

SOME INTERCONNECTIONS BETWEEN MODERN ALGEBRA AND MATHEMATICAL LOGIC⁽¹⁾

BY

LEON HENKIN

Mathematical logic originated when mathematical methods were brought to bear on traditional questions of logic, especially the problem of what constitutes a valid proof. For the most part work in this field has remained close to foundational questions. Recent results, however, have indicated the possibility that the methods of mathematical logic may be of use in tackling specific problems in other branches of mathematics. This possibility is illustrated in the present paper, which presupposes no knowledge of mathematical logic.

1. Some concepts of logic. We shall first focus our attention on algebraic structures consisting of a set D on which two binary operations are defined. Rings are familiar examples of such structures; but to begin with we do not make any restrictions on the nature of the binary operations. Instead, we proceed to construct a simple, specialized *language*, L , which can be used to refer to any one of our structures. First we provide two symbols, “+” and “ \cdot ,” to be used as names of the operations. Next we wish to have symbols (called *individual constants*) which can be used as names of particular elements in D . In the case of rings, for example, it is customary to employ the symbols “0” and “1” in this way; for our more general purpose, however, we shall reserve the letter “ v ,” to be used with various distinguishing subscripts. In addition to referring to particular elements of D we wish to make general statements about *all* elements of D , and for this purpose we introduce further symbols “ x ,” “ y ,” “ z ,” “ x_1 ,” “ y_1 ,” \dots (called *individual variables*), which will be used as variables whose range is D . Additional symbols are to include parentheses, an equality sign, and the following words: “not,” “and,” “or,” “if,” “then,” “all,” “exists.”

The symbols of L are used in constructing formulas and sentences as follows. An individual symbol (constant or variable) is called a *term*, and the result of putting a “+” or “ \cdot ” between two terms and enclosing the result in parentheses is also a term. *Basic sentences* are formed by placing an equality sign between two terms, and further *sentences* are built up from these basic ones in the following ways. If A and B are sentences, so are $(\text{not } A)$, $(A \text{ and } B)$,

Received by the editors January 25, 1952.

(¹) The principal ideas of this paper were contained in *The completeness of formal systems*, a doctoral dissertation accepted by Princeton University in October, 1947. In the present version of the paper there are incorporated suggestions of A. Tarski, S. Feferman, and the referee of the original version, for which we express our thanks.

$(A \text{ or } B)$, $(\text{if } A \text{ then } B)$; and if, furthermore, α is any of the individual variables, then $(\text{all } \alpha)A$ and $(\text{exists } \alpha)A$ are also sentences. Example:

$(\text{all } x)(\text{If } ((x \cdot x) \cdot x) = v_1 \text{ then } (x = v_1 \text{ or } (\text{exists } y)((y + y) = v_0 \text{ and } (y \cdot y) = x)))$.

An *interpretation* of L consists of selecting a particular domain D as the range for the variables of L , choosing two specific binary operations on D as denotations for the symbols “+” and “·,” and designating definite elements of D as denotations for each of the individual constants of L . A domain closed under two binary operations will be called a *model*. As soon as such an interpretation has been given, each sentence of L becomes either true or false, according to the familiar way of giving meaning to the sentences⁽²⁾. For example, if D is a ring with unit element, “+” and “·” denote respectively ring addition and multiplication, while “ v_0 ” and “ v_1 ” are assigned as names of 0 and 1 respectively, then the sample sentence given above will be true if and only if every ring element whose third power is unity is either the unit element itself, or else is the square of an element which is its own additive inverse. In general, it is a simple matter in the case of any particular sentence of L to write down a necessary and sufficient condition that it be true, as in the above example. However, it is also possible to give a precise, mathematical definition of what we mean in *general* by a true sentence of L (with respect to an arbitrary interpretation), as was first shown by Tarski⁽³⁾.

We have seen that a sentence of L may be true under certain interpretations and false under others. However, there are some sentences which are true under *every* interpretation, and these are called *valid*. Example:

$$(\text{all } x) (x + x) = (x + x).$$

It might be thought that all valid sentences have such a simple character, and that their validity can be so readily determined in each case that they cannot constitute a mathematically interesting class of sentences. However, this is not so, for it can be proved that there is no algorithm which can decide in a finite number of steps whether an arbitrarily given sentence of L is valid. Furthermore, many outstanding, unsolved problems of mathematics can be reduced to the question of the validity of some sentence of L .

Mathematical logicians have long been interested in systematizing the valid sentences of languages like L , and in providing a criterion whereby their validity could be recognized in specific cases. To this end certain sentences are selected and called *axioms*, and certain *operations* are specified

⁽²⁾ A sentence in which an individual variable occurs *freely* (that is, not within the scope of one of the quantifiers $(\text{all } \alpha)$ or $(\text{exists } \alpha)$) is interpreted as if the quantifier $(\text{all } \alpha)$ were prefixed to the sentence.

⁽³⁾ Alfred Tarski, *Der Wahrheitsbegriff in den formalisierten Sprachen*, *Studia Philosophica* vol. 1 (1936) pp. 261–405. The definition proceeds by induction on the length of the sentence; we shall not give details here.

for deriving one sentence from another (or from several others). The axioms and operations are described without reference to the *meaning* of the sentences of L under interpretation, but rather the description is given in purely *formal* terms⁽⁴⁾.

After the axioms and operations are specified, a *formal proof* is defined to be a (finite) column of sentences each of which is either an axiom, or else arises from preceding elements of the column by one of the specified operations; and the last line of such a formal proof is called a *formal theorem*. If we have chosen as axioms only formulas which we know to be valid, and if we have selected operations which lead only to valid sentences when applied to valid sentences, then a simple argument (involving induction on the length of formal proofs) shows that all formal theorems will be valid. The converse question, whether all valid sentences are formal theorems, is usually much more difficult to answer. A set of axioms and operations sufficient to yield *all* valid sentences as formal theorems is called *complete*. Gödel⁽⁵⁾ was the first to show (for a language similar to L) that a certain set of axioms and operations is complete.

Let us imagine that we have selected some standard set Σ of axioms and operations for the sentences of L , which is complete. We can form new formal deductive systems from this by adding to the axioms of Σ some new set of sentences, Γ (and retaining the operations of Σ). A set of sentences Γ is called *consistent* if the system (Σ, Γ) obtained in this way does not yield as formal theorems some sentence B , and also (*not* B).

This definition of consistency is purely formal, insofar as it involves reference only to axioms and operations. By contrast, the definition of satisfiability is given in terms of meanings: A set Γ of sentences is called *satisfiable* if there exists an interpretation of L which makes every sentence of Γ true.

Although the definitions of consistency and satisfiability are of very different kinds, the two notions can be proved equivalent. The proof that every satisfiable Γ is also consistent⁽⁶⁾ is quite simple, and depends on the fact that the operations of Σ not only preserve validity, but also preserve the property, *with respect to each interpretation of L* , of being a true sentence; from which it follows by induction that when Γ is satisfiable so is the set Λ of all formal theorems of (Σ, Γ) , whence we cannot have both B and (*not* B) as formal theorems. However, the proof that consistency implies satisfiability

⁽⁴⁾ We do not require the axioms to be finite in number. However, it is required that a method be supplied to decide in a finite number of steps whether any given sentence is an axiom or not. Similarly, in connection with the *operations*, it is required that a method be supplied to decide finitely whether a given sentence arises from one or more other given sentences by one of the operations.

⁽⁵⁾ Kurt Gödel, *Die Vollständigkeit der Axiome des logischen funktionen Kalküle*, Monatshefte für Mathematik und Physik vol. 37 (1930) pp. 349–360.

⁽⁶⁾ This fact, of course, is familiar enough among mathematicians, who often establish the consistency of some axiom set by furnishing a model which satisfies it.

ity⁽⁷⁾ is much more difficult. Indeed, the depth of this result is seen from the fact that the completeness of Σ is a simple consequence of it. For let B be a valid sentence of L . Then (*not* B) is false for every interpretation of L , and so is not satisfiable. If we have established that consistency implies satisfiability, it thus follows that (*not* B) is inconsistent. But if (*not* B) leads to a formal contradiction, then (just as in ordinary mathematical reasoning) this furnishes a formal proof of B . That is, every valid sentence is a formal theorem, and so Σ is complete.

We intend to apply to problems in abstract algebra the result described above, in the following stronger form which can be proved: *If Γ is a consistent set of sentences of L , then there exist interpretations satisfying Γ in which the domain D has at most the same cardinal number as the set of symbols of L .* It should be mentioned that in order to establish this result it appears necessary to well-order the sentences of L , so that when L contains a nondenumerable number of individual constants recourse is made to the axiom of choice. The structure of the model satisfying Γ depends on this well-ordering.

Actually, we shall only have to use the following corollary of the quoted theorem.

Let Γ be any set of sentences of L . Suppose every finite subset of Γ is satisfiable. Then there exist interpretations satisfying Γ in which the domain D has cardinality at most equal to that of the set of symbols of L .

To establish this corollary, it is necessary only to observe that the hypothesis guarantees that Γ must be consistent. For suppose Γ were inconsistent. Then in the system (Σ, Γ) we could find two formal proofs, one of some sentence B and the other of (*not* B). But since these formal proofs are finite columns of formulas, we see that some finite subset of Γ is already inconsistent. This, however, is incompatible with the hypothesis that every finite subset of Γ is satisfiable, since we had previously noted that satisfiability implies consistency⁽⁸⁾.

(7) The first formulation and proof of this theorem was given by Gödel, loc. cit., although an idea which is easily converted into a proof appears earlier in Th. Skolem, *Über einige Grundlagenfragen der Mathematik*, Skrifter utgitt av Det Norske Videnskaps-Akademi i Oslo, 1929, no. 4. These proofs were formulated for systems which resemble L in all significant respects, except that the number of individual constants is considered to be at most denumerable—a restriction on which we have not insisted. A. Malcev (*Untersuchungen aus dem Gebiete der mathematischen Logik*, Matematičeskij Sbornik, N.S. vol. 1 (1936) pp. 323–336) showed that Gödel's proof could be extended to cover systems in which a nondenumerable number of constants were admitted. A more direct proof of the general result can be found in L. Henkin, *The completeness of the first order functional calculus*, Journal of Symbolic Logic vol. 14 (1949) pp. 159–166.

(8) It is curious that although this corollary deals only with sentences and models used to interpret them, any proof of the corollary seems to bring in references to formal deductive systems, with their paraphernalia of axioms and operations of formal inference. It is true that we know of a systematic way to eliminate such reference, but the resulting proof then appears highly artificial and cumbersome.

In the sequel we shall refer to this corollary as "*our basic result from logic.*"

2. Applications to algebra. Given a sentence S of L , and a model⁽⁹⁾ D with respect to which L can be interpreted, we have seen that S takes on a definite value, truth or falsity. Thus, with each sentence S there is associated a *property* of models, namely the property P_S which holds just for those models D which make S true; or, instead of speaking of properties we may speak of *classes*⁽¹⁰⁾ of models, P_S being simply the class of models D for which S is true. A property or class associated in this way with a sentence of L is called an *arithmetical class*⁽¹¹⁾. For example, the property of being a group is arithmetical, since each group axiom can be expressed by a sentence of L , and the conjunction S of these sentences yields the class of groups as its associated class P_S . Similarly (as may easily be seen), the class of rings, the class of integral domains, the class of fields, the class of fields of characteristic two—are all arithmetical classes. On the other hand (as we shall show), the class of finite groups, and the class of fields of characteristic zero, are not arithmetical. A model having the arithmetical property P will be called a P -model.

THEOREM 1. *Let P be an arithmetical class. Let D be any infinite model. A sufficient (and trivially necessary) condition that D have an extension E which is a P -model is: that every finite subset of D be isomorphic to a subset of a P -model. Furthermore, such extensions E exist having the same cardinality as D ⁽¹²⁾.*

(An isomorphism ϕ of D' into E , where D' is a subset of D , is a one-one mapping of D' into E which preserves sums and products of elements of D' when these sums and products are also in D' .)

Proof of Theorem 1. For each element a of D we provide an individual constant v_a in L , to serve as a name for it. Now form the set, Γ , of sentences of L , as follows. For each distinct pair a, b of elements of D we place the sentence (*not* $v_a = v_b$) in Γ . Whenever we have a relation $a + b = c$ (resp. $a \cdot b = c$) holding among elements a, b, c in D , we place in Γ the sentence⁽¹³⁾ $(v_a + v_b) = v_c$ (resp. $(v_a \cdot v_b) = v_c$). Finally, we place in Γ a sentence S which

⁽⁹⁾ In this section we shall frequently speak of a model D , when strictly we should speak of an interpretation of L whose domain is D . This is a generalization of the innocent confusion which one finds in discussions of algebra when there is reference to "a group, G ," when what is meant is a group whose operations are defined on a set G .

⁽¹⁰⁾ The classes involved here are so large (e.g. the class of all rings) that precautions must be taken in order to avoid the classical paradoxes. One method is to consider our whole theory to be relative to some large, fixed set from whose elements all models are to be constructed.

⁽¹¹⁾ This terminology is due to Tarski, who pioneered in the investigation of these classes; Tarski showed that it is possible to define them in a purely algebraic manner, without making any reference to sentences of languages like L . Cf. *Sur les ensembles définissables de nombres réels*. I, Fund. Math. vol. 17 (1931) pp. 210–239; and *Arithmetical classes and types of mathematical systems*, Bull. Amer. Math. Soc. vol. 55 (1949) pp. 63–64.

⁽¹²⁾ Of any standard set of axioms for group theory.

⁽¹³⁾ That is, Γ contains the addition and multiplication tables for D .

defines P (i.e. such that P_s is the given P); this must exist since P is arithmetical.

Now let Γ' be any finite subset of Γ , and let D' be the (finite) subset of D consisting of those elements a such that v_a occurs in a sentence of Γ' . By hypothesis (that is, by the condition whose sufficiency we are trying to establish), there exists a P -model E' and an isomorphic mapping ϕ of D' into E' . Now use E' as a model with which to interpret L , assigning the individual constant v_a as a name of $\phi(a)$ for each a in D' (and for other a assigning the denotation of v_a in an entirely arbitrary way). Under this interpretation every sentence of Γ' is true—as one sees by remembering that ϕ is an isomorphism, and examining in turn each kind of sentence that may appear in D' . (In the case of the sentence S , this will be true since E' is a P -model.)

We have thus shown that any finite subset Γ' , of Γ , is satisfiable. By our basic result from logic it follows that there is an interpretation of L , satisfying Γ , in which the domain E has a cardinality at most equal to that of the set of symbols of L . Since the symbols other than the individual constants are denumerable, and since there is one symbol v_a for each element of (the infinite set) D , we see that E can be chosen to have a cardinal number at most equal to that of D .

Now define a mapping ψ of D into E by setting $\psi(a)$ equal to that element of E which is denoted by v_a in the interpretation which satisfies Γ . Clearly ψ is one-one since E satisfies (*not* $v_a = v_b$) whenever $a \neq b$. Similarly, ψ is an isomorphism since E satisfies $(v_a + v_b) = v_{a+b}$ and $(v_a \cdot v_b) = v_{a \cdot b}$ for all pairs a, b of D . Finally, E is a P -model since it satisfies S . Thus D is isomorphic to a submodel of the P -model E . This completes the proof of the theorem.

An application of Theorem 1. Every Boolean ring R is isomorphic with a ring of sets⁽¹⁴⁾. If R is infinite, these sets can be chosen so that their union will have at most the same cardinality as R .

It will be recalled that a ring is called *Boolean* if for every element a , $aa = a$; from this it follows that multiplication is commutative and addition nilpotent ($a + a = o$). The subsets of a fixed set form a Boolean ring when multiplication is defined as intersection, and addition as union minus intersection; a subring of such a ring is called a *ring of sets*.

An element a , of a Boolean ring R , is called an *atom* if $a \neq o$ and ab is either a or o for each b in R . Let R^* be the ring of all sets of atoms of R . For any b in R , let $\phi(b)$ be the set of all atoms a such that $ab = a$. From the definition of *atom* and the Boolean properties of addition and multiplication listed above, it is a simple matter to see that ϕ is a homomorphism of R into R^* . This fact was recognized early in the study of Boolean rings⁽¹⁵⁾; but it does

⁽¹⁴⁾ This is the well known representation theorem for Boolean rings. See M. Stone, *The theory of representations for Boolean algebras*, Trans. Amer. Math. Soc. vol. 40 (1936) pp. 37–111.

⁽¹⁵⁾ E. V. Huntington, *New sets of postulates for the algebra of logic*, Trans. Amer. Math. Soc. vol. 35 (1933) pp. 274–275.

not make the representation theorem trivial because for many Boolean rings ϕ is not a one-one mapping (i.e. there are elements $b \neq o$ such that $\phi(b) = o$). However, it is easy to show that for every *finite* Boolean ring R , ϕ is one-one; for starting with any nonzero element b , each maximal sequence of nonzero terms b, bc, bcd, \dots , in which the successive factors b, c, d, \dots are all distinct, must terminate in an element of $\phi(b)$.

Now it is easy to see that the class of Boolean rings R for which ϕ is one-one is an arithmetical class. For let S_0 be the following sentence of L :

$$(all\ x)(If\ (not\ x = v_0)\ then\ (exists\ y)((y \cdot x = y\ and\ (all\ z) \\ (y \cdot z = v_0\ or\ y \cdot z = y))\ and\ (not\ y = v_0))).$$

Let S_1 be the sentence $(all\ x)\ x \cdot x = x$, and let S_2, \dots, S_k be sentences of L expressing any standard set of axioms for rings (using the symbols “+” and “ \cdot ” of L to denote ring addition and multiplication respectively, and using “ v_0 ” to denote the zero element of the ring). Finally, let S_{at} be the sentence $(\dots((S_0\ and\ S_1)\ and\ S_2)\ and\ \dots\ and\ S_k)$. Then the class $P_{S_{at}}$ of models which make S_{at} true is precisely the class of Boolean rings for which ϕ is an *isomorphism* of R into R^* .

Since $P_{S_{at}}$ is arithmetical, we may contemplate an application of Theorem 1. For this purpose, let R be any Boolean ring, and let R' be any finite subset of its elements. The ring E' generated by R' must also be finite. (For since multiplication is commutative and all powers of an element are equal to the element itself, at most 2^n elements can be formed by multiplication alone, n being the number of elements in R' ; and since addition is commutative and nilpotent, it follows that E' can have at most 2^{2^n} elements.) But E' , being a finite Boolean ring, must be a $P_{S_{at}}$ -model, as previously observed. Thus R' can be mapped isomorphically into a $P_{S_{at}}$ -model by the identity mapping. The hypothesis of Theorem 1 being verified, the conclusion follows: R is isomorphic to a $P_{S_{at}}$ -model with cardinality at most equal to that of R ⁽¹⁶⁾. This is precisely our representation theorem⁽¹⁷⁾.

The representation theorem for distributive lattices may be accomplished in a manner entirely analogous to the treatment we have employed for representing Boolean rings. In these cases we apply our Theorem 1 to show that every model of some arithmetical class \mathcal{Q} can be extended to a model having some specified arithmetical property P , by showing that: (i) every *finite*

⁽¹⁶⁾ Of course some (but not all) Boolean rings R can be represented as an algebra of sets, using points whose cardinality is actually *less* than that of R . We do not know of any algebraic characterization of those R for which this is possible. Compare Horn and Tarski, *Measures in Boolean algebras*, Trans. Amer. Math. Soc. vol. 64 (1948) pp. 467–497.

⁽¹⁷⁾ It will be observed that our proof of the representation theorem proceeds by establishing the equivalent theorem that every Boolean ring can be extended to an atomistic one. This technique for proving representation theorems has been used in connection with structures which are Boolean rings having additional operations. Cf. Jónsson and Tarski, *Boolean algebras with operators*, Amer. J. Math. vol. 73 (1951) pp. 891–939.

\mathcal{Q} -model is a \mathcal{P} -model, and (ii) every finite set of elements of a \mathcal{Q} -model generates a finite \mathcal{Q} -model (and hence can be extended to a \mathcal{P} -model).

Now in general, if we know merely that every finite \mathcal{Q} -model is a \mathcal{P} -model (where \mathcal{P} and \mathcal{Q} are arithmetical) we cannot conclude that every \mathcal{Q} -model can be extended to a \mathcal{P} -model. (For example, let \mathcal{Q} be the class of ordered fields, and let \mathcal{P} be the empty class.) We can only use Theorem 1 to conclude that if every *finitely generated* \mathcal{Q} -model can be imbedded in a \mathcal{P} -model, then so can every \mathcal{Q} -model.

Thus, in the case of each particular arithmetical \mathcal{Q} we can raise the question: Does the condition that all finite \mathcal{Q} -models have some arithmetical property \mathcal{P} imply that every \mathcal{Q} -model can be extended to a \mathcal{P} -model? We see (by Theorem 1) that a condition sufficient to insure this is that every finite set of elements selected from an arbitrary \mathcal{Q} -model be isomorphic to a set of elements of some finite \mathcal{Q} -model.

For example, this condition holds for the class \mathcal{Q} of abelian groups⁽¹⁸⁾. To see this, consider first the case of an infinite cyclic group generated by an element a . Any finite set of elements $a^{i_1}, a^{i_2}, \dots, a^{i_n}$ can be mapped isomorphically into a cyclic group of order $K = \max_{1 \leq i \leq n} |i_i|$ by the function $\phi(a^{i_i}) = b^{i_i}$ (where b is an element of order K). Next observe that if ϕ maps elements a_1, \dots, a_n of a group G isomorphically into a finite group G_1 , while ψ maps elements b_1, \dots, b_m (of some other group H) into a finite group H_1 , then the elements $a_i b_j$ of the direct product $G \times H$ are mapped isomorphically into the finite group $G_1 \times H_1$ by the function $\sigma(a_i b_j) = \phi(a_i) \psi(b_j)$. Since every finitely-generated abelian group is the direct product of cyclic groups, it now follows that any finite set of elements of an abelian group can be imbedded in a finite abelian group. Thus any arithmetical class \mathcal{P} which contains all finite abelian groups contains an extension of every abelian group.

However, we do not know whether the corresponding theorems are true for arbitrary groups.

We next derive two theorems which throw some light on the nature of arithmetical classes, but whose principal interest is due to applications which can be made of certain generalizations.

THEOREM 2. *Let M be any infinite model of some arithmetical class \mathcal{P} , and let α be any cardinal number equal to or greater than that of M . Then \mathcal{P} contains a proper extension of M having cardinality α .*

Proof. For each element a of M furnish an individual constant v_a in the language L . Form a class Γ of sentences by taking all sentences of the forms: (not $v_a = v_b$) for $a \neq b$, $(v_a + v_b) = v_{a+b}$, and $(v_a \cdot v_b) = v_{a \cdot b}$. Add to L a new individual constant v and put in Γ all sentences (not $v = v_a$) for each a of M . Finally, add to Γ a sentence defining \mathcal{P} .

⁽¹⁸⁾ This was pointed out to me by John Tate.

Now M itself will satisfy any finite set of sentences of Γ , since M is an infinite model in \mathbf{P} . Hence, by our basic result from logic, there is a model satisfying every sentence of Γ , and this will clearly be a proper extension of M which is also in \mathbf{P} . To obtain extensions of arbitrarily high cardinality it is only necessary to modify the argument by adding to L not merely one new individual constant v , but a whole set of constants v_i (where i ranges over a set of any preassigned cardinality). All sentences (*not* $v_i = v_j$), for distinct i, j , must be added to Γ to secure the desired extension.

Theorem 2 shows that no particular infinite model—for instance the field of rationals—can be characterized arithmetically. However, every finite model can be so characterized (to within isomorphism). For an example, consider the arithmetical class defined by the sentence

$$((\text{all } x)(x = v_0 \text{ or } x = v_1) \text{ and } (\text{not } v_0 = v_1)),$$

which consists of all two-element models. By conjoining further clauses to this sentence we could obtain, e.g., the arithmetic class consisting solely of two-element fields.

THEOREM 3. *If an arithmetical class \mathbf{P} contains arbitrarily large finite models, it must also contain an infinite model.*

Proof. Form a set Γ (of sentences of L) by adding to the sentence defining \mathbf{P} the following infinite list Φ of sentences.

$$\begin{aligned} & \text{not } (\text{exists } y)(\text{all } x)x = y, \\ & \text{not } (\text{exists } y)(\text{exists } z)(\text{all } x)(x = y \text{ or } x = z), \\ & \text{not } (\text{exists } y)(\text{exists } z)(\text{exists } y_1)(\text{all } x)((x = y \text{ or } x = z) \text{ or } x = y_1), \\ & \dots \end{aligned}$$

Any set of sentences of this list which is contained among the first n will be satisfied by any model with n or more elements. Since \mathbf{P} contains arbitrarily large finite models, it must contain a model satisfying all sentences of this list (by our basic result from logic). But this is clearly an infinite \mathbf{P} -model.

3. Generalizations. Instead of considering the set of models which make some *one* sentence of L true, we may consider the set of all models which satisfy each member of some preassigned class of sentences of L . Such a set (or property) of models I call *quasi-arithmetical*. In general a quasi-arithmetical class defined by a set of sentences Γ is contained in, but not equal to, the intersection of the arithmetical classes defined by the separate sentences of Γ ⁽¹⁹⁾. It is easily seen that all of the theorems and remarks

⁽¹⁹⁾ Mention should be made here of the very interesting and suggestive classification given by Tarski at the 1950 International Congress of Mathematicians. Using " AC " to denote an arithmetical class of models, Tarski calls an AC_δ (AC_σ) any countable intersection (union) of AC 's, and then goes on to consider the notion of an $AC_{\delta\sigma}$, $AC_{\sigma\delta}$, $AC_{\delta\sigma\delta}$, etc., in analogy with the

stated in the previous section for arithmetical classes hold also for quasi-arithmetical classes, and we shall henceforth refer to Theorems 1, 2, and 3 in this extended form. To modify the proofs of the theorems so as to obtain the stronger results, it is only necessary (in forming sets Γ of sentences) to replace the single formula defining an arithmetical class P by a set of formulas defining a quasi-arithmetical class.

The class of all infinite fields is quasi-arithmetical since it is defined by adding a set of axioms for fields to the set Φ of sentences described in the proof of Theorem 3. However its complement, the class of all finite fields, is not quasi-arithmetical (and so surely not arithmetical) as we see at once from Theorem 3. Hence the class of infinite fields is an example of a class which is quasi-arithmetical but not arithmetical; for if it were arithmetical it would be defined by a sentence S , and so the sentence (*not* S) would define the class of all finite fields to be arithmetical.

If P is *any* quasi-arithmetical but not arithmetical class, then (as in the case above) its complement Q cannot be quasi-arithmetical. For suppose Λ and Γ are sets of formulas defining P and Q respectively. Since P is not arithmetical, no finite subset of Λ defines P (else the conjunction of the sentences of such a finite subset would be a single sentence defining P). Thus, every finite subset of Λ is satisfied by some model from the complement of P , and hence every finite subset drawn from the union of Λ and Γ is satisfied (by a model of Q). By our basic result from logic, this means that there is a model satisfying all sentences of the union of Λ and Γ —contrary to the fact that Λ and Γ define disjoint classes.

Another respect in which the results of the previous section generalize has to do with the symbols of L . Instead of having just two symbols, $+$ and \cdot , denoting binary operations, L may have any number of symbols each denoting (in each interpretation) a particular n -ary operation (with n not necessarily the same for all symbols). Further, in addition to (or instead of) symbols denoting operations, L may have symbols (constants) denoting classes and relations. The basic result from logic holds for all such languages, and so our discussion remains pertinent.

For example, arithmetical classes composed of ordered sets are studied by means of a language L containing a single symbol, say $<$, which is used to denote a binary relation (so that the basic sentences of this L have the forms $\alpha < \beta$ and $\alpha = \beta$, where α and β are any individual variables or constants).

Using Theorem 1 for this language we immediately obtain "the ordering

familiar construction of Borelian sets on the real line. The notion of an AC_3 is similar to, but not the same as, that of a quasi-arithmetical class. For example, the set of all fields isomorphic to an extension of the field of real numbers is quasi-arithmetical, but not an AC_3 . The result established below that the class of well-ordered systems is not quasi-arithmetical is thus a strengthened form of the theorem, established by Tarski in 1936 (*Grundzüge des Systemenkalküls*), that this class is not an AC_3 .

theorem" to the effect that every set can be ordered by a transitive relation which holds in exactly one direction between any two elements. This follows from the obvious facts that any finite subset of elements drawn from an arbitrarily given set can be so ordered, while an ordering of some extension of the given set automatically furnishes an ordering of the set itself.

If we could strengthen this result to obtain a proof of the *well-ordering* theorem, it would show that our basic result from logic was equivalent to the axiom of choice (with whose help it was established). However, it seems unlikely that this can be done, for the well-ordered systems do not form a quasi-arithmetical class. To see this, it is only necessary to remark that if the property of being well-ordered *were* quasi-arithmetical, we could use Theorem 1 to conclude that every ordered system can be extended to a well-ordered system (since every finite subset of an ordered system is well-ordered); but this is manifestly impossible since if an ordered set contains an infinite, descending sequence of elements so does every extension.

The precise determination of the relative strength of the axiom of choice and our basic result from logic thus remains open. One plausible conjecture is that any property of sets (such as the ordering theorem) which can be proved with the axiom of choice, and which can be expressed by a set of sentences of a first-order language L , can also be proved using our basic result from logic.

We now come to a simple but important generalization of Theorem 2.

THEOREM 4. *Let \mathcal{C} be any infinite family of disjoint arithmetical classes C_i . Let Q be the union of the C_i , and let \bar{Q} be its complement. If P is any quasi-arithmetical class which meets infinitely many C_i , then P also meets \bar{Q} ⁽²⁰⁾.*

Proof. Let Λ be a set of formulas defining P , and (for each i) let S_i be a sentence defining C_i . Form Γ by adding to Λ every sentence (*not* S_i). Given any finite subset of Γ there is a model making each of its sentences true; for by hypothesis, being given any finite collection of the C_i we can find a model of P not in any of them. Hence we can apply our basic result from logic to Γ to obtain Theorem 4.

By combining the technique of this proof with that of Theorem 1 we can, in some cases, obtain a stronger conclusion.

THEOREM 5. *Let \mathcal{C} be an infinite class of disjoint arithmetical classes C_i ,*

⁽²⁰⁾ The substance of this theorem was apparently known to Tarski as early as 1946. At the Princeton Bicentennial Conference in December, 1946, he cited as an application the possibility of proving the existence of non-Archimedean ordered fields. (For this application C_i is taken as the arithmetical class defined by the sentence ($iv_2 < v_3$ and (*not* $(i+1)v_2 < v_3$)), $i = 1, 2, 3, \dots$, while P is defined by a set of ordered field axioms together with the sentences (*all* x) $x \cdot v_0 = v_0$, $v_0 < v_2$, and $v_2 < v_3$. Thus any model which is in both P and \bar{Q} is an ordered field in which v_2 is a positive element, $v_2 < v_3$, while for no $i = 1, 2, 3, \dots$ is $iv_2 < v_3 \leq (i+1)v_2$.) The theorem was rediscovered independently by me (but later—in the spring of 1947), and several applications were included in my doctoral dissertation.

\mathcal{Q} their union, and $\overline{\mathcal{Q}}$ its complement. Let \mathcal{P} be a quasi-arithmetic class, let A be a model, and suppose that any finite set of elements of A can be imbedded in the intersection $\mathcal{P} \cap \mathcal{C}_i$ for infinitely many \mathcal{C}_i . Then there is an extension of A in the intersection $\mathcal{P} \cap \overline{\mathcal{Q}}$.

Proof. Add to the language L new individual constants v_a , one for each element a of A . Add to the set Γ (in the proof of Theorem 4) the basic sentences defining the structure of A (as in the proof of Theorem 1). Then apply our basic result from logic.

With the aid of Theorem 5 we can extend the bare existence theorem mentioned in footnote 20 to show that if F is any ordered field and x any of its elements > 0 , there exists a non-Archimedean extension of F containing elements y and z such that $y^n < x$ and $x^n < z$ for all $n = 1, 2, 3, \dots$.

Interesting applications of these theorems arise when \mathcal{C}_i is taken to be the class of fields of characteristic q_i , where q_i is the i th prime. \mathcal{C}_i may be defined by the sentence⁽²¹⁾ (A and (all x) $q_i x = v_0$), where A is the conjunction of some set of field axioms in which the symbol v_0 denotes the zero element.

Thus from Theorem 4 we learn that if there are fields, with some quasi-arithmetic property \mathcal{P} , of infinitely many different prime characteristics, then there must also be a field of characteristic zero having the property \mathcal{P} . While from Theorem 5 we can infer that if a quasi-arithmetic class \mathcal{P} contains *every* field having the prime characteristic q_i , for infinitely many i , then \mathcal{P} contains an extension of *every* field of characteristic zero. This last inference is possible because any finite set of elements from any field of characteristic zero can be imbedded in fields of prime characteristic q_i for all but a finite number of i , as the following argument⁽²²⁾ shows.

We classify our finite set of elements into those which are in the prime field (which can be represented as rational numbers), next a sequence of elements x, y, \dots, z each transcendental over the field obtained by adjoining the others to the field of rationals, and finally the remaining elements which will be algebraic over the field $R(x, y, \dots, z)$. Thus we can think of our elements as algebraic functions in the "letters" x, y, \dots, z . Now it is known that any finite set of algebraic relations (equalities and inequalities), holding among a finite set of such functions, can be preserved when the letters are "specialized" to suitably chosen rational numbers (and the functions replaced by an appropriate set of their values)⁽²³⁾. Thus we can represent our finite set of field elements as a set of algebraic numbers. And now it

⁽²¹⁾ It should be borne in mind that the symbol " $q_i x$ " which occurs here is, like " A ," an abbreviation. It stands for a row of q_i occurrences of the symbol " x " separated by plus signs (and with parentheses suitably introduced so that the whole is a *term* of the language L). The symbol " q_i " itself is not part of L . Similar remarks apply to the formulas of footnote 20.

⁽²²⁾ This argument is due to Emil Artin.

⁽²³⁾ Cf. van der Waerden, *Moderne Algebra*, 2d ed., §92. The theorem is there proved for single relations, but is easily extended to the case of finite sets of relations.

is clear that the ideal generated by these numbers can have only a finite number of prime ideals as divisors, while any other prime ideal leads to a quotient field of prime characteristic in which our given set of elements can be imbedded.

Notice, from this proof, that if we start with a finite set of elements *in an algebraic number field*, then we can imbed them in fields of prime characteristic, for almost all primes, which are simply obtained from the given field by forming the quotient field with respect to some prime ideal. Hence if an arithmetical class \mathbf{P} contains infinitely many such quotient fields, for some given algebraic number field F , then \mathbf{P} must also contain an extension of F . For instance, if a polynomial in several variables over F factors modulo infinitely many prime ideals, then the polynomial must factor in an extension of F .

Other interesting applications of Theorems 4 and 5 arise when we take \mathbf{C}_i to be the class of groups for which i is the maximum order of any element. In this case, however, we do not know whether any finite set of elements taken from an arbitrary group can be imbedded in a group with elements of bounded order.

Still another type of structures to which these methods are applicable is the infinite group with finite layers⁽²⁴⁾. For example, let G be such a group, and let K_i be the (finite) set of elements of G whose order is $\leq i$, $i = 1, 2, 3, \dots$. Let \mathbf{P} be a quasi-arithmetical class and suppose that, for each i , K_i can be extended to a \mathbf{P} -group, G_i . Then G itself can be extended to a \mathbf{P} -group. Further, if the extensions G_i can be obtained without adding to K any new elements of order $\leq i$, then the new elements in the extension of G will all have infinite order.

Although the theory of arithmetical classes has been suggested by the study of interpretations of the language L , it can be established in a purely algebraic fashion. This was first observed by Tarski⁽²⁵⁾, by whom the theory has since been developed more elaborately, as well as applied to algebraic problems⁽²⁶⁾.

4. Languages of higher order. Although, in the previous section, we have allowed ourselves wide latitude in the kind of constants which could be incorporated into the language L , we have retained only one type of variable—namely, variables which range over elements of the model when L is given an interpretation. This is the characteristic feature of what logicians call a *first-order language*.

⁽²⁴⁾ These are groups which have only a finite number of elements of order n , for each $n = 1, 2, \dots$. Cf. S. N. Cernikov, *Infinite groups with finite layers*, *Matematicheskii Sbornik* N. S. vol. 22 (1948) pp. 101–133.

⁽²⁵⁾ Cf. Tarski, *Sur les ensembles définissables de nombres réels*, I. *Fund. Math.* vol. 17 (1931) pp. 210–239; and *Grundzüge des System Kalküls*, *Fund. Math.* vol. 26 (1936) pp. 283–301.

⁽²⁶⁾ Cf. *Bull. Amer. Math. Soc.* vol. 55 (1949) pp. 63–65. Also the Proceedings of the International Congress of Mathematicians at Harvard.

Now many properties of algebraic models which are discussed in the literature are described with the aid of other types of variables. For example, a *simple* group is a nontrivial group which satisfies the sentence

$$(all\ G)(if\ sub(G)\ then\ (all\ x)(if\ x \in G\ then\ x = v_0)),$$

where $sub(G)$ is an abbreviation for the conjunction of sentences stating that G is a proper normal subgroup. Here the variable G ranges over all sets of model elements, while \in is interpreted as denoting the relation of membership.

An extension of the language L is called *second-order* if it contains the symbol \in , and in addition variables which may range over sets of model elements and relations defined on model elements, as well as over functions of n model elements whose values are model elements. (That is, variables are permitted for all categories which were represented by constants in the first-order languages). Of course the definition of "term" is broadened, in setting up this language formally, so as to permit the new function variables to operate on terms to form new terms, while the definition of "basic sentence" is enlarged to include expressions of the forms $\tau \in \Phi$, where τ is any term and Φ any set-variable, $\Psi(\tau_1, \dots, \tau_n)$, where Ψ is a relation-variable, $\Phi_1 = \Phi_2$, and $\Psi_1 = \Psi_2$.

Higher order languages contain constants denoting, and variables ranging over, sets whose elements may be sets or functions of model elements, as well as functions and relations defined over sets or functions of model elements⁽²⁷⁾. And then there are languages of still higher order. The study of these languages leads to a theory of types.

Consider for the moment a second-order language in which only variables ranging over *sets* of model elements have been added. A *standard interpretation* for such a language consists in specifying a particular domain (the model) as the range for the individual variables, and assigning denotations of the appropriate type to each constant of the language. Under such an interpretation each sentence takes on a definite truth value, truth or falsity, it being understood that a sentence of the form $(all\ G)A$ is to be read "for every class G of model elements, A ." Thus each sentence defines a property (or class) of models—namely those models for which the sentence becomes true. In this way we are led to consider second-order classes where previously we studied arithmetical (or first-order) classes of models. And then we may go on to study higher-order classes.

Naturally we are led to inquire whether our basic result from logic holds

(27) Another type of variable which occurs in many mathematical papers (including this one) is a variable ranging over natural numbers. However, no special provision need be made for these, for it is well known (since the time of Frege) that the natural numbers can be identified with certain nameable sets of sets of model elements, and that the collection of these "numbers" can be described by a formula of a suitably high-ordered language.

for these higher order languages as well as for the first-order case. But it is at once apparent that this cannot be true. For example, let S be the second-order sentence which states that for every complete order-relation there is a last element. (Thus S determines the second-order class consisting of all finite models.) Take individual constants v_i , $i = 1, 2, 3, \dots$, and form a set Γ of sentences by adding to S all sentences (*not* $v_i = v_j$) for $i \neq j$. Clearly every finite subset of Γ is satisfiable, while Γ itself is not⁽²⁸⁾.

However, there exists a simple class of interpretations for the higher-order languages which is more extensive than the standard interpretations. Reverting again to the simple case of a second-order language where only set-variables have been added to the first-order language, we may consider as model any set of elements—together with a specified family (not necessarily all) of sets of these elements. Calling the sets of this family *admissible*, we may now reinterpret the sentences of our language with the understanding that a sentence of the form $(\text{all } G)A$ is to mean "for every *admissible* class G of model elements, A "⁽²⁹⁾. Similarly, in the case of higher-order languages, we consider general models in which a family of admissible classes, relations, or functions is specified as the range for each type of variable which appears.

The formal axioms and rules of inference which logicians had set up for giving structural organization to the sentences which are true under every standard interpretation turn out to yield (as formal theorems) sentences which are true for all general models (which we will call *valid* sentences). Indeed, it has been proven⁽³⁰⁾ that for every set of sentences which is consistent with respect to these rules, there is a model⁽³¹⁾ making every sentence of the set true (under the broad interpretation); and hence the rules must be complete, in the sense that they yield as formal theorems *all* valid sentences.

⁽²⁸⁾ Since every finite subset of Γ is satisfiable, Γ is *consistent*; i.e., no formal contradiction can be inferred from Γ when appropriate formal rules of inference are supplied for second-order languages. Thus there are consistent sets of sentences which are not satisfiable. In fact, there are *single* sentences which are consistent but not satisfiable—although this is very much harder to show. This last fact is equivalent to the *incompleteness* of the formal rules of deduction—a famous result due to Gödel.

⁽²⁹⁾ Of course the family of admissible sets cannot be chosen in a completely arbitrary way, if every sentence of the language is to have a meaningful interpretation with respect to the model. For example, because of the presence of the words *not*, *and*, *or*, in our language, the family of admissible sets must be closed under the Boolean operations. Because of the presence of quantifiers such as $(\text{all } x)$ and $(\text{exists } x)$ the admissible sets must also be closed under the operations which Tarski has called *cylindrifications*. The presence of quantifiers on set-variables imposes still further restrictions on the families which may be proposed for the admissible sets in an interpretation of the language. And similar considerations apply in the case of languages of higher order.

⁽³⁰⁾ Cf. Leon Henkin, *Completeness in the theory of types*, Journal of Symbolic Logic vol. 15 (1950) pp. 81–91.

⁽³¹⁾ The elements, together with all admissible sets, relations, and functions of this model, can be so chosen that their cardinal number is no greater than that of the set of all symbols of the language.

From these facts there emerges the following generalized form of our basic result from logic: *If Γ is any set of sentences of a higher-order language, and if every finite subset of Γ is satisfied by some general model, then there is a general model for which every sentence of Γ is true.*

Let us call a property (or class) of models *definable* if it consists of all general models which make some given sentence (of any higher-order language) true. Similarly, a set of models satisfying a set of sentences will be called *quasi-definable*. Thus our basic result from logic (in its generalized form) can be rephrased to assert that a family of quasi-definable classes in which the members of every finite subfamily have models in common must itself have a nonempty intersection.

We can speak of a definable class of second order, or higher order, according to the type of variables which appear in the defining sentence. A first order definable class is simply an arithmetical class.

Remember that a *standard* model is one in which each family of admissible classes (or relations or functions), of any type, consists of *all* classes (or relations or functions) of that type. The intersection of a definable class of models with the family of all standard models will be called a *standard-definable* class. The class of topological spaces, the class of rings with descending chain condition, and the class of well-ordered systems are familiar examples of standard-definable classes.

Except in the arithmetical (first order) case, no definable class containing an infinite model is a standard-definable class, since every such definable class contains a model whose admissible classes have the same cardinality as its domain of elements, according to our basic result from logic. On the other hand there are nonempty definable classes which contain *no* standard models, as follows from Gödel's example of a consistent sentence which is not true for any standard model. It is this last fact which severely curtails the range of interesting applications of our basic result from logic, since nonstandard models of higher-order axiom systems are generally ignored by mathematicians.

It thus appears that the interesting applications are limited to sets of sentences for which we can be sure, in advance, that the existence of a general model satisfying them entails also the existence of a standard model satisfying them⁽³²⁾. However, this still leaves us a certain leeway.

For instance, consider a set Γ of second-order sentences such that no class, relation, or function variables appear in any universal quantifier, while every such variable which occurs in a sentence appears in a single existential quantifier placed at the beginning of the sentence (except possibly for other quantifiers). A moment's reflection will show that if one general model makes the sentences of Γ true, so will any other model consisting of the same elements,

(32) In this connection see Andrzej Mostowski, *On absolute properties of relations*, Journal of Symbolic Logic vol. 12 (1947) pp. 33-42.

but with a family of admissible classes, relations, and functions which contains those of the first model properly. Hence, in particular, the standard model with the same elements will satisfy all sentences of Γ .

To take a specific example from the literature, consider the following theorem⁽³³⁾ first proved by Everett and Whaples. Let I be a set of indices, and for each $i \in I$ let T_i be a finite set. A sufficient (and trivially necessary) condition for the existence of a choice function f such that $f(i) \in T_i$ for each $i \in I$, while $f(i_1) \neq f(i_2)$ for $i_1 \neq i_2$, is that the union of the sets T_i , for any set of n indices ($n = 1, 2, 3, \dots$), contains at least n distinct elements. In the case where I is a finite set of indices the result was obtained by elementary methods by P. Hall. We shall assume Hall's result, and show that the generalization is a simple consequence of our basic result from logic.

For this purpose, suppose I and sets T_i given, satisfying the condition. Consider a higher-order language which contains the following symbols: An individual constant v_i for each i in I , and a class-constant G_I which will be used to denote I ; an individual constant u_a for each element a in one or more of the sets T_i ; a constant S , having the type of functions from individuals to classes, to be used so that $S(v_i)$ denotes the class T_i ; and variables, such as g , having the type of functions from individuals to individuals. In this language form the set Γ containing the following sentences.

- (i) $u_a \in S(v_i)$, for each a and i such that a is in T_i ;
- (ii) (*all* x) (*if* $x \in S(v_i)$ *then* ($x = u_{a_1}$ *or* \dots *or* $x = u_{a_n}$)), for each i , where a_1, \dots, a_n are all of the elements of the (finite) set T_i ;
- (iii) $v_i \in G_I$, for each i in I ;
- (iv) (*exists* g) ((*all* x) (*if* $x \in G_I$ *then* $g(x) \in S(x)$) *and* (*all* x) (*all* y) (*if* ($\text{not } x = y$) *then* ($\text{not } g(x) = g(y)$))).

Now any finite subset Γ' of Γ contains only a finite number of the symbols v_i , and hence (by Hall's theorem) there is a model satisfying each of the sentences of Γ' . Applying our generalized result from logic we see, therefore, that there must be a model for which all sentences of Γ are true. By (iii), such a model will contain a set I' (denoted by G_I) of individuals, of which a subset can be identified with I . By (i) and (ii), there will be a function (denoted by S), whose value for each i in I is T_i . And by (iv) there will be a function f (denoted by g) which, when restricted to the range I , fulfills the promise of the theorem.

It should be noted that if one of the classes T_i is infinite, this proof will not work. For in that case the corresponding sentence (ii) could not be formed, according to our rules for forming sentences in these languages. And if we omit the sentence from Γ , the class denoted by $S(v_i)$ will contain (but not necessarily equal) T_i ; hence there is no guarantee from (iv) that $g(v_i)$ will

⁽³³⁾ Cf. C. J. Everett and George Whaples, *Bull. Amer. Math. Soc.* Abstract 53-5-170. This theorem was evidently considered so fascinating that two other proofs were subsequently published—to which we now add a fourth.

be in T_i . Of course this limitation is not serious, since the theorem is false if the T_i are allowed to become infinite.

A more widespread use of the basic result from logic in the case of higher-order systems must wait until more information has been gathered concerning the structure of general models⁽³⁴⁾.

UNIVERSITY OF SOUTHERN CALIFORNIA,
LOS ANGELES, CALIF.

(³⁴) *Historical note (added December 15, 1952)*. Since this paper was written two works have appeared which overlap it in content: Tarski, *Some notions and methods on the borderline of algebra and metamathematics*, Proceedings of the International Congress of Mathematicians, 1950, vol. 1, pp. 705–720, and Abraham Robinson, *On the metamathematics of algebra*, Amsterdam, North-Holland, 1951. It seems appropriate, therefore, to write a few words about the history of these ideas.

There is no doubt that credit for first envisaging the possibility of applications of “our basic result from logic” is due to Tarski. Related ideas appear in his papers as early as 1931, and an announcement of results was made in 1946 to the Princeton Bicentennial Conference, although without a description of methods. Explicit published references to the theory appeared in 1949 in the form of several abstracts in Bull. Amer. Math. Soc. vol. 55 (1949) pp. 63–65. A full account appears in the above-mentioned paper presented at the 1950 International Congress; it will be observed that Theorem 20 (17) is closely related to our Theorems 2 and 3 (4). A further development of the theory was described by Tarski at the Colloquium Lectures of the American Mathematical Society in September, 1952.

The possibility of applying “our basic result from logic” to problems of algebra was rediscovered by me in the Spring of 1947. Aside from detailed applications, two new basic ideas were added to those which had been developed by Tarski. One was the use of individual constants, together with addition and multiplication tables, to represent a particular structure in the language L —as is done in our Theorem 1. The other was the generalization to higher-order languages described in our last section.

Finally, in the period September 1947–April 1949, the basic ideas were once again found in independent work by Abraham Robinson. Using both the “basic result from logic” and the technique of individual constants, he obtained some of our results relating to the characteristic of models in an arithmetical class of commutative fields, adding important new examples. He also obtained further results in this direction, including the important theorem that an arithmetical class containing one algebraically closed field contains all others of the same characteristic (which was obtained by Tarski in a very different way). Results on non-Archimedean ordered fields also appear in Robinson’s work, and further original material having no counterpart in our work.