NEW DECIDABLE FIELDS OF ALGEBRAIC NUMBERS

L. VAN DEN DRIES

Abstract. A formally real field of algebraic numbers is constructed which has decidable elementary theory and does not have a real closed or $p$-adically closed subfield.

Introduction. In his list of problems [7], A. Robinson remarked (p. 501, loc. cit.): "I do not know of any proper subfield of the field of algebraic numbers, other than the fields of algebraic real or $p$-adic numbers, that has been shown to be decidable". Taken literally, this remark is rather strange, because the well-known results of Ax-Kochen-Eršov of 1964–1965 provide several decidable fields of algebraic numbers other than the fields mentioned by Robinson. But each of these is henselian with respect to a certain nontrivial valuation, so has a $p$-adically closed subfield for some prime $p$. (See [3] for the notion of $p$-adically closed field. A field of algebraic numbers is $p$-adically closed iff it is isomorphic with the field of algebraic $p$-adic numbers, similarly as a field of algebraic numbers is real closed iff it is isomorphic with the field of real algebraic numbers.)

It is also easy to see that a field extension of finite degree over a decidable field of algebraic numbers is a decidable field. But applying this result to one of the fields indicated above gives again fields with a $p$-adically closed or real closed subfield.

So probably Robinson wanted a decidable field of algebraic numbers which has no $p$-adically closed or real closed subfield. In §2 we will construct such fields.

I am indebted to Jan Denef for calling my attention to the question answered in this paper.

1. Preliminaries. In this and the next section, $n$ is a fixed integer larger than 1. We define $OF_n$ as the 1st order theory whose models are the structures $(K, P_1, \ldots, P_n)$ with $(K, P)$ an ordered field, i.e. $K$ is a field and $P_i + P_i \subseteq P_i$, $P_i \cdot P_i \subseteq P_i$, $P_i \cap P_i = \{0\}$, $P_i \cup (-P_i) = K$ ($1 < i < n$). The language of $OF_n$ is $\{0, 1, +, \cdot, -, P_1, \ldots, P_n\}$, where $0, 1, +, \cdot, -$ are the usual ring operation symbols and $P_1, \ldots, P_n$ are unary predicate symbols. The models of $OF_n$ are also called $n$-ordered fields.

Let us make a list of facts which we will need.

Received by the editors September 27, 1978.

AMS (MOS) subject classifications (1970). Primary 02H15, 02G05.

© 1979 American Mathematical Society

0002-9939/79/0000-0516/$02.50

251
Fact 1 (from [1, p. 54]; see also [5] for the notion of ‘model companion’). \( O_{F_n} \) has a model companion \( \overline{O_{F_n}} \). The models of \( \overline{O_{F_n}} \) are those \( n \)-ordered fields \((K, P_1, \ldots, P_n)\) which satisfy:

(\(\alpha\)) \( P_i \) and \( P_j \) induce different (interval) topologies on \( K \), for all \( i \neq j \).

(\(\beta\)) For each irreducible \( f(X, Y) \in K[X, Y] \), monic in \( Y \), and each \( a \in K \) such that \( f(a, Y) \) changes sign on \( K \) with respect to each of the orderings \( P_i \), there exists \( (c, d) \in K \times K \) with \( f(c, d) = 0 \).

(In the formulation of [1, p. 54], \( f(X, Y) \) in (\(\beta\)) was not restricted to be monic in \( Y \), but the usual ‘linear transformation of variables’ argument easily shows that we need only consider \( f(X, Y) \) which are monic in \( Y \).)

\( \overline{O_{F_n}} \) is even a decidable theory (cf. [1, p. 74]), but I do not see how this can be used to obtain a decidable model of \( \overline{O_{F_n}} \) which is algebraic over \( \mathbb{Q} \). In §2 we shall construct just such a model.

Fact 2. Suppose \( K \) is an algebraic number field, \( P_1, \ldots, P_n \) are different orderings on \( K \), \( f(X, Y) \in K[X, Y] \) is monic in \( Y \) and irreducible, and \( a \in K \) such that \( f(a, Y) \) changes sign on \( K \) w.r.t. each of the orderings \( P_i \) on \( K \). Then there is a \( b \in K \) such that \( f(b, Y) \) still changes sign on \( K \) w.r.t. each \( P_i \), and \( f(b, Y) \in K[Y] \) is irreducible.

Because an algebraic number field is Hilbertian (cf. [4, Chapter 8]), and its different orderings induce different interval topologies, this fact follows from:

if \( \tau_1, \ldots, \tau_n \) are different nondiscrete \( V \)-topologies on a Hilbertian field \( K \) and for each \( i \in \{1, \ldots, n\} \) \( U_i \) is a nonempty \( \tau_i \)-open subset of \( K \), while \( H \) is a Hilbert set over \( K \), then \( U_1 \cap \cdots \cap U_n \cap H \neq \emptyset \) (cf. [1, p. 62]).

Fact 3. There is an algorithm which, given \( f(Y) \in \mathbb{Q}[Y] \setminus \mathbb{Q} \), decides whether \( f(Y) \) is irreducible in \( \mathbb{Q}[Y] \). (In [8, p. 79] such an algorithm is given for \( \mathbb{Z}[Y] \), and by Gauss’ lemma we get one for \( \mathbb{Q}[Y] \).)

Let \( \mathbb{Q} \) be in the following a fixed algebraic closure of \( \mathbb{Q} \). An algebraic number field is then any subfield \( K \) of \( \mathbb{Q} \) with \( [K : \mathbb{Q}] < \infty \). We also fix a 1-1 map of \( \mathbb{Q} \) onto a recursive subset of \( \mathbb{R} = \{0, 1, 2, \ldots\} \), such that addition and multiplication on \( \mathbb{Q} \) correspond under this map with recursive functions. Let us call the image of \( a \in \mathbb{Q} \) under this map the index of \( a \). The existence of such an indexing is proved by Rabin in [6].

The phrase ‘given \( a \in \mathbb{Q} \)’ will simply mean: ‘given the index of an element \( a \) of \( \mathbb{Q} \).’ Similarly a polynomial in \( \mathbb{Q}[X_1, \ldots, X_n] \) is given if its degree \( d \) is given and the vector of the coefficients of its monomials up to degree \( d \) is given.

An index of an algebraic number field \( K \) is the index of a generator \( K \) over \( \mathbb{Q} \), i.e. of an \( a \in \mathbb{Q} \) with \( K = \mathbb{Q}(a) \). ‘Given an algebraic number field’ will mean: ‘given an index of an algebraic number field’.

Fact 4. There are algorithms (I), (II), (III), (IV), (V) such that:

(1) given \( a \in \mathbb{Q} \), (I) determines the minimum polynomial of \( a \) over \( \mathbb{Q} \);
(2) given \( a \in \mathbb{Q} \), (II) determines whether \( a \in \mathbb{Q} \) holds;
NEW DECIDABLE FIELDS OF ALGEBRAIC NUMBERS

(3) given \(a, b \in \mathbb{Q}\), (III) determines \(c \in \mathbb{Q}\) with \(\mathbb{Q}(a, b) = \mathbb{Q}(c)\);
(4) given \(a, b \in \mathbb{Q}\), (IV) determines whether \(\mathbb{Q}(a) = \mathbb{Q}(b)\);
(5) given an algebraic number field \(K\) and \(f \in K[Y] \setminus K\), (V) decides whether \(f\) is irreducible in \(K[Y]\).

We obtain (I) from Fact 3, (II) by using (I) and looking at the degree of the minimum polynomial. Given \(a, b \in \mathbb{Q}\), there is a \(c \in \mathbb{Q}\) with \(\mathbb{Q}(a, b) = \mathbb{Q}(c)\), hence such a \(c\) will be found by trying all possibilities, so (III) exists. Computing the degrees of \(\mathbb{Q}(a)\), \(\mathbb{Q}(b)\) and \(\mathbb{Q}(a, b)\) over \(\mathbb{Q}\) by using (I) and (III) and looking at whether they are equal, gives (IV). A similar argument gives (V).

Suppose now that \(a \in \mathbb{Q}\) has minimum polynomial \(f(X) \in \mathbb{Q}[X]\) and that \(f(X)\) has precisely \(r_f\) real roots and that \(r_1, \ldots, r_n\) are integers with \(1 < r_1 < r_2, \ldots, 1 < r_n < r_f\). Let \(\alpha \in \omega\) be the index of \(a\). Then \((\alpha, r_1, \ldots, r_n)\) is said to be an index of the \(n\)-ordered field \((\mathbb{Q}(a), P_1, \ldots, P_n)\), where for each \(i = 1, \ldots, n\), \(P_i\) is the unique ordering on \(\mathbb{Q}(a)\) such that \(a\) is the \(r_i\)th root of \(f(X)\) in the real closure of \((\mathbb{Q}(a), P_i)\), these roots being numbered in increasing order. Using (IV) and Sturm's theorem, the following will be clear:

**Fact 5.** There is an algorithm which, given \((\alpha, r_1, \ldots, r_n) \in \omega^{n+1}\), decides whether it is an index of an \(n\)-ordered field \(\mathcal{K}\), and if so, computes the unique index \((\beta, s_1, \ldots, s_n)\) of \(\mathcal{K}\) with minimal \(\beta\).

Let us call this index \((\beta, s_1, \ldots, s_n)\) the minimal index of \(\mathcal{K}\). It will now be clear what the phrase 'given an \(n\)-ordered algebraic number field' means.

Finally we will use in §2 a fixed recursive bijection \(\pi: \omega \rightarrow \omega \times \omega\) such that the first coordinate of \(\pi(m)\) is \(< m\), for all \(m \in \omega\).

2. Construction of the field. Let \(\mathcal{F} = (F, P_1, \ldots, P_n)\) be any given \(n\)-ordered algebraic number field such that \(P_i \neq P_j\) for \(i \neq j\). We define \(\mathcal{C}\) as the set of all \(n\)-ordered algebraic number fields \(\mathcal{K}\) with \(\mathcal{F} \subset \mathcal{K}\). We fix for each \(\mathcal{K} \in \mathcal{C}\) an enumeration \(\alpha_{\mathcal{K}}: (f, a)_{j \in \omega}\) of all pairs \((f, a)\) with \(f \in K[X, Y]\) monic and of positive degree in \(Y\), and \(a \in K\) (\(K\) is the underlying field of \(\mathcal{K}\)). We suppose uniform effectiveness: there should be an algorithm which, given \(\mathcal{K} \in \mathcal{C}\) and \(j \in \omega\), constructs the pair \((f_j, a_j) = \alpha_{\mathcal{K}}(j)\).

Now we can construct an ascending sequence \((\mathcal{K}_m)_{m \in \omega}\) in \(\mathcal{C}\) as follows (where we write \(\mathcal{K}_m = (K_m, Q_1, \ldots, Q_{n,m})\)): \(\mathcal{K}_0 = \mathcal{F}\). Suppose \(\mathcal{K}_0 \subset \mathcal{K}_1 \subset \cdots \subset \mathcal{K}_m\) have already been constructed. Let \(\pi(m) = (i, j)\), so \(i < m\). Then \(\alpha_{\mathcal{K}_i}(j)\) is a pair \((f, a)\) with \(f \in K[i, X, Y]\), monic and of positive degree in \(Y\), and \(a \in K_i\).

If \(f(a, Y)\) does not change sign on \(K_m\) with respect to one of the orderings \(Q_k, m (1 < k < n)\), then we put: \(\mathcal{K}_{m+1} = \mathcal{K}_m\). Suppose \(f(a, Y)\) changes sign on \(K_m\) with respect to each of the orderings \(Q_{k,m}\) on \(K_m\). Then two cases can occur:

**Case 1.** \(f(X, Y)\) is irreducible in \(K_m[X, Y]\). In this case, there is by Fact 2 of §1 an element \(c \in K_m\) such that \(f(c, Y) \in K_m[Y]\) is still irreducible and still
changes sign on $K_n$ with respect to each of the $n$ orderings $Q_{k,m}$ ($k = 1, \ldots, n$). Using (V) of Fact 4, §1, and Sturm’s theorem we will certainly find such a $c$ with the smallest possible index, and for this $c$ we compute the root $d \in \bar{Q}$ of $f(c, Y)$ with minimal index and define: $K_{m+1} = (K_m(d), Q_{1,m+1}, \ldots, Q_{n,m+1})$, where $Q_{k,m+1}$ is the unique ordering on $K_m(d)$ extending $Q_{k,m}$, such that $d$ is the smallest root of $f(c, Y)$ in the real closure of $(K_m(d), Q_{k,m+1})$.

Case 2. $f(X, Y)$ is reducible in $K_m[X, Y]$. If this is the case we will discover this by trying out decompositions of $f$. If we find one, we put $K_{m+1} = K_m$. By construction of the chain $(K_m)_m$ it is clear that the map $m \mapsto$ minimal index of $K_m$ is recursive.

We put $K_m = \bigcup_{m \in \omega} K_m$, and write $K_{\omega} = (K_{\omega}, Q_{1,\omega}, \ldots, Q_{n,\omega})$.

Claim 1. $K_{\omega} \models \overline{OF_n}$. (See §1, Fact 1.)

Proof. $Q_{1,\omega}, \ldots, Q_{n,\omega}$ are $n$ distinct orderings on $K_{\omega}$, because they extend the $n$ distinct orderings $P_1, \ldots, P_n$ on $K_0$. As they are archimedean, they induce $n$ different interval topologies on $K_{\omega}$, so (a) of Fact 1 is satisfied. Suppose now that $f(X, Y) \in K_{\omega}[X, Y]$ is irreducible, monic in $Y$, and $f(a, Y)$ changes sign on $K_{\omega}$ with respect to each of the orderings $Q_{k,\omega}$, where $a \in K_{\omega}$. We have to show that $f(c, d) = 0$ for some $(c, d) \in K_2$. Clearly there is $(i, j) \in \omega \times \omega$ with $\alpha_{\omega}(j) = (f, a)$.

Let $m \in \omega$ be such that $\pi(m) = (i, j)$. Then by construction of the sequence $(K_m)_m$ we have: $K_{m+1} \models \exists c \exists d, f(c, d) = 0$, so $K_{\omega} \models \exists c \exists d, f(c, d) = 0$.

Claim 2. Th$(K_{\omega})$ is decidable.

Proof. By model completeness of $\overline{OF_n}$ and Claim 1 we have that $\overline{OF_n} \cup \text{Diag}(K_{\omega})$ is a complete theory. But $\text{Diag}(K_{\omega}) = \bigcup \{ \text{Diag } K_m | m \in \omega \}$, so $\text{Diag}(K_{\omega})$ is recursively enumerable. Hence $\overline{OF_n} \cup \text{Diag}(K_{\omega})$ is a complete theory with a recursively enumerable axiomatization. This implies in particular that there are two recursive functions, one enumerating Th$(K_{\omega})$, the other enumerating $\{ \sigma | \neg \sigma \in \text{Th}(K_{\omega}) \} = \text{the complement of Th}(K_{\omega})$ within the set of $\overline{OF_n}$-sentences). Hence Th$(K_{\omega})$ is decidable.

Corollary. $K_{\omega}$ is a decidable subfield of $\bar{Q}$ and does not have any real closed or $p$-adically closed subfield.

(Because $K_{\omega}$ is formally real, and $p$-adically closed fields are not formally real.)

Remark. The above arguments simply constructivize the proof of Theorem (3.1) in Chapter II of [1].


Lemma. Let the field $K$ be an algebraic extension of $Q$. Then $K$ is an atomic model of Th$(K)$. (The reader will see in the proof what this means.)

Proof. Let $(k_1, \ldots, k_m) \in K^m$. Clearly there is a formula $\theta(x_1, \ldots, x_m)$ in the language $\{ +, \cdot, -, 0, 1 \}$ which is satisfied by only finitely many $m$-tuples
NEW DECIDABLE FIELDS OF ALGEBRAIC NUMBERS

in \( K^m \), among which is \((k_1, \ldots, k_m)\). Take \( M > 1 \) minimal such that there is such a \( \theta(x_1, \ldots, x_m) \) with \( K \models (\exists^M(x_1, \ldots, x_m)\theta(x_1, \ldots, x_m)) \land \theta(k_1, \ldots, k_m) \). \( (\exists^M(x_1, \ldots, x_m) \) stands for: there are exactly \( M \) \( m \)-tuples such that.)

Let now \( \phi(x_1, \ldots, x_m) \) be any formula with \( K \models \phi(k_1, \ldots, k_m) \). We will show that \( K \models \forall x_1, \ldots, \forall x_m(\theta(x_1, \ldots, x_m) \rightarrow \phi(x_1, \ldots, x_m)) \). If this were not the case, then put \( \Psi(x_1, \ldots, x_m) := \theta(x_1, \ldots, x_m) \land \phi(x_1, \ldots, x_m) \), and we have: \( K \models (\exists^{M-1}(x_1, \ldots, x_m)\Psi(x_1, \ldots, x_m)) \land \Psi(k_1, \ldots, k_m) \) for some \( i > 1 \), contradicting the minimality of \( M \). So \( \theta(x_1, \ldots, x_m) \) generates the type of \((k_1, \ldots, k_m)\) with respect to \( \text{Th}(A) \). \( \square \)

**Corollary.** Let the decidable field \( K \) be an algebraic extension of \( Q \). Then each field extension \( L \) of \( K \) with \([L : K] < \infty\) is also a decidable field.

**Proof.** Let \( L = K(\alpha) \), and let \( X^m + k_1X^{m-1} + \cdots + k_m \) be the minimum polynomial of \( \alpha \) over \( K \). Let \( \theta(x_1, \ldots, x_m) \) be a generator of the type realized by \((k_1, \ldots, k_m)\) in \( K \) (which exists by the lemma). We consider now the 1st order theory \( T_{(K,\theta)} \) whose models are the structures \((L', K', k_1', \ldots, k_m')\) such that \( L' \) is a field with subfield \( K' \); \( K' \equiv K \) and \( L' = K'(\alpha') \) for some \( \alpha' \) whose minimum polynomial over \( K' \) is \( X^m + k_1'X^{m-1} + \cdots + k_m' \), and \( K' \models \theta(k_1', \ldots, k_m') \). Because \( \text{Th}(K) \) is decidable, \( T_{(K,\theta)} \) has a recursive axiomatization. We claim that \( T_{(K,\theta)} \) is a complete theory: it is easy to see that, given any sentence \( \sigma \) in the language of \( T_{(K,\theta)} \), one can construct a sentence \( \bar{\sigma} \) in the language of rings such that for every model \((L', K', k_1', \ldots, k_m')\) of \( T_{(K,\theta)} \):

\[
(L', K', k_1', \ldots, k_m') \models \sigma \iff (K', k_1', \ldots, k_m') \models \bar{\sigma}.
\]

But for such a model we have: \( \text{Th}(K', k_1', \ldots, k_m') = \text{Th}(K, k_1, \ldots, k_m) \). Combining this with the above equivalence we see that \( T_{(K,\theta)} \) is complete. As it is also recursively axiomatizable, \( T_{(K,\theta)} \) is decidable. Because \((L, K, k_1, \ldots, k_m) \models T_{(K,\theta)} \), \( \text{Th}(L) \) is decidable. \( \square \)

**Remark.** I do not know whether the following converse holds. If \( K, L \) are fields, \( Q \subset K \subset L \), \( L|Q \) is algebraic, \([L : K] < \infty\) and \( L \) is a decidable field, is then \( K \) a decidable field? If \( Q \) is replaced by a finite prime field, this is true by Eršov’s classification of algebraic extensions of \( F_p \) with decidable theory (cf. [2]).

**References**


Department of Mathematics, University of Utrecht, Utrecht, Netherlands

Current address: Department of Mathematics, Yale University, New Haven, Connecticut 06520