [8].

11. The method of eliminating quantifiers occurs in a more or less explicit form in the papers Löwenheim [11] (section 3), Skolem [18] (section 4), Langford [10], and Presburger [15]. In Tarski's university lectures for the years 1926-1928 this method was developed in a general and systematic way; cf. Presburger [15], p.95, footnote 4, and p.97, footnote 1.

12. The results obtained in Theorems 27 and 29, and culminating in Theorem 31, seem to deserve interest even from the purely mathematical point of view. They are closely related to the well-known theorem of Sturm, and in proving them we have partly used Sturm's methods.

The theorem most closely related to Sturm's ideas is Theorem 27. In fact, by analyzing, and slightly generalizing, the proof of this theorem we arrive at the following formulation. Let α and β be any two polynomials in a variable ξ, and κ and μ any two real numbers with $\kappa < \mu$. We construct a sequence of polynomials $\gamma_1, \gamma_2, \dots, \gamma_n$ — which may be called the Sturm chain for α and β — by taking α for γ_1, β for γ_2, and assuming that γ_i, with $i > 2$, is the negative remainder of γ_{i-2} and γ_{i-1}; we discontinue the construction when we reach a polynomial γ_n which is a divisor of γ_{n-1}. Let $\kappa_1, \dots, \kappa_n$ and $\mu_1, \dots, \mu_n$ be the sequences of values of $\gamma_1, \dots, \gamma_n$ at $\xi = \kappa$ and $\xi = \mu$, respectively; let k be the number of changes in sign of the sequence $\kappa_1, \dots, \kappa_n$, and let m be the number of changes in sign of the sequence $\mu_1, \dots, \mu_n$. Then it turns out that k-m is just the number $g(\alpha,\beta)$ defined as in the proof of Theorem 27, but with the roots assumed to lie between κ and μ. (In Theorem 27 we were dealing, not with the arbitrary interval (κ,μ), but with the interval $(-\infty, +\infty)$.)

Sturm himself considered two particular cases of this general theorem: the case where β is the derivative of α — when the number k-m proves to be simply the number of distinct roots of α in the interval (κ,μ); and the case where β is arbitrary but α is a polynomial without multiple roots — when k-m proves to be the difference between the number of roots of α at which β agrees in sign with the derivative of α, and the number of roots of α at which β disagrees in sign with the derivative of α — the roots being taken from the interval (κ,μ). These two special cases easily follow from the theorem, and we have made an essential use of this fact in the proof of Theorem 29. The general formulation was found recently by J.C.C. McKinsey; it contributed to a simplification, not of the original decision method itself, but of its mathematical description.

Apart, however, from technicalities connected with the notion and construction of Sturm chains, the mathematical content of Sturm's theorem essentially consists in the following: given any algebraic equation in one variable x, and with the coefficients a_0, $a_1,\ldots,$ a_n, there is an elementary criterion for this equation to have exactly k real solutions (which may be in addition subjected to the condition that they lie in a given interval): such a criterion is obtained by constructing a certain finite sequence of systems, each consisting of finitely many equations and inequalities which involve the coefficients a_0, $a_1,\ldots,$ a_n of the given equation (and possibly the end-points b and c of the interval); it is shown that the equation has exactly k roots if and only if its coefficients satisfy all the equations and inequalities of at least one of these systems. (When applied to an equation with constant coefficients, the criterion enables us actually to determine the number of roots of the equation, but this is only a by-product of Sturm's theorem.) By applying Sturm's theorem we obtain in particular an elementary condition for an algebraic equation in one unknown to have at least one real solution. Theorem 31 gives directly an extension of this special result to an arbitrary system of algebraic equations and inequalities with arbitrarily many unknowns. It is easily seen, however, that from our theorem one can obtain stronger consequences: in fact, criteria for such systems to have exactly k real solutions. To clear up this point, let us consider the simple case of a system consisting of one equation in two unknowns

$$F(x,y) = 0 \quad . \tag{i}$$

We form the following system of equations and inequalities

$$\left\{\begin{array}{l} F(x,y) = 0 \\ F(x',y') = 0 \\ (x - x')^2 + (y - y')^2 > 0 \quad . \end{array}\right. \tag{ii}$$

By Theorem 31 we have an elementary criterion for the system (ii) to have at least one solution. But it is obvious that this criterion is at the same time a criterion for (i) to have at least two solutions. In the same way, we can obtain criteria for (i) to have at least 3,4,..., k real solutions. Hence we also obtain a criterion for (i) to have exactly k solutions (since an equation has exactly k solutions if it has at least k, but not at least k + 1, solutions).

The situation does not change if the solutions are required to satisfy additional conditions — namely, to lie within given bounds. We can thus say that *Theorem 31 constitutes an extension of Sturm's theorem* (or, at least, of the essential part of this theorem) *to arbitrary systems of equations and inequalities with arbitrarily many unknowns.*

It may be noticed that by Sturm's theorem a criterion for solvability (in the real domain) involves systems which contain inequalities as well as equations. Hence, to obtain an extension of this theorem to systems of equations in many unknowns, it seemed advisable to consider inequalities from the beginning, and in the first step to extend the theorem to arbitrary systems of equations and inequalities in one unknown. As a result of this preliminary extension, the subsequent induction with respect to the number of unknowns becomes almost trivial.

In its most general form the mathematical result obtained above seems to be new, although, in view of the extent of the literature involved, we have not been able to establish this fact with absolute certainty. At any rate some precedents are known in the literature. From what can be found in Sturm's original paper, the extension of his result to the case of one equation and one inequality with one unknown can easily be obtained; Kronecker, in his theory of characteristics, concerned himself with the case of n (independent) equations with n unknowns. It seems, on the other hand, that such a simple problem as that of finding an elementary criterion for the solvability in the real domain of one equation in two unknowns has not been previously treated; the same applies to the case of a system of inequalities (without equations) in one unknown — although this case is essential for the subsequent induction. (Cf. in this connection, Weber [24], pp.271 ff., and Runge [17], pp.416 ff., where further references to the literature are also given.)

13. The result established in Theorem 31 and discussed in the preceding note has various interesting consequences. To formulate them, we can use, for instance, a geometric language and refer the result to n-dimensional analytic space with real coordinates — or, what is slightly more convenient, to the infinite-dimensional space S_ω, in which, however, every point has only finitely many coordinates different from zero. By an elementary algebraic domain in S_ω we understand the set of all points $\langle x_0, x_1, \dots, x_n, \dots \rangle$ in which the coordinates $x_{k_1}, x_{k_2}, \dots, x_{k_m}$ satisfy a given algebraic equation or inequality

$$F\left(x_{k_1}, \dots, x_{k_m}\right) = 0$$

or

$$F\left(x_{k_1}, \dots, x_{k_m}\right) > 0 \ ,$$

and the remaining coordinates are zeros. Let $\mathfrak{J}$ be the smallest family of point sets in S_ω which contains among its elements all elementary algebraic domains and is closed under the operations of finite set-addition, finite set-multiplication, set-complementation, and projection parallel to any axis. (The projection of a set A parallel to the n^{th} axis is the set obtained by replacing by zero the n^{th} coordinate of every point of A.) Now Theorem 31 in geometric formulation implies that the family $\mathfrak{J}$ consists of those and only those sets in S_ω which are finite sums of finite products of elementary algebraic domains. The possibility of passing from the original formulation to the new one is a consequence of the known relations between projection and existential quantifiers.

Theorem 31 has also some implications concerning the notion of arithmetical (or elementary) definability. A set A of real numbers is called arithmetically definable if there is a formula Φ in our system containing one free variable and such that A consists of just those numbers which satisfy Φ. In a similar way we define an arithmetically definable binary, ternary, and in general an n-ary, relation between real numbers. Now Theorem 31 gives us a simple characterization of those sets of real numbers, and relations between real numbers, which are arithmetically definable. We see, for instance, that a set of real numbers is arithmetically definable if and only if it is a set-theoretical sum of a finite number of intervals (bounded, or unbounded; closed, open, or half-closed, half-open) with algebraic end-points; in particular, a real number (i.e., the set consisting of this number alone) is arithmetically definable if and only if it is algebraic. Hence it follows that an arithmetically definable set of real numbers which is bounded above has an arithmetically definable least upper bound — a consequence which is relevant in connection with a result mentioned near the end of Note 9. As further consequences we conclude that the sets of all integers, of all rationals, etc., are not arithmetically definable, which justifies some remarks made in the Introduction.

As a simple corollary of Theorem 31 we obtain: For every formula Φ there is an equivalent formula Ψ with the same free variables of the following form:

$$\Psi \equiv (E\xi_1)\ldots(E\xi_n)\left[\alpha = 0\right] .$$

This corollary can also be interpreted geometrically.

For the notions used in this note, cf. Tarski [19] and Kuratowski-Tarski [9].

14. In other words, using terminology introduced in Note 10, we state that the number-theoretic function correlated with WU is general recursive. Actually this function is easily seen to be a general recursive function of a very simple type — what is called a "primitive" recursive function.

15. If we take the axiomatic point of view outlined in Note 9 and replace in our whole discussion the notion of truth by that of provability, then the meaning and extent of the fundamental results obtained in Section 2 undergo some essential changes. In the new interpretation, Theorem 36 implies that every sentence of elementary algebra is provably equivalent to one of the sentences $0 = 0$ or $0 = 1$. In addition, we can easily show that $WU(\Phi) \equiv (0 = 0)$ if and only if $WU(\sim\Phi) \equiv (0 = 1)$, and that for any provable sentence Φ we have $WU(\Phi) \equiv (0 = 0)$. By combining these results, we arrive at the conclusion that the axiomatic system of elementary algebra is consistent and complete, in the sense that one and only one of any pair Φ and $\sim\Phi$ of contradictory sentences is provable. The proof of this fact has what is called a constructive character. The completeness of the system implies by itself the existence of a decision method for the class of all provable sentences (even without the knowledge that the number-theoretical function correlated with WU is general recursive); cf. Kleene [8].

We further notice that all the axioms listed in Note 9 are satisfied, not only by real numbers, but by the elements of any real closed field in the sense of Artin and Schreier (cf. van der Waerden [23], chapter IX). Thus all the results just mentioned can be extended to the elementary theory of real closed fields. From the fact that this theory is complete it follows that there is no sentence expressible in our formal system of elementary algebra which would hold in one real closed field and fail in another. In other words, any arithmetically definable property (in the sense of Note 13) which applies to one real closed field also applies to all other such fields: i.e., any two real closed fields are arithmetically indistinguishable.

In general, when applied to axiomatized theories, the notions of truth and provability do not have the same extension. Usually it can be shown only that every provable sentence is true. Since, however, in the case of elementary algebra the class of provable sentences turns out to be complete, we conclude that in this particular case the converse holds, and hence that the two classes coincide. Thus in the case of elementary algebra three equivalent definitions of a true sentence are available: (i) the definition of a true sentence as a sentence Φ such that $WU(\Phi) \equiv (0 = 0)$; (ii) the definition of a true sentence as a provable sentence; (iii) the definition based on the general method of defining truth developed in Tarski [21]. Correspondingly, when starting to develop elementary algebra, we have three methods of stipulating which sentences will be accepted in this algebra — i.e., recognized as true. Apart from any educational and psychological considerations, the first method has in principle a great advantage: it implies directly that the class of sentences recognized as true is general recursive. Hence it provides us from the beginning with a mechanical device to decide in each particular case whether a sentence should be accepted, and serves as a basis for the construction of a decision machine. The second method — which is the usual axiomatic method — is less advantageous: it has as a direct consequence only the fact that the class of sentences recognized as true is what is called recursively enumerable (not necessarily general recursive). It leads to the construction of a machine which would be much less useful — to a machine which would construct, so to speak, blindly, the infinite sequence of all sentences accepted as true, without being able to tell in advance whether a given sentence would ever appear in this sequence. The third method, though very important for certain theoretical considerations, is even less advantageous than the second. It does not show that the class of accepted sentences is recursively enumerable; it can hardly be applied to a practical construction of a theory unless it is combined on a metamathematical level with the first or the second method. It goes without saying that in the particular case with which we are concerned — that is, in the case of elementary algebra — by establishing the equivalence of these possible definitions of truth we have *eo ipso* shown that in this case the three methods determine eventually the same class of sentences.

16. We can also consider a more restricted elementary system of complex algebra, from which the symbols > and *Rl* have been eliminated. The decision method applies to such a system as well, and even becomes much simpler. By taking the axiomatic point of view and basing the discussion on the notion of provability, we can carry over to this restricted system of complex algebra all the results pointed out in Note 15. Since the axioms of this system prove to

be satisfied by elements of an arbitrary algebraic closed field with characteristic zero (thus, in particular, by the complex algebraic numbers), the results apply to the general elementary theory of such fields; in particular, any two algebraic closed fields with characteristic zero turn out to be arithmetically indistinguishable. A slight change in the argument permits us further to extend the results just mentioned to algebraic closed fields with any given characteristic p. (For these notions, cf. van der Waerden [23], chapter 5.)

On the other hand, as was mentioned in the Introduction, no decision method can be given for the arithmetic of rationals, nor for the elementary theory of arbitrary fields. For most special fields the decision problem still remains open. This applies, for instance, to finite algebraic extensions of the field of rational numbers and to the field of all numbers expressible by means of radicals. It would be interesting to solve the decision problem for some of these special fields, or even to obtain a simple mathematical characterization of all those fields for which the solution of the decision problem is positive.

17. As in the case of elementary algebra (see Note 8), some of the symbols listed could be eliminated from the system of elementary geometry and treated merely as abbreviations. It is known, for example, that in n-dimensional geometry with $n \geq 2$ the symbol "B" of the betweenness relation can be defined in terms of the symbol "D" of the equidistance relation.

18. Exactly as in the case of elementary algebra, we can treat the system of elementary geometry in an axiomatic way, and base our discussion of the decision problem on the notion of provability. If we restrict ourselves to the case of two dimensions, we can take, for instance (in addition to the general logical axioms mentioned in Note 9), the following geometrical axioms:

(i) $(Ax)(Ay)B(x,y,y)$:

(ii) $(Ax)(Ay)\left[B(x,y,x) \longrightarrow (x = y)\right]$;

(iii) $(Ax)(Ay)(Az)\left[B(x,y,z) \longrightarrow B(z,y,x)\right]$;

(iv) $(Ax)(Ay)(Az)(Au)\left\{\left[B(x,y,u) \wedge B(y,z,u)\right] \longrightarrow B(x,y,z)\right\}$;

(v) $(Ax)(Ay)(Az)(Au)\left\{\left[B(x,y,z) \wedge B(y,z,u) \wedge \sim(y = z)\right] \longrightarrow B(x,y,u)\right\}$;

(vi) $(Ax)(Ay)(Az)(Au)\left\{\left[B(x,y,u) \wedge B(x,z,u)\right] \longrightarrow \left[B(x,y,z) \vee B(x,z,y)\right]\right\}$;

(vii) $(Ax)(Ay)(Az)(Au)\left\{\left[B(x,y,z) \wedge B(x,y,u) \wedge \sim(x = y)\right] \longrightarrow \right.$
$\left. \left[B(x,z,u) \vee B(x,u,z)\right]\right\}$;

(viii) $(Ex)(Ey)(Ez)\left[\sim B(x,y,z) \wedge \sim B(y,z,x) \wedge \sim B(z,x,y)\right]$;

(ix) $(Ax)(Ay)(Az)(Az')(Au)\left\{\left[B(x,z',z) \wedge B(y,z,u)\right] \longrightarrow \right.$
$\left. (Ey')\left[B(x,y',y) \wedge B(y',z',u)\right]\right\}$;

$$\text{(x)}\quad \begin{aligned}&(Ax)(Ay)(Az)(Az')(Au)\Big\{\big[B(x,z,z')\wedge B(y,z,u)\wedge\sim(x=z)\big]\longrightarrow\\&\qquad (Ey')(Eu')\big[B(x,y,y')\wedge B(x,u,u')\wedge B(y',z',u')\big]\Big\};\end{aligned}$$

$$\text{(xi)}\quad \begin{aligned}&(Ax)(Ay)(Az)(Au)(Ev)\Big\{\big[\big(B(x,u,v)\vee B(u,v,x)\vee B(v,x,u)\big)\wedge B(y,v,z)\big]\vee\\&\qquad\big[\big(B(y,u,v)\vee B(u,v,y)\vee B(v,y,u)\big)\wedge B(z,v,x)\big]\vee\\&\qquad\big[\big(B(z,u,v)\vee B(u,v,z)\vee B(v,z,u)\big)\wedge B(x,v,y)\big]\Big\};\end{aligned}$$

$$\text{(xii)}\quad (Ax)(Ay)\,D(x,y;y,x)$$

$$\text{(xiii)}\quad (Ax)(Ay)(Az)\big[D(x,y;z,z)\longrightarrow(x=y)\big]$$

$$\text{(xiv)}\quad (Ax)(Ay)(Az)(Au)(Av)(Aw)\Big\{\big[D(x,y;z,u)\wedge D(x,y;v,w)\big]\longrightarrow D(z,u;v,w)\Big\};$$

$$\text{(xv)}\quad \begin{aligned}&(Ax)(Ay)(Az)(Az')(Au)\Big\{\big[\sim(x=y)\wedge D(x,z;x,z')\wedge D(y,z;y,z')\wedge\\&\qquad B(y,u,z')\wedge\big(B(x,u,z)\vee B(x,z,u)\big)\big]\longrightarrow(z=z')\Big\};\end{aligned}$$

$$\text{(xvi)}\quad \begin{aligned}&(Ax)(Ax')(Ay)(Ay')(Az)(Az')(Au)(Au')\Big\{\big[D(x,y;x',y')\wedge D(y,z;y',z')\wedge\\&\qquad D(x,u;x',u')\wedge D(y,u;y',u')\wedge\\&\qquad B(x,y,z)\wedge B(x',y',z')\wedge\\&\qquad \sim(x=y)\wedge\sim(y=z)\big]\longrightarrow D(z,u;z',u')\Big\};\end{aligned}$$

$$\text{(xvii)}\quad (Ax)(Ay)(Ay')(Az')(Ez)\Big\{B(x,y,z)\wedge D(y,z;y',z')\Big\};$$

$$\text{(xviii)}\quad \begin{aligned}&(Ax)(Ax')(Ay)(Ay')(Az')(Av)\Big\{D(x,y;x',y')\longrightarrow\\&\qquad (Ez)(Eu)\big[D(x,z;x',z')\wedge D(y,z;y',z')\wedge B(z,u,v)\wedge\\&\qquad \big(B(x,y,u)\vee B(y,u,x)\vee B(u,x,y)\big)\big]\Big\}.\end{aligned}$$

To these is added the axiom schema which comprehends all particular cases of the axiom of continuity (e.g., in the Dedekind form) that are expressible in our system: i.e., all sentences of the following form:

$$\text{(xix)}\quad \begin{aligned}&(A\xi_1)\ldots(A\xi_n)\Big\{(E\mu)(A\eta_1)(A\eta_2)\big[(\Phi\wedge\Psi)\longrightarrow B(\mu,\eta_1,\eta_2)\big]\longrightarrow,\\&\qquad (E\mu)(A\eta_1)(A\eta_2)\big[(\Phi\wedge\Psi)\longrightarrow B(\eta_1,\mu,\eta_2)\big]\Big\},\end{aligned}$$

where neither μ nor η_2 is free in the formula Φ, and neither μ nor η_1 is free in the formula Ψ.

The reader will notice the formal simplicity of most of the axioms just given— which we have tried to put into evidence by avoiding (contrary to the prevailing custom) the use of any defined terms in formulating the axioms. On the other hand, however, the reader will easily recognize a close similarity between our axiom system and various systems which can be found in the comprehensive literature of the foundations of geometry; see, e.g., Hilbert [6].

By means of some obvious changes in (viii) and (xi) one can obtain from this axiom system a system of axioms for elementary geometry of any number of dimensions.

Again as in the case of algebra, one of the achievements attained by the axiomatic treatment of the subject is a constructive consistency proof for the whole of elementary geometry. This improves a result to be found in Hilbert-Bernays [7] (vol.2, pp. 38 ff.). It may also be mentioned that in Hilbert [6] (section 35, pp. 96-98) a result is given which is closely connected with the decision method for elementary geometry, but which has a rather restricted character.

19. As is known, ordinary projective geometry can be treated as a specialized branch of lattice theory — more specifically, of the theory of modular lattices: see Birkhoff [1], where references to earlier papers of Menger can also be found. The decision method applies to this branch of the theory of modular lattices as well.

20. In the axiomatic presentation, the introduction of the new symbol *Exp* would require the addition of new axioms. The following three axioms can be used, for instance, for this purpose:

$$(Ax)(Ay)\Big[(x > y) \longrightarrow (Exp(x) > Exp(y))\Big]$$

$$(Ax)(Ay)\Big[(Exp(x)\cdot Exp(y)) = Exp(x + y)\Big]$$

$$Exp(1) = 1 + 1.$$

21. Similar decision problems arise if we introduce into our system of elementary algebra the symbol *Al* to denote the property of being an algebraic number, or the symbol *Cn* to denote the property of being a constructible number (i.e., a number which can be obtained from the number 1 by means of the rational operations, together with the operation of extracting square roots). If the solution of the decision problem for elementary algebra with the addition of the symbol *Cn* were positive, this result would have an interesting application for geometry: in fact, we should obtain a decision method which would enable us, not only to decide on the truth of every sentence of elementary geometry, but also — in the case of existential sentences (like the sentence stating the possibility of trisecting an arbitrary angle) — to decide whether the truth of such a sentence can be established using only the so-called elementary constructions: i.e., constructions by means of rule and compass. It seems unlikely, however, that the solution of the problem in question is indeed positive; probably we shall be able to show that such a sharper decision method for elementary geometry cannot be found.

BIBLIOGRAPHY

[1] Birkhoff, G., *Lattice theory.* [American Mathematical Society Colloquium publications, vol. 25.] Revised edition, New York, 1948.

[2] Carnap, R., *The logical syntax of language.* New York and London, 1937.

[3] Church, A., "An unsolvable problem of elementary number theory". *American journal of mathematics,* vol. 58, pp. 345-363, 1936.

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

[5] Herbrand, J., *Recherches sur la théorie de la démonstration.* [Prace Towarzystwa Naukowego Warszawskiego, Wydział III, no. 33.] Warsaw, 1930.

[6] Hilbert, D., *Grundlagen der Geometrie.* Seventh edition, Leipzig and Berlin, 1930.

[7] Hilbert, D., and Bernays, P., *Grundlagen der Mathematik.* Vol. 1, Berlin, 1934; vol. 2, Berlin, 1939.

[8] Kleene, S. C., "General recursive functions of natural numbers". *Mathematische Annalen,* vol.112, pp. 727-742, 1935-1936.

[9] Kuratowski, C., and Tarski, A., "Les opérations logiques et les ensembles projectifs". *Fundamenta mathematicae,* vol. 17, pp. 240-248, 1931.

[10] Langford, C. H., "Some theorems on deducibility". *Annals of mathematics,* vol. 28, pp. 16-40, 1926-1927. "Theorems on deducibility (second paper)". *Ibid.,* pp. 459-471.

[11] Löwenheim, L., "Über Möglichkeiten im Relativkalkül". *Mathematische Annalen,* vol. 76, pp. 447-470, 1915.

[12] McKinsey, J. C. C., "The decision problem for some classes of sentences without quantifiers". *Journal of symbolic logic,* vol. 8, pp. 61-76, 1943.

[13] Pieri, M., "La geometria elementare instituita sulle nozioni di 'punto' e 'sfera' ". *Memorie di matematica e di fisica della Società Italiana delle Scienze,* ser. 3, vol. 15, pp. 345-450, 1908.

[14] Post, E. L., "Introduction to a general theory of elementary propositions". *American journal of mathematics,* vol. 43, pp. 163-185, 1921.

[15] Presburger, M., "Über die Vollständigkeit eines gewissen Systems der Arithmetik ganzer Zahlen, in welchem die Addition als einzige Operation hervortritt". *Sprawozdanie z I Kongresu Matematyków Krajów Słowiańskich,* pp. 92-101 and 395, Warsaw, 1930.

[16] Rosser, B., "Extensions of some theorems of Gödel and Church". *Journal of symbolic logic*, vol. 1, pp. 87-91, 1936.

[17] Runge, C., "Separation und Approximation der Wurzeln". *Encyklopädie der mathematischen Wissenschaffen mit Einschluss ihrer Anwendungen*, vol. 1, pp. 404-448, Leipzig, 1898-1904.

[18] Skolem, T., *Untersuchungen über die Axiome des Klassenkalküls und über Produktations - und Summationsprobleme, welche gewisse Klassen von Aussagen betreffen.* [Skrifter utgit av Videnskapsselskapet i Kristiania, I. klasse 1919, no. 3.] Oslo, 1919.

[19] Tarski, A., "Sur les ensembles définissables de nombres réels I". *Fundamenta mathematicae*, vol. 17, pp. 210-239, 1931.

[20] Tarski, A., "Einige Betrachtungen über die Begriffe der ω-Widerspruchsfreiheit und der ω-Vollständigkeit". *Monatshefte für Mathematik und Physık*, vol. 40, pp. 97-112, 1933.

[21] Tarski, A., "Der Wahrheitsbegriff in den formalisierten Sprachen". *Studia philosophica*, vol. 1, pp. 261-405, 1936.

[22] Tarski, A., "New investigations on the completeness of deductive theories". (Abstract.) *Journal of symbolic logic*, vol. 4, p. 176, 1939.

[23] van der Waerden, B. L., *Moderne Algebra*. Second edition, vol. 1, Berlin, 1937.

[24] Weber, H., *Lehrbuch der Algebra*. Vol. 1, Braunschweig, 1895.

SUPPLEMENTARY NOTES

1. The references to decision methods previously established given on p. 1 and in Note 2, p. 47, were not intended to be complete. For some further results and additional references compare the series of abstracts by Mostowski, Mrs. Szmielew, and Tarski in the *Bulletin of the American Mathematical Society,* vol. 55, pp. 63-66 and 1192, 1949, as well as the following papers:

> Gentzen, G., "Untersuchungen über das logische Schliessen". *Mathematische Zeitschrift,* vol. 39, pp. 176-210, 1934.
>
> McKinsey, J. C. C., "A solution of the decision problem for the Lewis systems S2 and S4, with an application to topology". *Journal of symbolic logic,* vol. 6, pp. 117-134, 1941.
>
> McKinsey, J. C. C., and Tarski, A., "The algebra of topology". *Annals of mathematics,* vol. 45, pp. 141-191, 1944.
>
> Skolem, T., *Über einige Satzfunktionen in der Arithmetik.* [Skrifter utgitt av det Norske Videnskaps-Akademi i Oslo, I. klasse 1930, no. 7.] Oslo, 1931.
>
> Szmielew, W., "Decision problem in group theory". *Proceedings of the Tenth International Congress of Philosophy,* fasc. 2, pp. 763-766, Amsterdam, 1949.

2. The results of Mrs. Robinson, Mostowski, and the author mentioned in the first paragraph of p. 2 appeared in print (some only in outline form) after the first edition of this monograph. See the series of abstracts in the *Journal of symbolic logic,* vol. 14, pp. 75-78, 1949, as well as the article:

> Robinson, J., "Definability and decision problems in arithmetic". *Journal of symbolic logic,* vol. 14, pp. 98-114, 1949.

Some related results can be found in the article:

> Robinson, R. M., "Undecidable rings". *Transactions of the American Mathematical Society,* vol. 70, pp. 137-159, 1951.

3. The following remarks refer to the discussion on pp. 4 and 5. Many examples of open problems in elementary algebra and geometry are known; one comes across discussions of such problems by looking through any issue of the *American mathematical monthly*. However, the problem of describing the behavior of the function *d* does not seem to have been previously treated in the literature. For a discussion of a related problem — involving the decomposition of *P* and *Q,* not in triangles, but in arbitrary polygons — see the following article (where references to earlier papers of Moese and the author can also be found):

> Tarski, A., "Uwagi o stopniu róẇnowaźności wielokatow". (Remarks on the degree of equivalence of polygons, in Polish.) *Parametr,* vol. 2, 1932.

It may be interesting to mention that some conclusions concerning the function *d* can be derived from the general results stated in Note 13, p. 53. In fact, it can be shown that every bounded interval (*a, b*) can be divided into finitely many subintervals such that the function *d* is constant within each of these subintervals; all the endpoints of these subintervals are algebraic, with the possible exception of *a* and *b.*

4. The statement in Note 12, p. 52, to the effect that the case of a system of inequalities in one unknown was not previously treated in the literature, seems to be correct when applied to the situation which existed at the time when the results of this work were found and first mentioned in print (1931), as well as for many years thereafter. However, the author's attention has been called to the fact that this case has recently been treated in the paper:

> Meserve, B. E., "Inequalities of higher degree in one unknown". *American journal of mathematics*, vol. 49, pp. 357-370, 1947.

5. The discussion in Note 13, pp. 52-53, may convey the impression that the notions considered in the first paragraph have but little in common with those considered in the second paragraph. Actually, these notions are very closely related to each other. In fact, if the notion of arithmetical definability is applied to arbitrary sets of sequences of real numbers, i.e., to point sets in S_ω, then the family of all arithmetically definable point sets simply coincides with the family $\mathfrak{J}$.

6. It was stated in Note 13, p. 53, that every real number which is arithmetically definable is algebraic. An interesting application of this result to the theory of games has recently been found by O. Gross and is discussed in his paper "On certain games with transcendental values" (to appear in the *American mathematical monthly*).

7. As was pointed out in Note 15, p. 54, the completeness theorem for elementary algebra leads to the following result: every arithmetically definable property which applies to one real closed field also applies to all other such fields. It is important to realize that the result just mentioned extends to a comprehensive class of properties which are not arithmetically definable (i.e., which are not expressible in our formal system of elementary algebra). This class includes in particular all the properties expressed by sentences of the form $(Am)\Phi_m$, $(Am)(En)\Psi_{m,n}$, . . . where m, n, . . . are variables assumed to range over all positive integers and where Φ_m, $\Psi_{m,n}$, . . . are formulas which involve m, n, . . . (as free variables) and which, for any particular values of m, n, . . ., are equivalent in any real closed fields to sentences of elementary algebra. In fact, consider a sentence of this kind, say, $(Am)\Phi_m$. If this sentence holds in a given real closed field, the same obviously applies to all the particular sentences of the form Φ_m, i.e., to Φ_1, Φ_2, Φ_3 . . . . Each of these particular sentences is equivalent to a sentence of elementary algebra and hence, by the result discussed, it holds in every real closed field. Consequently, the universal sentence $(Am)\Phi_m$ also holds in every real closed field. Various theorems of these types are known which were originally established for the field of real numbers using essentially the continuity of this field (sometimes with the help of difficult topological methods) and whose extension to arbitrary real closed fields presented a new and difficult problem; in view of our general result such an extension now becomes automatic. As examples the following three theorems may be mentioned.

I. *Let R be an m-dimensional region defined as the set of all points $\langle x_0, x_1, \ldots, x_{m-1}\rangle$ satisfying a finite system of inequalities $P_i(x_0, x_1, \ldots, x_{m-1}) \geq 0$ where the P_i's for $i = 0, 1, \ldots, n-1$ are polynomials of degree at most p; let F be a rational function whose denominator does not vanish on R. Then there is a positive integer q (dependent exclusively on m, n, and p) such that the set S of all function* *values of F on R is a sum of at most q closed intervals; if R is bounded, then all these intervals are also bounded, and hence F reaches a maximum and minimum on R.*

II. *For every system of m polynomials $P_0, P_1, \ldots, P_{m-1}$ in m variables there are real numbers $c \geq 0$, $x_0, x_1, \ldots, x_{m-1}$ such that $P_i(x_0, x_1, \ldots, x_{m-1}) = c \cdot x_i$ for $i = 0, 1, \ldots, m-1$.*

III. *Every commutative division algebra — whether associative or not — over the field of real numbers is of order 1 or 2; if it has a unit, it coincides either with the field of real numbers or with the algebraic closure of this field (i.e., with the field of complex numbers).*

While I is simply a particular case of a familiar theorem concerning continuous functions, and the same applies to the "eigenvalue theorem" II, Theorem III has a specifically algebraic character; it was proved, with the help of topology, in the article:

> Hopf, H., "Systeme symmetrischer Bilinearformen und euklidische Modelle der projectiven Räume". *Vierteljahrsschrift der Naturforschenden Gesellschaft in Zürich,* vol. 85, supplement No. 32, pp. 165-177, 1940.

The research to extend these and similar results, obtained by means of topological methods, to arbitrary real closed fields was initiated by H. Hopf. Compare the following papers where partial results in this direction (in particular, extensions of some special cases of Theorem I) have been achieved directly, without the help of our general method:

> Behrend, F., "Über Systeme algebraischer Gleichungen". *Compositio mathematica,* vol. 7, pp. 1-19, 1939.
>
> Habicht, W., "Ein Existenzsatz über reelle definite Polynome". *Commentarii mathematici helvetici,* vol. 18, pp. 331-348, 1946.
>
> Habicht, W., "Über die Lösbarkeit gewisser algebraischer Gleichungssysteme". *Commentarii mathematici helvetici,* vol. 18, pp. 154-175, 1946.
>
> Kaplansky, I., "Polynomials in topological fields". *Bulletin of the American Mathematical Society,* vol. 54, pp. 909-916, 1948.

8. In view of the results stated in Note 16, pp. 54-55, the remarks made in the preceding note will still hold if, instead of real closed fields, we consider the class of algebraically closed fields with a given characteristic.