COMPUTABLE FIELDS AND ARITHMETICALLY DEFINABLE ORDERED FIELDS

A. H. LACHLAN AND E. W. MADISON

Introduction. A computable field is one whose elements may be placed in one-one correspondence with the natural numbers in such a way that the number theoretic functions corresponding to the field operations are recursive. In the same vein a field is called arithmetically definable (AD for short) if its elements may be placed in one-one correspondence with the natural numbers in such a way that the number theoretic functions corresponding to the field operations are arithmetical. These notions clearly extend in an obvious way to ordered fields and indeed to algebraic structures in general.

The term computable structure (group, ring, etc.) was probably introduced for the first time by M. O. Rabin [4], however, a similar notion was discussed a few years earlier by Fröhlich and Shepherdson [1]. Each of these references contains a number of interesting theorems on computable structures. Some results concerning AD structures appear in [2].

The main purpose of the present paper is to show that the fields of real algebraic numbers, constructible numbers, and solvable numbers, which were shown to be AD in [2], are in fact computable. This answers a question raised in footnote (2) of [2].

1. **Computable fields.** With the aid of classical algebra—in particular Galois theory—it was shown in [2] that the three fields mentioned above are AD. In this section we show that these fields are in fact computable by using the decidability of the elementary theory of real numbers [5].

Let α be an algebraic number; a *notation* for α is any triple (f, ρ, n) where f is a polynomial in one variable with integer coefficients, ρ is a complex rational, and n is a natural number such that $\xi = \alpha$ is the unique solution of

$$f(\xi) = 0 \wedge |\xi - \rho| < 1/n.$$

We suppose that some canonical indexing $\{T_j\}$ of all such triples has been given such that given any j we can effectively write down the unique triple T_j whose index it is, and vice-versa. Given any triple

Received by the editors April 21, 1968 and, in revised form, May 14, 1969.

(f, ρ, n) we can effectively decide whether or not it is a notation for some α, because the proposition

$$(\exists!\xi)[f(\xi) = 0 \wedge |\xi - \rho| < 1/n]$$

is easily reduced to a sentence in the elementary theory of real numbers. Let $\xi = x + iy$, $\rho = (a + ib)/c$ where x, y are real and a, b, c are integers with $c > 0$. From f we can find polynomials $p(x, y)$, $q(x, y)$ with integer coefficients such that $f(x, y) = p(x, y) + iq(x, y)$. The proposition can now be written:

$$(\exists!x)(\exists!y)[p(x, y) = 0 \wedge q(x, y) = 0 \wedge n^2\{(x - a)^2 + (y - b)^2\} < c^2].$$

Using the decision method of Tarski mentioned above, this last sentence can be effectively decided. Define $\langle x \rangle$ to be the algebraic number for which T_x is a notation if there is one, and to be 0 otherwise. It is easy to see that the relations $\langle x \rangle = \langle y \rangle$, $\langle x \rangle$ is real, $\langle x \rangle = 0$, $\langle x \rangle = 1$, $\langle x \rangle + \langle y \rangle = \langle z \rangle$, $\langle x \rangle \langle y \rangle = \langle z \rangle$ are all recursive, because an instance of any of these relations can easily be transformed into an elementary sentence about the real numbers in the manner demonstrated above.

Call a set Ξ of algebraic numbers *strongly r.e.* (*s.r.e.*) if $\{x | \langle x \rangle \in \Xi\}$ is r.e. It is immediately clear that the real algebraic numbers are s.r.e. The constructible numbers are just those algebraic numbers which can be obtained from 1 in a finite number of steps by rational operations (i.e., addition, subtraction, multiplication, and division) and extraction of square roots. The solvable numbers are similarly defined except that extraction of nth roots is permitted for any $n > 0$. If we effectively generate the graphs of all the relations listed above, then for any $\langle x \rangle$ which is constructible it will be apparent that $\langle x \rangle$ is constructible at some finite stage of the generating process. Thus the set of constructible numbers is s.r.e.; similarly for the solvable numbers. The same is true for the real constructible numbers and the real solvable numbers.

Observe that if an s.r.e. set of algebraic numbers forms a field then that field is computable. (The converse is also true but not required here.) For suppose Ξ is such a field, then since $\{x | \langle x \rangle \in \Xi\}$ is r.e. and since $\langle x \rangle = \langle y \rangle$ is recursive, we can effectively generate $x_0, x_1, \cdots$ such that $\langle x_j \rangle = \langle x_k \rangle$ only if $j = k$ and such that $\Xi = \{\langle x_j \rangle | j \geqq 0\}$. We obtain a canonical indexing Φ of Ξ by letting $\Phi(\xi)$ be the unique j such that $\xi = \langle x \rangle$. We have shown in particular that the fields of constructible and solvable numbers are computable. The reader will readily observe that the computability extends to the order in each case since $\langle x \rangle < \langle y \rangle$ is clearly a recursive relation. In summary we have:

THEOREM 1.1. *The fields of real algebraic numbers, constructible numbers, and solvable numbers are all computable ordered fields.*

2. **The fields of computable and arithmetical real numbers.** We begin this section with some definitions. Let ρ be a fixed effective mapping from the natural numbers onto the rationals where by 'effective' we mean that there are recursive functions f, g, h such that

$$\rho(x) = (-1)^{f(x)}(g(x)/h(x)).$$

It will be clear that everything we say below is independent of what effective ρ is chosen.

A real number α is said to be *computable* (*arithmetical*) just if the set $\{x \mid \rho(x) < \alpha\}$ is recursive (arithmetical). The computable (arithmetical) real numbers form a subfield of the real numbers denoted $\Re^C$ ($\Re^D$).

THEOREM 2.1. *If $\mathcal{K}$ is a computable (AD) ordered subfield of the field $\Re$ of real numbers then $\mathcal{K}$ is a proper subfield of $\Re^C$ ($\Re^D$).*

PROOF. Suppose $\mathcal{K}$ is computable. Let ψ be an admissible indexing for $\mathcal{K}$, i.e., ψ is a function from $\mathcal{K}$ onto a recursive set P of natural numbers such that for any x, y, z in P the relations

$$(1)\quad \psi^{-1}(x) + \psi^{-1}(y) = \psi^{-1}(z),\ \psi^{-1}(x)\psi^{-1}(y) = \psi^{-1}(z),\ \psi^{-1}(x) < \psi^{-1}(y)$$

are effectively decidable. We shall suppose for convenience that P is the set of all natural numbers. We can effectively find $\psi(0)$ since 0 is the only solution in $\mathcal{K}$ of $x+x=x$, and $\psi(1)$ since 1 is the only solution in $\mathcal{K}$ of $x^2=x$ and $x>0$. Similarly, for an arbitrary rational m/n supposed given by the ordered pair (m, n) with $n \neq 0$, we can effectively find $\psi(m/n)$. Now for a fixed member k of $\mathcal{K}$ we have $k < m/n$ if and only if $\psi^{-1}\psi(k) < \psi^{-1}\psi(m/n)$. Thus each such k determines a recursive cut of the rationals and hence is a recursive real number. This shows that $\mathcal{K} \subseteq \Re^C$.

Now suppose rationals r, s are given such that $r < s$. By an effective search we can find rationals r_0, s_0 such that $r \leqq r_0 < s_0 \leqq s$ and $\psi^{-1}(0) \notin [r_0, s_0]$; we have only to test all possible pairs (r_0, s_0) which satisfy $r \leqq r_0 < s_0 \leqq s$ until we find one such that $\psi^{-1}(0) < \psi^{-1}\psi(r_0)$ or $\psi^{-1}\psi(s_0) < \psi^{-1}(0)$. Iterating the process we can generate a recursive decreasing sequence $[r_0, s_0]$, $[r_1, s_1]$, $\cdots$ of nonempty rational intervals such that for all j, $\psi^{-1}(j) \notin [r_j, s_j]$. The intersection $\bigcap_{j=0}^{\infty} [r_j, s_j]$ clearly contains a recursive real number which is not in $\mathcal{K}$. This completes the proof when $\mathcal{K}$ is computable.

When $\mathfrak{K}$ is arithmetical the relations (1) are arithmetical rather than recursive; we can choose a fixed arithmetical set A in which each of the relations (1) is recursive. We then proceed as above with 'recursive in A' replacing 'recursive'. Since any set recursive in an arithmetical set is again arithmetical, the theorem is proved.

COROLLARY 2.2. $\mathfrak{R}^C$ ($\mathfrak{R}^D$) *is not a computable* (AD) *field.*

PROOF. Suppose $\mathfrak{R}^C$ were a computable field with an admissible indexing ψ mapping onto the natural numbers. Since $\mathfrak{R}^C$ is closed under the operation of square root applied to positive real numbers (this is proved in [**3**, p. 48]) we have

$$\psi^{-1}(x) < \psi^{-1}(y) \Leftrightarrow \exists z(\psi^{-1}(x) + (\psi^{-1}(z) \cdot \psi^{-1}(z)) = \psi^{-1}(y)).$$

Thus the relation on the left is r.e., and hence recursive because it is a linear ordering of all the natural numbers. Hence $\mathfrak{R}^C$ would be a computable ordered field in contradiction to the theorem. Similarly for $\mathfrak{R}^D$ mutatis mutandis.

COROLLARY 2.3. *Let $\mathfrak{K}$ be a subfield of $\mathfrak{R}$ which is not a proper subfield of $\mathfrak{R}^C(\mathfrak{R}^D)$. No ordered field containing $\mathfrak{K}$ whose order extends that of $\mathfrak{K}$ is computable* (AD).

PROOF. Let $\mathfrak{L}$ be a computable (AD) ordered extension of $\mathfrak{K}$ whose order extends that of $\mathfrak{K}$. From the first half of the proof of the theorem with ψ now an admissible indexing of $\mathfrak{L}$ any cuts of the rationals realized in $\mathfrak{L}$ are recursive (AD). Thus since $\mathfrak{K}$ is a subfield of $\mathfrak{R}$ but not a proper subfield of $\mathfrak{R}^C$ ($\mathfrak{R}^D$) we have $\mathfrak{K} = \mathfrak{R}^C$ ($\mathfrak{R}^D$). By the second half of the proof of the theorem we may construct a recursive cut of the rationals which is not realized in $\mathfrak{L}$. This contradicts $\mathfrak{K} \subseteq \mathfrak{L}$ and so the corollary is proved.

In contrast to the above notice that $\mathfrak{R}^D$ and thus $\mathfrak{R}^C$ also can be extended to a computable field. This is because the algebraic closure of $\mathfrak{R}^D$ contains $\mathfrak{R}^D$ and is characterized among all algebraically closed fields of characteristic zero by the fact that it has transcendence degree $\aleph_0$ over $\mathfrak{Q}$ the field of rationals. Thus we need only exhibit a computable field $\mathfrak{K}$ of characteristic zero whose transcendence degree over $\mathfrak{Q}$ is $\aleph_0$, because the algebraic closure of $\mathfrak{K}$ will be isomorphic to that of $\mathfrak{R}^D$ and computable by Theorem 7, [**4**, p. 354]. For $\mathfrak{K}$ we can take the field of fractions of the ring formed by the polynomials in indeterminates $x_0, x_1, x_2, \cdots$ with coefficients in $\mathfrak{Q}$.

THEOREM 2.4. $\mathfrak{R}^C$ *is an AD ordered field.*

PROOF. Let ρ be the effective enumeration of the rationals defined above and suppose for convenience that ρ is one-one. Let $\{f_i\}$ be an effective enumeration of the unary partial recursive functions. Let

$$J = \{i \mid f_i\rho^{-1} \text{ is the characteristic function of some left section of the rationals } \&(\forall_j)_{j<i}[f_i \neq f_j]\}.$$

Let $j(0)$, $j(1)$, $\cdots$ be an enumeration of J in order of magnitude. For each α in $\mathfrak{R}^C$ define $\psi(\alpha) = n$ just if $f_{j(n)}\rho^{-1}$ is the characteristic function of the set of rationals $<\alpha$. Then ψ maps $\mathfrak{R}^C$ one-one onto the natural numbers and using the classical definitions of sum, product, and order of Dedekind cuts it is easily verified that ψ is an admissible indexing of $\mathfrak{R}^C$ for arithmetic definability.

REFERENCES

1. A. Fröhlich and J. C. Shepherdson, *Effective procedures in field theory*, Philos. Trans. Roy. Soc. London Ser. A **248** (1956), 407–432. MR **17**, 570.

2. E. W. Madison, *Computable algebraic structures and nonstandard arithmetic*, Trans. Amer. Math. Soc. **130** (1968), 38–54. MR **36** #2498.

3. B. H. Mayoh, *Solvable and unsolvable problems in the theory of computable numbers*, Doctoral Dissertation, University of Illinois, Urbana, Ill., 1965.

4. M. O. Rabin, *Computable algebra, general theory and theory of computable fields*, Trans. Amer. Math. Soc. **95** (1960), 341–360. MR **22** #4639.

5. A. Tarski, *A decision method for elementary algebra and geometry*, 2nd ed., Univ. of California Press, Berkeley, Calif., 1951. MR **13**, 423.

SIMON FRASER UNIVERSITY AND
THE UNIVERSITY OF IOWA