COMPUTABLE ALGEBRAIC STRUCTURES AND NONSTANDARD ARITHMETIC

BY

EUGENE W. MADISON[1]

1. **Introduction.** M. O. Rabin [5] has proved a number of interesting theorems concerning computable algebraic structures. Prior to Rabin's paper, A. Froehlich and J. C. Shepherdson [1] proved a wealth of results concerning explicit fields, i.e., computable fields. Loosely speaking, a computable algebraic structure is an algebraic structure whose relations can be viewed as recursive number-theoretic relations. In this paper we are primarily interested in those algebraic structures whose relations can be viewed as arithmetical number-theoretic relations. We shall call such structures arithmetically definable structures (or, more simply, AD-structures). Since every recursive relation is arithmetical, it is immediate that every computable algebraic structure is an AD-structure.

Our interest in these structures grows out of an attempt to solve the following general problem:

(I) Let $\{\mathscr{A}; \mathscr{N}\}$ be an algebraic structure ($\mathscr{N}$ a copy of the natural numbers and $\mathscr{N} \subseteq \mathscr{A}$) and $\mathscr{N}^*$ any (strong) nonstandard model of arithmetic. Does there exist a structure $\mathscr{A}^*$ in which $\mathscr{N}^*$ is embedded such that $\{\mathscr{A}^*; \mathscr{N}^*\}$ is elementarily equivalent to $\{\mathscr{A}; \mathscr{N}\}$?

It is implicit in the above question that the structures under consideration are models of sets of sentences of some formulation of first-order logic. For our purposes we take a convenient formulation of first-order logic with extralogical constants E, S, P, N and 0 whose intended interpretations are equality, sum, product, "x belongs to some model of arithmetic" and zero, respectively.

Precise definitions of "strong model of arithmetic" and "elementary equivalence" are found in [7] and [6], respectively.

A rather natural question related to (I) is:

(II) Do we have uniqueness for any of the affirmative cases of I?

With reference to (I), we prove that the answer is in the affirmative for any AD-structure which contains a copy of $\mathscr{N}$. So, in particular, (I) holds for the field of algebraic numbers, since Rabin has proved that this field is computable. In §2

Received by the editors April 26, 1966.

[1] The author wishes to thank Professor A. Robinson for introducing him to the problems of this paper and making many helpful suggestions which aided in their ultimate solutions. He would also like to thank Professor T. G. McLaughlin for reading the original manuscript and making many helpful suggestions. Also, he wishes to thank Professor K. I. Appel for many suggestions for improving the exposition.

we weed out other fields for which (I) holds; in particular, we prove that the field of real algebraic numbers, the field of constructible numbers and the field of solvable numbers are examples of AD-structures[2] (for precise definitions of the field of constructible numbers and the field of solvable numbers, see [11] and [3], respectively).

With reference to (II), we are able to give an affirmative answer for the field of real algebraic numbers only.

2. **AD-structures.** We begin this section with a development of the computability of the field of rational numbers. Suppose that a mapping $\varphi: Q \rightarrow \mathcal{N}$ is defined in the following way: Using the fact that if $r \in Q$ then there exist unique $a, b \in \mathcal{N}$ $(b \neq 0)$ such that $(a, b) = 1$ and either $r = a/b$ or $r = -a/b$, we let $\varphi(r) = 2^{\delta}3^{a}5^{b}$, where

$$\begin{aligned} \delta &= 1, \qquad \text{for } r \geqq 0, \\ &= 2, \qquad \text{for } r < 0. \end{aligned}$$

φ is clearly a well-defined function from Q into $\mathcal{N}$.

Consider the following number-theoretic functions:

(2.1) $rm(a, b)$ (i.e., the remainder upon division of a by b).

(2.2) $1h(x)$ (i.e., the number of nonzero exponents in the canonical decomposition of x)

$$\begin{aligned} (x)_i &= 0, \qquad \text{for } x = 0, \\ &= a_i, \qquad \text{for } x \neq 0, \end{aligned} \tag{2.3}$$

where a_i is the exponent of the ith prime in the canonical decomposition of x. These functions are known to be recursive. It is clear that the function of (2.1) can be used to express "$d = $g.c.d. (a, b)" as a recursive predicate. Now it is possible to express "$x \in Q$" as a recursive predicate. Simply use

$$\begin{aligned} &[((x)_0 = 1) \vee ((x)_0 = 2)] \wedge (\exists u)_{u \leqq x}[(\exists u)_{v \leqq x}[((x)_1 = u) \wedge ((x)_2 = v) \\ &\qquad \wedge (v \neq 0) \wedge (\text{g.c.d. } (u, v) = 1)] \wedge (\exists y)_{y \leqq 3}[(1h(x) = y)[(u = 0) \leftrightarrow (y = 2)]]]. \end{aligned}$$

We choose to denote this recursive predicate by $J(x)$. As we pass from Q to Q' under φ, we allow the relation of equality to remain as the identity relation (i.e., our models will all be "normal"). Insofar as the relations S and P are concerned,

[2] It is our belief that each of the algebraic structures discussed in this paper enjoy the stronger property of computability. It is interesting that this property in the case of the real algebraic numbers is not a consequence of Rabin's proof of the computability of the field of algebraic numbers. It is further interesting that if we can establish the computability of a single archimedean ordered real-closed field, then this result is a consequence of our proof that $\mathcal{R}$ is an AD-structure. For the fields of constructible and solvable numbers, it appears that a closer scrutinizing of van der Waerden's approach to the effective construction of the Galois groups will give rise to computability. These stronger results, although interesting in their own right, are not needed for the present investigation.

we claim that we find recursive relations S' and P' such that the structure formed by Q' together with S' and P' is isomorphic to Q with relations S and P. One can show by "brute force" that S' and P' can be represented by recursive predicates. See [3].

We have used one of many possible ways of establishing the computability of the rational numbers; whence the field of rationals is an AD-structure. This result is also a byproduct of the following:

THEOREM 2A. *The field of real algebraic numbers is an AD-structure.*

Proof. Let K_0 denote the first-order theory for the concept of real-closed field. Since this theory can be formulated in such a way that its axioms are recursively enumerable, we can use Kleene's formulation of the Goedel completeness theorem (see [2]) to conclude that K_0 has an arithmetical model, say $\mathscr{R}$. Clearly, $\mathscr{R}$ contains an isomorphic copy of Q.

Now the model $\mathscr{R}$ is defined inside of $\mathscr{N}$ by an arithmetical predicate, say $K(x)$; and hence $\mathscr{R}$ is represented inside of $\mathscr{N}$ by a set, say $\mathscr{R}'$, which is defined by: $\mathscr{R}'=\{a \in \mathscr{N} \mid K(a) \text{ holds}\}$. Also the relations S and P are taken onto arithmetical relations S' and P'. Since the rational numbers are a subset of $\mathscr{R}$, it suffices to show that the rational numbers are taken onto an arithmetical subset of $\mathscr{N}$ under the mapping which gives rise to the predicate $K(x)$. Consider the function defined by:

$$\varphi(0) = 0',$$
$$\varphi(n+1) = \sigma(\varphi(n), 1'),$$

where $0'$ and $1'$ are the natural numbers which represent the natural numbers 0 and 1 respectively, and $\sigma(x, y)$ is the arithmetical function defined on $\mathscr{N}$ by the predicate $S'(x, y, z)$. φ is clearly arithmetical since it is recursive in the arithmetical function $\sigma(x, y)$. Moreover, it is clear that φ enumerates the set which represents the natural numbers, say $\mathscr{N}'$, without repetitions. Let $B(x, y)$ be the arithmetical predicate which represents $y=\varphi(x)$. This predicate enjoys the following properties:

(2.4) $(x)(\exists y)(z)[B(x, y) \wedge B(x, z) \supset E(y, z)]$,

(2.5) $(x)(y)(z)[B(x, y) \wedge B(z, y) \supset E(x, z)]$,

(2.6) $$[B(x_1, y_1) \wedge B(x_2, y_2) \wedge B(x_3, y_3)] \supset [[S(x_1, x_2, x_3) \leftrightarrow S'(y_1, y_2, y_3)] \wedge [P(x_1, x_2, x_3) \leftrightarrow P'(y_1, y_2, y_3)]].$$

Now, the following predicate defines the natural numbers arithmetically:

(2.7) $$N(x) \equiv K(x) \wedge (\exists y)B(y, x).$$

The integers are defined arithmetically by

(2.8) $$I(x) \equiv N'(x) \vee (\exists y)[N'(y) \wedge S'(x, y, 0)].$$

Clearly, one can give an arithmetical predicate which defines the rationals, say

(2.9) $$R(x) \equiv (\exists a)(\exists b)[I(a) \wedge I(b) \wedge \neg E(b, 0) \wedge P'(x, b, a)].$$

A discussion of algebraic numbers leads quite naturally to a consideration of polynomials (over Q) which are fortunately amenable to arithmetization via Goedel numbering. This arithmetization will enable us to express in our language the predicate "z is the value of $p(y)$ at x."

Our first step, however, is to show that we can express the predicate "w is the Goedel number of a polynomial (over Q)" by an arithmetical predicate, say $G(w)$. Consider $p(y)=x_0+x_1y+\cdots+x_ny^n$, where each $x_i \in Q$. We define the Goedel number of $p(y)$, say w, by: $w=2^n3^{x'_0}5^{x'_1}\cdots p_{n+2}^{x'_n}$ where each x'_i is the natural number which represents x_i under the aforementioned mapping. We see easily that each polynomial (over Q) has a unique Goedel number and given a natural number, one can effectively decide whether or not it is the Goedel number of a polynomial (over Q) since the image set Q' is effective.

To make the above rather informal discussion precise, we proceed to define the arithmetical predicate, $G(w)$. It can be clearly taken to be:

$$E(w,0) \wedge (\exists n)[((w)_0 = n) \wedge (\exists y)[(1h(w) = y) \wedge (y \leqq n + 2)]$$

$$\wedge\ (i)(\exists x)[(x = (w)_i) \wedge (0 < i \leqq n+2) \supset R(x)]],$$

where $R(x)$ is the arithmetical predicate of (2.9). The quantifiers are easily bounded, so we may assume that $G(w)$ is recursive.

Now we are prepared to determine a predicate expressing the evaluation of a polynomial at a number. More precisely, we determine an arithmetical function f such that "$f(w, y)=z$" expresses "z is the value of substituting y into the polynomial having Goedel number w."

Let σ and π be the arithmetical functions which represent S' and P' respectively. Then define an arithmetical function ρ by

$$\rho(0, y) = 1',$$
(2.10)
$$\rho(n+1, y) = \pi(y, \rho(n, y)),$$

where $1'$ is the natural number which corresponds to 1 under φ. There are three other arithmetical functions that are needed to define the desired function f. Let λ be given by

$$\lambda(w, i) = 0' \qquad \text{for } C_G(w) = 1,$$
(2.11)
$$= (w)_i \qquad \text{for } C_G(w) = 0,$$

where $0'$ is the natural number which corresponds to 0 under φ and $C_G(w)$ is the characteristic function of $G(w)$. λ is recursive by a result found in [5]. Now we further define functions ψ and s by the equations

(2.12) $$\psi(w, y, i) = \pi(\lambda(w, i), \rho(i, y)),$$

and

(2.13) $$s(w, y, 1) = (w)_1, \qquad s(w, y, k+1) = \sigma(s(w, y, k), \psi(w, y, k+1)).$$

These functions are obviously arithmetical. The desired function can now be defined simply by

$$(2.14)\qquad f(w, y) = s(w, y, n),$$

where w is the Goedel number of a polynomial and $n=(w)_0$. Since s is an arithmetical function, we are able to write the desired arithmetical predicate in the following way:

$$(2.15)\qquad G(w) \wedge (n)[R(w, 0, n) \wedge M(w, y, n, z)],$$

where $R(w, 0, n)$ is the arithmetical predicate for $(w)_0=n$ and $M(w, y, n, z)$ is the arithmetical predicate for $s(w, y, n)=z$. We denote the predicate of (2.14) by $V(w, y, z)$. It is clear that the arithmetical predicate

$$(2.16)\qquad A(x) \equiv (\exists w)[K(x) \wedge V(w, x, 0')]$$

expresses "x is a real algebraic number." Also, the sum and product relations for our isomorphic copy of $\mathscr{R}_0$ are just the restrictions of the sum and product relations of $\mathscr{R}'$ by $A(x)$. Our conclusion is that $\mathscr{R}_0$ is an AD-structure. We choose to use $\mathscr{R}_1$ for this isomorphic image of $\mathscr{R}_0$.

Our next theorem concerns the field of constructible numbers. For a precise definition, see [12]. The constructible numbers are simply those algebraic numbers which are generated from the number 1 via finitely many rational operations and extraction of square roots. A characterization which is crucial for our work here is that "α is constructible if and only if the order of the Galois group of the splitting field of the minimal polynomial of α (over Q) is a power of 2". There is need to admonish the incautious reader, for not every algebraic number of degree a power of 2 is constructible. As a prelude to our theorem we outline van der Waerden's approach to an effective construction of the Galois group of an irreducible polynomial (over Q).

Let $\alpha \in A_0$ (i.e., the field of algebraic numbers). And let $f(z)=\operatorname{Irr}(\alpha, Q)$ (i.e., $f(z)$ is the unique irreducible, monic polynomial of α over Q). If the degree of $f(z)$ is n then there exist n distinct conjugates of α, say $\alpha_1, \alpha_2, \ldots, \alpha_n$. Further, let $x_1, \ldots, x_n$ be n indeterminates and let

$$\theta = \sum_{i=1}^{n} x_i\alpha_i.$$

When $\sigma \in S_n$ (symmetric group on n symbols) we shall use $\theta\sigma$ to denote

$$\sum_{i=1}^{n} x_{i\sigma}\alpha_i.$$

Consider the following polynomial:

$$F(x_1, \ldots, x_n, z) = \prod_{\sigma\in S_n} (z - \theta\sigma).$$

Since this product is a symmetric function of the roots of $f(z)$, we can appeal to the theory of symmetric functions to conclude that $F(x_1, \dots, x_n, z) \in Q[x_1, \dots, x_n, z]$.

Let $F_1, \dots, F_r$ be the irreducible factors of F over $Q[x_1, \dots, x_n]$. We may assume that the factors have been ordered in such a way that $(z - \theta) \mid F_1$. Now it is clear that the following set (that we choose to denote by G_f) is a subgroup of S_n:

$$G_f = \{\sigma \in S_n : (z - \theta\sigma) \mid F_1\}.$$

In fact it is proved in [10] that G_f is the Galois group of polynomial $f(z)$ (relative to Q).

Let us not fail to observe two things concerning the above:

(2.17) θ is an algebraic element over the field $Q(x_1, \dots, x_n)$ and its irreducible polynomial has coefficients in a subring of this field, namely $Q[x_1, \dots, x_n]$.

(2.18) $$O(G_f) = \text{degree of } F_1.$$

THEOREM 2B. *The field of constructible numbers is an AD-structure.*[3]

Proof. Our task is to express formally in some way that "α is constructible", by expressing that "$O(G_f)$ is a power of 2", i.e., by expressing that "the degree of F_1 is a power of 2". This is sufficient since the degree of any normal extension of Q is equal to the order of its Galois group.

It is known that if $\mathscr{F}$ is a computable field then the ring $\mathscr{F}[x_1, \dots, x_n, \dots]$ (where $x_1, \dots, x_n, \dots$ is an infinite sequence of indeterminates) is computable. See, for example, [1]. Implicit in this proof of the computability of

$$\mathscr{F}[x_1, \dots, x_n, \dots]$$

is the fact that $\mathscr{F}[x_1, \dots, x_n, \dots]$ can be represented in $\mathscr{N}$ in such a way that the set $S' = \{x'_1, x'_2, \dots, x'_n, \dots\} \subseteq \mathscr{N}$ which represents $S = \{x_1, \dots, x_n, \dots\}$ is recursively enumerable in the given order.

For a proof of the fact that A_0 is computable, see [5].

So, without further delay, we assume that the ring $A_0[x_1, \dots, x_n, \dots]$ is computable; and assume further that the set $S' = \{x'_1, \dots, x'_n, \dots\}$ is recursively enumerable (in the given order). Let ϕ be a recursive function which enumerates S' (in the above order) without repetitions. It is easily verified that A_0, Q and $Q[x_1, \dots, x_n, \dots]$ are arithmetical substructures of $A_0[x_1, \dots, x_n, \dots]$.

We use arithmetical predicate "$A_0(a)$" and "$Rx(a)$" to denote "$a \in A_0$" and "$a \in Q[x_1, \dots . x_n, \dots]$", respectively.

Now in much the same way as before, we assign Goedel numbers to the elements of $A_0[x_1, \dots, x_n, \dots][z]$. So, for some $a_0, \dots, a_m$ such that

$$a_0, \dots, a_m \in A_0[x_1, \dots, x_n, \dots],$$

if $p(z) = a_0 + a_1 z + \cdots + a_m z^m$, $(a_m \neq 0)$ then for the Goedel number of $p(z)$, we take w, defined by: $w = 2^m 3^{a'_0} \cdots p_{m+2}^{a'_m}$ where each a'_i is the natural number which

[3] See footnote (2).

represents a_i in $\mathscr{N}$. Denote the totality of these numbers by "$\mathscr{D}$". As before, we can express arithmetically that the arithmetical predicate $G(w)$ asserts "w is the Goedel number of a polynomial in $A[x_1, \ldots, x_n, \ldots][z]$".

At this point we remind ourselves of the fact that the following predicates are arithmetical:

(2.19) $C(w, i, a)$, which expressed that "a is the ith-coefficient of the polynomial having Goedel number w".

(2.20) $D(w, n)$, which expresses that "n is the degree of the polynomial having Goedel number w".

For (2.19) we use:

$$G(w) \wedge (i \geqq 0) \wedge (\exists j)[(i+1 = j) \wedge ((w)_j = a)].$$

In addition, we want to be able to express the following arithmetically:

(2.21) "β is the value which results when the indeterminate z of the polynomial of Goedel number w is replaced by α";

(2.22) "the polynomial of Goedel number w is the minimal polynomial for α".

Certainly (2.21) brings to mind the predicate "$V(w, \alpha, \beta)$" of the earlier paragraphs of this section; however, we must keep in mind that the size (relative to set-containment) of the set of polynomials has been increased. Let us recall that the polynomials $p(z) \in A_0[x_1, \ldots, x_n, \ldots][z]$ that we are considering have their coefficients in the computable structure $A_0[x_1, \ldots, x_n, \ldots]$ and they have been assigned Goedel numbers in the same manner as the polynomials $p(z) \in Q[z]$. Now to obtain the arithmetical predicate of (2.21) we simply mimic the above approach for determining the arithmetical predicate $V(w, \alpha, \beta)$. To avoid confusion, we choose to denote the resulting arithmetical predicate by "$V_1(w, \alpha, B)$".

A point of clarification is needed in the case of (2.22); since when one talks about the minimal polynomial of an "algebraic element", the ground field should be clearly delineated. Otherwise the word "algebraic element" is ambiguous. Our work in this section requires that we distinguish two cases:

(2.23) "The polynomial of Goedel number w is the minimal polynomial for α over Q".

(2.24) "The polynomial of Goedel number w is the minimal polynomial for θ' over $Q(x_1, x_2, \ldots, x_n)$.

For number (2.23) simply take

$$(\exists n)[[D(w, n) \wedge C(w, n, 1) \wedge V(w, \alpha, 0')] \\ \wedge (w_1)(k)[[D(w_1, k) \wedge V(w_1, \alpha, 0')] \supset (k \geq n)]].$$

We choose to denote this arithmetical predicate by "$M(w, \alpha)$".

In the case of (2.24), we find that things are not so simple; since in our discussion so far we have used only the computability of $A_0[x_1, \ldots, x_n, \ldots]$ and various of its subsystems. The field $Q(x_1, \ldots, x_n)$ is not included among these. However, the only elements algebraic over $Q(x_1, \ldots, x_n)$ that we are worried about are those elements $\theta\sigma (\sigma \in S_n)$ which were referred to in our brief discussion of Galois theory. Recall that the minimum polynomials for these elements have their coefficients in $Q[x_1, \ldots, x_n]$. We shall see shortly that there is no need to express "$\theta' = \theta\sigma$ (for some $\sigma \in S_n$) is algebraic over $Q(x_1, \ldots, x_n)$"; it suffices to express "$\theta' = \theta\sigma \in A_0[x_1, \ldots, x_n, \ldots]$ implies that there exists a unique monic polynomial of minimum degree, say $p(z)$, such that $p(z) \in Q[x_1, \ldots, x_n, \ldots][z]$ and $P(\theta') = 0$". Before continuing our proof, we need to establish:

2.25. Lemma. *Let $p(z) \in Q[x_1, \ldots, x_n][z]$ such that $p(z)$ is the minimum polynomial for θ'.*

(a) *If $q(z)$ is a monic polynomial of $Q[x_1, \ldots, x_n, x_{n+1}][z]$ such that $q(\theta') = 0$ and* $\deg (q(z)) \leqq \deg (p(z))$ *then* $q(z) = p(z)$ (*so*, $\deg (q(z)) \not< \deg (p(z))$).

(b) *For any $r > 1$, if $q(z)$ is a monic polynomial over $Q[x_1, \ldots, x_n, x_{n+1}, \ldots, x_{n+r}]$ such that $q(\theta') = 0$ and* $\deg (q(z)) \leqq \deg (p(z))$ *then* $q(z) = p(z)$ (*so*, $\deg (q(z)) \not< \deg (p(z))$).

Proof. We can do (a) very simply as follows: Let $q(z)$ be as in (a). Rewrite $q(z)$ as a polynomial in x_{n+1}. So $q(z) = b_0(z) + b_1(z)x_{n+1} + b_2(z)x_{n+1}^2 + \cdots + b_k(z)x_{n+1}^k$, where each $b_i(z) \in Q[x_1, \ldots, x_n][z]$. Since $q(\theta') = 0$, necessarily $b_0(\theta') = b_1(\theta') = \cdots = b_k(\theta') = 0$. But $b_0(z)$ must contain the largest power of z and $b_0(z)$ is monic; moreover, since $\deg (p(z)) \geqq \deg (b_0(z))$, $b_0(z)$ is monic and $b_0(\theta') = 0$, we must have that $b_0(z) = p(z)$. Therefore

$$q(z) = p(z) + b_1(z)x_{n+1} + \cdots + b_k(z)x_{n+1}^k.$$

But we should observe further that since $q(z)$ is monic $b_0(z)$ contains the largest power of z and no other b_j contains the largest power of z, each $b_i(z)$ is such that either $b_i(z) \equiv 0$ or $\deg (b_i(z)) < \deg (p(z))$. But each $b_i(z)$ is such that $b_i(\theta') = 0$, therefore $b_i(z) \equiv 0$ for each i and $p(z) = q(z)$.

The proof of (b) follows very simply by induction on r.

Now if $q(z) \in Q[x_1, \ldots, x_n, \ldots][z]$, $q(z)$ is monic, and such that $\deg (q(z)) = \deg (p(z))$ and $q(\theta') = 0$, then for some $s \geqq 1$, we have that $q(z) \in Q[x_1, \ldots, x_s][z]$. Either $s \leqq n+1$ or $s > n+1$; and hence either $q(z) \in Q[x_1, \ldots, x_n, x_{n+1}][z]$ or $q(z) \in Q[x_1, \ldots, x_n, x_{n+1}, \ldots, x_{n+r}][z]$, for some $r \geqq 1$. By either (a) or (b) we have that $q(z) = p(z)$.

Now, for the desired arithmetical predicate we take

$$V_1(w, \theta', 0') \wedge [(i)(a)(i > 0) \wedge C(w, i, a) \supset Rx(a)] \wedge (\exists n)[[D(w, n) \wedge C(w, n, 1)] \\ \wedge (w_1)(k)[D(w_1, k) \wedge V_1(w_1, \theta', 0')] \supset (k \geqq n)].$$

Denote this predicate by "$M_1(w, \theta')$".

Our major task for the moment is to express arithmetically "θ is of the form $\sum_{i=1}^{n} x_i\alpha_i$ where α_i are the distinct conjugates of α".

Let $\psi(a_0+a_1z+\cdots+a^mz^m)=a_0+a_1x+\cdots+a_mx_m$; this is to say z^i is replaced by x_i throughout the given polynomial. Let $\mathscr{D}_0$ be the set:

$\{w\in\mathscr{N}$: w is the Goedel number of a polynomial in $A_0[z]\}$. It is clear that $\mathscr{D}_0$ is a recursive set. We use "$G_0(w)$" to express that $w\in\mathscr{D}_0$.

Let $\psi':\mathscr{D}_0\rightarrow\mathscr{N}$ be the function induced by the function ψ above. This is to say, corresponding to $p(z)\in A_0[z]$ is a natural number $w\in\mathscr{D}_0$ and corresponding to $\psi(p(z))$ is a natural number $\lambda\in\mathscr{N}$; so we have that $\psi'(w)=\lambda$.

Observe that ψ' is completely determined by the following pair of equations

$$\psi'(2^0 3^{a_0'}) = a_0',$$

$$\psi'(2^{k+1}3^{a_0'}\cdots p_{k+1}^{a_{k+1}'}) = \sigma(\psi(2^k 3^{a_0'}\cdots p_k^{a_k'}), \pi(a_{k+1}', \phi(k+1))),$$

where σ represents "sum" in $A_0[x_1',\ldots,x_n',\ldots]$, π represents "product" in $A_0[x_1',\ldots,x_n',\ldots]$ and ϕ is the recursive function which enumerates $S'=\{x_1', x_2',\ldots,x_n',\ldots\}$ (in the given order) without repetitions. We want a (total) recursive function which behaves like ψ' on $\mathscr{D}_0$.

Define a binary (total) function τ by

$$\tau(k, x) = 2^k \prod_{1\leqq x\leqq k} p_i^{(x)_i}.$$

Previous observations give rise immediately to the fact that τ is recursive. Further we define a binary (total) function ψ_1 by

$$\psi_1(0, x) = (x)_1,$$

$$\psi_1(k+1, x) = \sigma(\psi_1(k, \tau(k, x)), \pi((x)_{k+1}, \varphi(k+1))).$$

ψ_1 is clearly recursive in the functions π, σ, τ, (x), and φ; and so ψ_1 is recursive. Also, let us observe the action of ψ_1 on those pairs of the form $((x)_0, x)$ where $x\in\mathscr{D}_0$. It is indeed clear that ψ_1 behaves as desired on such pairs; i.e., $\psi_1((x)_0, x)=\psi'(x)$, when $x\in\mathscr{D}_0$. Therefore, if we denote the arithmetical predicate which the function ψ_1 defines by "$L_1(n, w, \lambda)$", then the desired arithmetical predicate can be expressed as follows:

$$(\exists n)[L_1(n, w, \lambda) \wedge G_0(w) \wedge ((w_0) = n)].$$

We choose to denote this arithmetical predicate by "$L(w, \lambda)$". $L(w, \lambda)$ expresses that "λ represents a polynomial in $A_0[x_1,\ldots,x_n,\ldots]$ which is the image (under ψ_0) of the polynomial in $A_0[z]$ whose Goedel number is w".

Now, let us get back to the task of expressing "θ represents an element of the form $\sum_{i=1}^{n} x_i\alpha_i$" in our language. This is now easy to do. Suppose $p(z)$ is of the form $\alpha_1z+\alpha_2z^2+\cdots+\alpha_nz^n$ where $\alpha_1,\ldots,\alpha_n$ are the distinct conjugates of α (in any order). Then $\psi(p(z))=\alpha_1x_1+\alpha_2x_2+\cdots+\alpha_nx_n$. Consider the following arithmetical predicate:

$$(2.26)\quad \begin{aligned}&(\exists n)[[D(w, n) \wedge G_0(w)] \wedge (\exists w_0)[M(w_0, \alpha) \wedge D(w_0, n)]\\ &\qquad \wedge C(w, 0, 0') \wedge (i)_i<_n(\exists\alpha')[C(w, i, \alpha') \supset V(w_0, \alpha', 0')]].\end{aligned}$$

This expresses "w is the Goedel number of a polynomial of the above form", where the requirement for distinct conjugates is not enforced. One can get the requirement of distinct conjugates by simply using $(\exists n)[D(w, n) \wedge G_0(w) \wedge M(w,\alpha)]$. So we further let $T(n, \alpha, w)$ denote the arithmetical predicate of (2.26) with the initial existential quantifier deleted. Then, let $T_1(\alpha, w)$ be the following arithmetical predicate:

$$(\exists n)[T(n, \alpha, w) \wedge (i)(j)(\gamma)(\delta)[(i < j \leqq n) \wedge C(w, i, \gamma) \wedge C(w, j, \delta) \supset (\gamma \neq \delta)]].$$

The arithmetical predicate $T_1(\alpha, w)$ expresses "w is the Goedel number of a polynomial of the above form".

Now use "$R(\alpha, \theta)$" for "$(\exists w)[T_1(\alpha, w) \wedge L(w, \theta)]$". This arithmetical predicate expresses that θ represents an expression of the desired form. Speaking loosely, we have been able to express that θ is constructed from the x_i's and the conjugates of α according to the dictates of Van der Waerden's approach to the construction of Galois groups.

Consider the predicate $G_1(\alpha, m)$ which is given by:

$$(2.27)\qquad (\exists\theta)(\exists w_1)[R(\alpha, \theta) \wedge M_1(w_1, \theta) \wedge D(w_1, m)].$$

This arithmetical predicate expresses, in effect, "the Galois group of the splitting field for the minimal polynomial of α has order m". Now we can express arithmetically that "α is constructible" with the arithmetical predicate

$$A_0(\alpha) \wedge (\exists m)[G_1(\alpha, m) \wedge (\exists k)(m \mid 2^k)].$$

Denote this arithmetical predicate by "$C_0(\alpha)$". This establishes our theorem.

We shall call an algebraic number α *solvable* (a "surd") in case its minimal polynomial is solvable by radicals; i.e., α is a solvable number in case the Galois group of its minimal polynomial is a solvable group. It is clear that the set of solvable numbers is a subfield of the field of algebraic numbers since our definition is equivalent to: "α is solvable if and only if it results from the number 1 by a finite number of rational operations and extraction of roots $((\cdot)^{1/2}, (\cdot)^{1/3}, \ldots)$".

THEOREM 2C. *The field of solvable numbers is an AD-structure.*[4]

Proof. From the above discussion on the field of constructible numbers, we borrow the arithmetical predicate of (2.27), i.e., $G_1(\alpha, m)$. Recall that this predicate expresses "the Galois group of the splitting field for the minimal polynomial of α

[4] See footnote [2].

has order m". In addition to the predicate $G_1(\alpha, m)$, we shall determine an arithmetical predicate, say $S_1(w, \beta)$, which expresses "β is an element of the splitting field of the minimal polynomial having Goedel number w". It appears that $S_1(w, \beta)$ can best be determined after we have been able to express "θ_0 is a primitive element for the splitting field of the polynomial having Goedel number w" by an arithmetical predicate, say $P_1(w, \theta_0)$. Consider the arithmetical predicate

$$(\exists w)[M(\alpha, w) \wedge D(w, n)]$$

which expresses "α is of degree n"; denote it by "$D_1(\alpha, n)$". Now for the arithmetical predicate $P_1(w, \theta_0)$, we simply take

$$(2.29) \qquad (\alpha)[M(w, \alpha) \supset (\exists w')[V(w', \theta_0, \alpha) \wedge (\exists n)[D_1(\theta_0, n) \wedge G_1(\alpha, n)]]].$$

It is clear that (2.29) expresses "θ_0 is a primitive element of the splitting field of the minimal polynomial of Goedel number w". Now trivially the arithmetical predicate

$$(\exists \theta_0)[P_1(w, \theta_0) \wedge (w_1)V(w_1, \theta_0, \beta)]$$

expresses "β is an element of the splitting field of the minimal polynomial of Goedel number w". We remind the reader that this arithmetical predicate is denoted by "$S_1(w, \beta)$".

Before proceeding further with our problem, we find it necessary to take a brief excursion into the theory of finite groups. Recall that a finite group is said to be solvable if and only if it has a composition series whose factor groups are cyclic of prime order. Also, recall the following definition:

(2.30) Let G be a group of order $p^m s$, where p is a prime and g.c.d. $(p^m, s) = 1$. A subgroup of G of order s is a p-complement of G.

Using this definition we can state a characterization theorem for finite solvable groups which is due to P. Hall. See [8] for a proof of

(2.31) A finite group is solvable if and only if it has a p-complement, for every prime p.

This result will allow us to express arithmetically "the Galois group of the splitting field of the polynomial of Goedel number w is solvable". Consider the following:

$$(2.32) \qquad \begin{aligned} &(\exists w)(\exists n)[[M(w, \alpha) \wedge G_1(\alpha, n)] \wedge (m)(p)[Pr(p) \\ &\quad \wedge (s)((\text{g.c.d. } (s, p^m) = 1) \wedge (p^m s = n)) \supset (\exists \beta)[D_1(\beta, p^m) \wedge S_1(W, \beta)]]] \end{aligned}$$

where $Pr(p)$ expresses that "p is a prime". This arithmetical predicate expresses, in fact, that whenever the degree n of the splitting field of the minimal polynomial of α is of the form $p^m s$ (where $(p^m, s) = 1$) then the splitting field has an element β of degree p^m. Of course, by purely algebraic considerations, we know that $Q(\beta)$ is of degree p^m and is a subfield of Q_f (i.e., the splitting field for $f(x) = \text{Irr}(\alpha, Q)$).

Therefore $[Q_f\colon Q(\beta)]=s$; hence, by the fundamental theorem of Galois Theory, G_f (i.e., the Galois group of the splitting field of $f(x)$) has a subgroup of order s.

We have, in effect, been able to express that G_f has a p-complement for every prime p; thus by the theorem of P. Hall above, we have that G_f is solvable and hence $f(x)$ is solvable by radicals. Whence, any zero of $f(x)$ is a solvable number. So, (2.32) is used to express "α is a solvable number". This establishes our theorem.

3. **Some existence theorems.** We shall, first of all, prove a theorem concerning the field of real algebraic numbers, $\mathscr{R}_0$. Let H denote the Peano axioms relativized by the predicate $N(x)$. Further, let $K_1=K_0\cup H$, where K_0 is the set of axioms for the concept of real-closed field. Any model of K_1 is a real-closed field whose elements which satisfy $N(x)$ constitute a (weak) model of arithmetic. The model $\{\mathscr{R}_0;\mathscr{N}\}$ is a model of K_1.

THEOREM 3A. *Let $\mathscr{N}^*$ be any (strong) model of arithmetic. There exists a model, say $\mathscr{R}^*$, in which $\mathscr{N}^*$ is embedded such that $\{\mathscr{R}^*;\mathscr{N}^*\}$ is a model of K_1 and is, moreover, elementarily equivalent to $\{\mathscr{R}_0;\mathscr{N}\}$.*

Proof. A. Robinson has shown in [6] that K_1 is not complete; thus, this assertion is not a consequence of completeness. We should mention again that our technique in this section is essentially the same that A. Robinson used in [6] to establish a similar result for the field of algebraic numbers. Recall from §2 the predicates $N'(x)$ and $A(x)$ of (2.7) and (2.16), respectively. The predicate $A(x)$ defines the "set-part" of the arithmetical structure which is isomorphic to $\mathscr{R}_0$. As a model of K_1, we choose to denote this structure by $\{\mathscr{R}_1;\mathscr{N}_1\}$ where $\mathscr{N}_1$ is the subset of $\mathscr{N}$ which is defined by the predicate $N'(x)$. The sum and product relations of $\{\mathscr{R}_1;\mathscr{N}_1\}$ are defined by $[A(x)\wedge A(y)\wedge A(z)]\wedge S'(x,y,z)$ and $[A(x)\wedge A(y)\wedge A(z)]\wedge P'(x,y,z)$, respectively.

For notation, let $\mathscr{R}_*$ and $\mathscr{N}_*$ be subsets of $\mathscr{N}^*$ defined by

$$\mathscr{R}_* = \{z\in\mathscr{N}^* \mid A(z) \quad \text{holds in } \mathscr{N}^*\}$$

and

$$\mathscr{N}_* = \{z\in\mathscr{N}^* \mid N'(z) \quad \text{holds in } \mathscr{N}^*\}.$$

We shall use $\{\mathscr{R}_*;\mathscr{N}_*\}$ to denote the algebraic structure (with distinguished subset $\mathscr{N}_*$) whose sum and product relations are defined in $\mathscr{N}^*$ by the above predicates which define sum and product for $\{\mathscr{R}_1;\mathscr{N}_1\}$ in $\mathscr{N}$.

We shall presently show that the structure $\{\mathscr{R}_*;\mathscr{N}_*\}$ behaves according to the dictates of our theorem; i.e., on the one hand $\{\mathscr{R}_*;\mathscr{N}_*\}$ is a model of K_1 which is elementarily equivalent to $\{\mathscr{R}_0;\mathscr{N}\}$ and on the other hand $\mathscr{N}_*$ is isomorphic to $\mathscr{N}^*$.

Let X be any true sentence of $\{\mathscr{R}_0;\mathscr{N}\}$. "Translate" X into a sentence, say X', according to the following prescription:

(3a) Replace each occurrence of 0 by $0'$.

(3b) Replace each occurrence of the relational symbols $S(x, y, z)$, $P(x, y, z)$ and $N(x)$ by the arithmetical predicates $S'(x, y, z)$, $P'(x, y, z)$ and $N'(x)$, respectively.

(3c) Relativize the sentence resulting from applications of (a) and (b) by the arithmetical predicate $A(x)$.

Since $\{\mathscr{R}_0; \mathscr{N}\}$ and $\{\mathscr{R}_1; \mathscr{N}_1\}$ are isomorphic, we have that:

(i) $S(x, y, z)$ holds in $\{\mathscr{R}_0; \mathscr{N}\}$ if and only if $S'(x, y, z)$ holds in $\{\mathscr{R}_1; \mathscr{N}_1\}$,

(ii) $P(x, y, z)$ holds in $\{\mathscr{R}_0; \mathscr{N}\}$ if and only if $P'(x, y, z)$ holds in $\{\mathscr{R}_1; \mathscr{N}_1\}$,

(iii) $N(x)$ holds in $\{\mathscr{R}_0; \mathscr{N}\}$ if and only if $N'(x)$ holds in $\{\mathscr{R}_1; \mathscr{N}_1\}$.

It is clear from these observations, the fact that $\mathscr{N}_1 \subseteq \mathscr{R}_1$ and the construction of X' that X' is true in $\mathscr{N}$. Now, $\mathscr{N}^*$ is a strong model of arithmetic, therefore X' holds also in $\mathscr{N}^*$. Again, by the above observations, the fact that $\mathscr{N}_* \subseteq \mathscr{R}_*$ and the construction of X', we have that X holds in $\{\mathscr{R}_*; \mathscr{N}_*\}$.

Since this procedure works for an arbitrary true sentence in $\{\mathscr{R}_0; \mathscr{N}\}$, it is clear that $\{\mathscr{R}_*; \mathscr{N}_*\}$ is a model of K_1. It is not difficult to show that $\mathscr{N}^*$ is imbedded in the real-closed field $\mathscr{R}_*$; indeed, it suffices to show that $\mathscr{N}^*$ is isomorphic to $\mathscr{N}_*$. Consider the mapping $\lambda: \mathscr{N} \rightarrow \mathscr{N}_*$, defined by: $x\lambda = y$ if and only if $B(x, y)$ holds in $\mathscr{N}^*$, where $B(x, y)$ is introduced just preceding (2.4). Since $\mathscr{N}^*$ is a strong model of arithmetic, the sentences of (2.4), (2.5) and (2.6), which are true sentences in $\mathscr{N}$, are true in $\mathscr{N}^*$. As for the desired properties of the mapping λ, it is clear that the well-definedness and ontoness are immediate consequences of (2.4); while its one-to-oneness and the fact that it is a homomorphism follow from (2.5) and (2.6), respectively. Therefore, λ is an isomorphism of $\mathscr{N}^*$ onto $\mathscr{N}_*$.

Having successfully embedded $\mathscr{N}^*$ in a real-closed field using the theory of arithmetical definability, we can repeat the foregoing process to show that $\{\mathscr{R}_0; \mathscr{N}\}$ is elementarily equivalent to $\{\mathscr{R}_*; \mathscr{N}_*\}$. For any sentence X which holds in $\{\mathscr{R}_*; \mathscr{N}_*\}$ can, in the above way, be "translated" into a sentence X' which is true in $\mathscr{N}^*$. But, since $\mathscr{N}^*$ is a strong model of arithmetic, X' also holds in $\mathscr{N}$; and, as before, this implies that X holds in $\{\mathscr{R}_1; \mathscr{N}_1\}$. But, $\{\mathscr{R}_1; \mathscr{N}_1\}$ is isomorphic to $\{\mathscr{R}_0; \mathscr{N}\}$; whence, X holds in $\{\mathscr{R}_0; \mathscr{N}\}$. And so X holds in $\{\mathscr{R}_0; \mathscr{N}\}$ if and only if X holds in $\{\mathscr{R}_*; \mathscr{N}_*\}$. There is no further need to remind ourselves that $\mathscr{R}_* \subseteq \mathscr{N}^*$; so when we talk further about a model in which $\mathscr{N}^*$ is embedded which is elementarily equivalent to $\{\mathscr{R}_0; \mathscr{N}\}$, we shall use the notation $\{\mathscr{R}^*; \mathscr{N}^*\}$.

Once we observe that our proof has depended only on the fact that $\mathscr{R}_0$ is an AD-structure, we can state this result for an entire class of relation models. In particular, we have at once that

THEOREM 3B. *Given the field of constructible numbers $\{C_0; \mathscr{N}\}$ and any strong model of arithmetic $\mathscr{N}^*$, we can find a field C_0^* such that $\mathscr{N}^* \subseteq C_0^*$ and $\{C_0^*; \mathscr{N}^*\}$ is elementarily equivalent to $\{C_0; \mathscr{N}\}$.*

THEOREM 3C. *Given the field of solvable numbers $\{S_0; \mathscr{N}\}$ and any strong model of arithmetic $\mathscr{N}^*$, we can find a field S_0^* such that $\mathscr{N}^* \subseteq S_0^*$ and $\{S_0^*; \mathscr{N}^*\}$ is elementarily equivalent to $\{S_0; \mathscr{N}\}$.*

As a kind of corollary to Theorem 3A we shall prove a metamathematical analogue of a classical theorem of algebra. The theorem states simply that "$\mathscr{R}_0$ has no proper algebraic extensions"([5]).

THEOREM 3D. *$\{\mathscr{R}_0; \mathscr{N}\}$ has no proper elementary extension in which $\mathscr{N}$ is fixed. Equivalently, if $\{\mathscr{R}^*; \mathscr{N}^*\}$ is a proper elementary extension of $\{\mathscr{R}_0; \mathscr{N}\}$ then $\mathscr{N}^* \supsetneqq \mathscr{N}$.*

Proof. Assume, for the moment, that $\{\mathscr{R}^*; \mathscr{N}\}$ is a proper extension of $\{\mathscr{R}_0; \mathscr{N}\}$. Certainly, if $\mathscr{R}^*$ is an AD-structure then $\{\mathscr{R}^*; \mathscr{N}\}$ is not an elementary extension of $\{\mathscr{R}_0; \mathscr{N}\}$, lest one can proceed in the manner of §2 to get the sentence $(x)A(x)$ which holds in both $\{\mathscr{R}_0; \mathscr{N}\}$ and $\{\mathscr{R}^*; \mathscr{N}\}$. But this cannot happen since any such extension of $\{\mathscr{R}_0; \mathscr{N}\}$ contains transcendental elements. A careful examination of §1 should convince the careful reader that the notion of arithmetical definability of $\mathscr{R}^*$ is crucial for this simple argument to work.

Consider the following property of the elements of $\mathscr{R}_0$:

(3.1) If $\alpha \in \mathscr{R}_0$, then there exists a polynomial (over Q) $p(y)$ and rational numbers r and s such that whenever $r \leqq \lambda < \alpha$, then $p(\lambda) < 0$ and whenever $\alpha < \lambda \leqq s$, then $p(\lambda) > 0$.

This is one of many ways of expressing that α is a real algebraic number. With the help of certain predicates discussed so far and (3.1), we shall find a sentence which holds in $\{\mathscr{R}_0; \mathscr{N}\}$ and does not hold in any proper extension of the kind referred to above. It is only the computability of the rational numbers that we shall use for this task. From §2, we assume familiarity with the arithmetical predicates $B(x, y)$ and $V(w, x, y)$.

First of all, we want to find an arithmetical predicate, say $\bar{B}(x, y)$, which expresses that "the natural number y represents the rational number x" under the mapping which helps to establish the computability of Q.

Let $R(x, a, b)$ be the predicate which results by deleting the initial existential quantifiers of the predicate $R(x)$ of (2.9). We choose the following predicate relativised by $N(x)$ for $\bar{B}(x, y)$:

$$(\exists a)(\exists b)(\exists a')(\exists b')[R(y, a', b') \wedge B(a, a') \wedge B(b, b') \wedge P(b, x, a)].$$

So, $(x)(\exists y)\bar{B}(x, y)$ holds in Q.

Use $C(w, \alpha, s)$ and $D(w, \alpha, r)$ to denote the following predicates:

$$(\lambda)[(\alpha < \lambda \leqq s) \supset (\exists \lambda')(\exists \lambda)[\bar{B}(\lambda, \lambda') \wedge V(w, \lambda', u) \wedge (u \succ 0')]]$$

and

$$(\lambda)[(r \leqq \lambda < \alpha) \supset (\exists \lambda')(\exists u)[\bar{B}(\lambda, \lambda') \wedge V(w, \lambda', u) \wedge (u \prec 0')]],$$

[5] The statement "$\mathscr{R}$ has no proper algebraic extensions" is often taken as the definition of the concept of real-closed fields providing $\mathscr{R}$ is formally real. Here, we are using the definition of real-closed field formulated in [6], since it is expressible in our language, i.e., $\mathscr{R}$ is real-closed in case $\mathscr{R}$ is an ordered field in which every polynomial of odd degree (over $\mathscr{R}$) has a root in $\mathscr{R}$.

respectively. The symbol $0'$ is the natural number which represents 0 and $\succ$ and $\prec$ are the relations which represent $>$ and $<$ respectively.

The desired predicate is now easily expressed. Consider

$$(\exists w)(\exists r)(\exists s)[(r < \alpha < s) \wedge C(w, \alpha, s) \wedge D(w, \alpha, r)]. \tag{3.2}$$

Denote this predicate by "$\bar{A}(\alpha)$". $\bar{A}(\alpha)$ expresses in a rather artificial way that α is a real algebraic number. Now, $(\alpha)\bar{A}(\alpha)$ cannot possibly hold in a proper extension, say $\{\mathscr{R}^*; \mathscr{N}\}$ since such an extension must contain transcendental numbers.

4. A uniqueness theorem. Let $\{\mathscr{R}^*; \mathscr{N}^*\}$ be as in §3; i.e., a model of K_1 which is elementarily equivalent to $\{\mathscr{R}_0; \mathscr{N}\}$ and is definable (inside of $\mathscr{N}^*$) as in §3. Let $\mathscr{R}^{**}$ be another model containing $\mathscr{N}^*$ such that $\{\mathscr{R}^{**}; \mathscr{N}^*\}$ is also a model of K_1. The field of quotients from $\mathscr{N}^*$ (i.e., a nonstandard version of Q) is obviously embedded in both $\mathscr{R}^*$ and $\mathscr{R}^{**}$.

THEOREM 4A. *If $\{\mathscr{R}^*; \mathscr{N}^*\}$ and $\{\mathscr{R}^{**}; \mathscr{N}^*\}$ are elementarily equivalent (relative to Q^*) then they are, in fact, isomorphic.*

Proof. Consider the predicate of (2.38). Let $A_1(w, r, s, \alpha)$ be the predicate resulting from $A(x)$ by deleting the initial quantifiers. We can easily convince ourselves that the predicate $\bar{M}(w, \alpha)$ expressing "w is the Goedel number of the minimal polynomial of α or the negation of the minimal polynomial of α depending on which is increasing in a neighborhood of α" is arithmetical. Use $\bar{A}(w, r, s, \alpha)$ for $[A_1(w, r, s, \alpha) \wedge \bar{M}(w, \alpha)]$. It is clear that the following is a property of $\mathscr{R}_0$.

4.1. LEMMA. (a) *If $\alpha \in \mathscr{R}_0$ then there exists $w, r, s \in Q$ such that $A(w, r, s, \alpha)$ holds in $\mathscr{R}_0$.*

(b) $\bar{A}(w, r, s, \alpha) \Rightarrow [\bar{A}(w, r, s, \beta) \Rightarrow E(\alpha, \beta)]$ *holds in $\mathscr{R}_0$.*

Now if $\alpha \in \mathscr{R}^*$ then there exist $w_0, r_0, s_0 \in Q^*$ such that $\bar{A}(w_0, r_0, s_0)$ holds in $\mathscr{R}^*$. This follows by the (a) part of Lemma 4.2 and the elementary equivalence of $\{\mathscr{R}_0; \mathscr{N}\}$ and $\{\mathscr{R}^*; \mathscr{N}^*\}$. Now "$\bar{A}(w_0, r_0, s_0, \alpha)$ holds in $\{\mathscr{R}^*; \mathscr{N}^*\}$" implies that $(\exists x)\bar{A}(w_0, r_0, s_0, x)$ holds in $\{\mathscr{R}^*; \mathscr{N}^*\}$. By elementary equivalence, we have that $(\exists x)\bar{A}(w_0, r_0, s_0, x)$ holds in $\{\mathscr{R}^{**}; \mathscr{N}^*\}$; and hence there exists a $\beta \in \mathscr{R}^{**}$ such that $\bar{A}(w_0, r_0, s_0, \beta)$ holds in $\{\mathscr{R}^{**}; \mathscr{N}^*\}$. Define $h: \mathscr{R}^* \to \mathscr{R}^{**}$ by $h(\alpha) = \beta$.

Claim. h is an isomorphism of $\mathscr{R}_0^*$ onto $\mathscr{R}^{**}$.

4(i). *h is well-defined.*

If γ is such that $h(\alpha) = \gamma$ and $h(\alpha) = \beta$, then $\bar{A}(w_0, r_0, s_0, \gamma)$ and $\bar{A}(w_0, r_0, s_0, \beta)$ hold in $\mathscr{R}^{**}$. From Lemma 4.1 we obtain immediately that $E(\gamma, \beta)$ holds in $\mathscr{R}^*$.

4(ii). *h is onto.*

Let $\beta \in \mathscr{R}^{**}$. Then there exists $w_0, r_0, s_0 \in Q^*$ such that $\bar{A}(w_0, r_0, s_0, \beta)$ holds in $\mathscr{R}^{**}$. Thus $(\exists x)\bar{A}(w_0, r_0, s_0, x)$ holds in $\mathscr{R}^{**}$; and by elementary equivalence of $\mathscr{R}^*$ and $\mathscr{R}^{**}$ (relative to Q^*) we have that $(\exists x)\bar{A}(w_0, r_0, s_0, x)$ holds in $\mathscr{R}^*$. Therefore, there is an $\alpha \in \mathscr{R}^*$ such that $\bar{A}(w_0, r_0, s_0, \alpha)$ holds in $\mathscr{R}^*$. Whence, by definition of h, we have that $h(\alpha) = \beta$.

4(iii). *h is a homomorphism.*

We find it convenient to prove a lemma from which an immediate proof of this assertion follows.

4.2. Lemma. *Let $w_1, a_1, b_1, w_2, a_2, b_2, w, a, b \in Q^*$ and $\alpha_1, \alpha_2, \alpha \in \mathscr{R}^*$ such that $\bar{A}(w_1, a_1, b_1, \alpha_1)$, $\bar{A}(w_2, a_2, b_2, \alpha_2)$, $\bar{A}(w, a, b, \alpha)$ and $S(\alpha_1, \alpha_2, \alpha)$ hold in $\mathscr{R}^*$. Also let $\beta_1, \beta_2, \beta \in \mathscr{R}^{**}$ such that $\bar{A}(w_1, a_1, b_1, \beta_1)$, $\bar{A}(w_2, a_2, b_2, \beta)$ and $S(\beta_1, \beta_2, \beta)$ hold in $\mathscr{R}^{**}$. Our conclusion is that $\bar{A}(\beta, w, a, b)$ holds in $\mathscr{R}^{**}$.*

Proof. By choice of the constants in the hypotheses of Lemma 4.2, it is clear that the following sentence holds in $\mathscr{R}^*$:

$$(z)[S(\alpha_1, \alpha_2, z) \supset \bar{A}(w, a, b, z)].$$

And likewise, $\bar{A}(w_1, a_1, b_1, \alpha_1) \wedge \bar{A}(w_2, a_2, b_2, \alpha_2)$ holds in $\mathscr{R}^*$. Therefore

$$[\bar{A}(w_1, a_1, b_1, \alpha_1) \wedge \bar{A}(w_2, a_2, b_2, \alpha_2)] \wedge (z)[S(\alpha_1, \alpha_2, z) \supset \bar{A}(w, a, b, z)]$$

holds in $\mathscr{R}^*$. By the properties established in Lemma 4.1 it is clear that

$$(\exists ! x)(\exists ! y)[[\bar{A}(w_1, a_1, b_1, x) \wedge \bar{A}(w_2, a_2, b_2, y)] \wedge (z)[S(x, y, z) \supset \bar{A}(w, a, b, z)]]$$

holds in $\mathscr{R}^*$. But since $\mathscr{R}^*$ and $\mathscr{R}^{**}$ are elementarily equivalent (relative to Q^*) it is clear that the last sentence holds in $\mathscr{R}^{**}$. Again, by the choice of the constants in Lemma 4.2, we have that

$$[\bar{A}(w_1, a_1, b_1, \beta_1) \wedge \bar{A}(w_2, a_2, b_2, \beta_2)] \wedge (z)[S(\beta_1, \beta_2, z) \supset \bar{A}(w, a, b, z)]$$

holds in $\mathscr{R}^{**}$. But $\bar{A}(w_1, a_1, b_1, \beta_1) \wedge \bar{A}(w_2, a_2, b_2, \beta_2)$ holds in $\mathscr{R}^{**}$; and so $(z)[S(\beta_1, \beta_2, z) \supset \bar{A}(w, a, b, z)]$ holds in $\mathscr{R}^{**}$. And so, $S(\beta_1, \beta_2, \beta) \supset \bar{A}(w, a, b, \beta)$ holds in $\mathscr{R}^{**}$. Also, by the hypotheses $S(\beta_1, \beta_2, \beta)$ holds in $\mathscr{R}^{**}$. Therefore $\bar{A}(w, \beta, a, b)$ holds in $\mathscr{R}^{**}$. This proves our Lemma 4.2.

Further, we claim that if in the statement and proof of Lemma 4.2 we replace the predicate $S(x, y, z)$ by $P(x, y, z)$ then all is well and we have precisely the machinery that we need to prove 4(iii). Call the resulting statement Lemma 4.3.

The proof of 4(iii) follows once we reinterpret Lemma 4.2 and the unwritten Lemma 4.3 in light of the definition of the mapping h. From Lemma 4.2 we infer that: If $h(\alpha_1) = \beta_1$, $h(\alpha_2) = \beta_2$, $\alpha = \alpha_1 + \alpha_2$ and $\beta = \beta_1 + \beta_2$ then $h(\alpha) = \beta$. From the unwritten Lemma 4.3, we infer that: If $h(\alpha_1) = \beta_1$, $h(\alpha_2) = \beta_2$, $\alpha = \alpha_1 \cdot \alpha_2$ and $\beta = \beta_1 \cdot \beta_2$ then $h(\alpha) = \beta$. Now we come to the final property of h that is needed to complete the proof of the theorem.

4(iv). *h is one-one.*

Suppose that for some $\alpha \in \mathscr{R}^*$, $h(\alpha) = 0$. Then, there exist $w_0, r_0, s_0 \in Q^*$ such that $\bar{A}(w_0, r_0, s_0, \alpha)$ holds in $\mathscr{R}^*$ while $\bar{A}(w_0, s_0, r_0, 0)$ holds in $\mathscr{R}^{**}$. But the constants 0, w_0, s_0, and r_0 all belong to Q^* and hence by elementary equivalence $\bar{A}(w_0, r_0, s_0, 0)$ holds in $\mathscr{R}^*$. Another look at Lemma 4.1 establishes that $E(\alpha, 0)$ holds in $\mathscr{R}^*$. We have established that the kernel of the homomorphism consists of the single element

0; thus the one-to-oneness of h follows. Our conclusion is that $\mathscr{R}^*$ and $\mathscr{R}^{**}$ are isomorphic.

Finally, we want to call the reader's attention to a relationship between Theorem 4A of the present section and Theorem 3D of §3. First of all, the conclusion of our uniqueness theorem still holds if we assume that $\{\mathscr{R}^{**}; \mathscr{N}^*\}$ and $\{\mathscr{R}^*; \mathscr{N}^*\}$ are elementarily equivalent with respect to $\mathscr{R}^{**} \cap \mathscr{R}^*$. Now if we assume that $\mathscr{N}^* = \mathscr{N}$ and that $\mathscr{R}^* \subseteqq \mathscr{R}^{**}$, then $\mathscr{R}^{**}$ is an elementary extension of $\mathscr{R}^*$ and hence by Theorem 3D, we have that $\mathscr{R}^{**} = \mathscr{R}^*$; i.e., in this special case of our uniqueness theorem our conclusion of the existence of an isomorphism between the two structures is strengthened to the conclusion that the structures are identical.

References

1. A. Froehlich and J. C. Shepherdson, *Effective procedures in field theory*, Trans. Roy. Philos. Soc. London Ser. A **248** (1956), 407–432.

2. S. C. Kleene, *Introduction to metamathematics*, Van Nostrand, New York, 1952.

3. E. W. Madison, *Computable algebraic structures and nonstandard arithmetic*, Ph.D. Thesis, Univ. of Illinois, Urbana, 1966.

4. E. Mendelson, *Introduction to mathematical logic*, Van Nostrand, Princeton, N. J., 1964.

5. M. O. Rabin, *Computable algebra*, Trans. Amer. Math. Soc. **95** (1960), 341–360.

6. A. Robinson, *An introduction to model theory*, North-Holland, Amsterdam, 1963.

7. ———, *Model theory and non-standard arithmetic. Infinitistic methods*, Proc. Sympos. Foundations of Math., Warsaw, 1959, pp. 265–302, Pergamon, Oxford and Państwowe Wydawnictwo Naukowe, Warsaw, 1961.

8. J. Rotman, *Introduction to group theory*, Allyn and Bacon, Boston, Mass., 1965.

9. T. Skolem, *Über die Nicht-charakterisierbarkeit der Zahlenreihe mittels endlich oder abzählbar unendlich vieler Aussagen mit ausschliesslich Zahlenvariablen*, Fund. Math. **23** (1934), 150–161.

10. A. Tarski and R. Vaught, *Arithmetical extensions of relational systems*, Compositio Math. **18** (1957), 81–102.

11. B. L. van der Waerden, *Modern algebra*, Vol. I, rev. English ed., Ungar, New York, 1949.

12. S. Warner, *Modern algebra*, Vol. II, Prentice-Hall, Englewood Cliffs, N. J., 1965.

University of Iowa,
Iowa City, Iowa