The Journal of Symbolic Logic
Volume 82, Number 2, June 2017

DECIDABLE ALGEBRAIC FIELDS

MOSHE JARDEN AND ALEXANDRA SHLAPENTOKH

Abstract. We discuss the connection between decidability of a theory of a large algebraic extensions of $\mathbb{Q}$ and the recursiveness of the field as a subset of a fixed algebraic closure. In particular, we prove that if an algebraic extension K of $\mathbb{Q}$ has a decidable existential theory, then within any fixed algebraic closure $\tilde{\mathbb{Q}}$ of $\mathbb{Q}$, the field K must be conjugate over $\mathbb{Q}$ to a field which is recursive as a subset of the algebraic closure. We also show that for each positive integer e there are infinitely many e-tuples $\boldsymbol{\sigma} \in \mathrm{Gal}(\mathbb{Q})^e$ such that the field $\tilde{\mathbb{Q}}(\boldsymbol{\sigma})$ is primitive recursive in $\tilde{\mathbb{Q}}$ and its elementary theory is primitive recursively decidable. Moreover, $\tilde{\mathbb{Q}}(\boldsymbol{\sigma})$ is PAC and $\mathrm{Gal}(\tilde{\mathbb{Q}}(\boldsymbol{\sigma}))$ is isomorphic to the free profinite group on e generators.

Introduction. The main theme of this work is the interplay between decidability of large algebraic extensions of $\mathbb{Q}$ and their recursiveness in a fixed algebraic closure $\tilde{\mathbb{Q}}$ of $\mathbb{Q}$. One of the main results of [8] gives for each positive integer e a recursive procedure to decide whether a sentence θ in the language of rings is true in the field $\tilde{\mathbb{Q}}(\boldsymbol{\sigma})$ for all $\boldsymbol{\sigma} \in \mathrm{Gal}(\mathbb{Q})^e$ outside a set of Haar measure zero (see also [4, p. 442, Theorem 20.6.7]). Here, $\mathrm{Gal}(\mathbb{Q}) = \mathrm{Gal}(\tilde{\mathbb{Q}}/\mathbb{Q})$ is the absolute Galois group of $\mathbb{Q}$, and for each $\boldsymbol{\sigma} = (\sigma_1, \ldots, \sigma_e) \in \mathrm{Gal}(\mathbb{Q})^e$, $\tilde{\mathbb{Q}}(\boldsymbol{\sigma})$ is the fixed field of $\sigma_1, \ldots, \sigma_e$ in $\tilde{\mathbb{Q}}$. The results of [2] even give a primitive recursive procedure for the same decision problem (see also [4, p. 722, Theorem 30.6.1]).

Note that the above procedures give no information about individual fields of the form $\tilde{\mathbb{Q}}(\boldsymbol{\sigma})$. Indeed, by Proposition 4.1 below, there are uncountably many elementary equivalence classes of fields $\tilde{\mathbb{Q}}(\boldsymbol{\sigma})$. On the other hand, since the language of rings is countable, there are at most countably many decision procedures. Hence, all but at most countably many fields of the form $\tilde{\mathbb{Q}}(\boldsymbol{\sigma})$ are undecidable.

Another question that could be asked in this context is about the relation between an individual field $\tilde{\mathbb{Q}}(\boldsymbol{\sigma})$ and $\tilde{\mathbb{Q}}$. To this end we recall that one may order the elements of $\tilde{\mathbb{Q}}$ in a primitive recursive sequence and give a primitive recursive procedure for the field theoretic operations among the elements of that sequence. It therefore makes sense to ask about a subfield M of $\tilde{\mathbb{Q}}$ whether M is a recursive subset of $\tilde{\mathbb{Q}}$ (in which case M is also a recursive (or a computable) subfield of $\tilde{\mathbb{Q}}$).

Usually, this is not the case, because $\tilde{\mathbb{Q}}$ has only countably many recursive subsets. Even if the elementary theory of M is decidable, it may happen that M has uncountably many conjugates (Example 1.6, when M is a real or a p-adic closure of $\mathbb{Q}$). The elementary theory of each of them is the same as that of M, so is also decidable. But only countably many of them are recursive in $\tilde{\mathbb{Q}}$.

Received December 2, 2015.
2010 *Mathematics Subject Classification.* 12E30, 03C07, 03D35.
Key words and phrases. decidable theory, recursive subsets.

0022-4812/17/8202-0004
DOI:10.1017/jsl.2017.10

We shed light on these problems by proving two results:

THEOREM A. *Let M be a subfield of $\tilde{\mathbb{Q}}$ whose existential elementary theory is decidable (resp. primitive recursively decidable). Then, M is conjugate to a recursive (resp. primitive recursive) subfield M' of $\tilde{\mathbb{Q}}$.*

In view of this theorem, given a subfield of $\tilde{\mathbb{Q}}$ with an undecidable existential (or elementary) theory in the language of rings, one can distinguish between two cases. The theory can be undecidable because the field has no computable conjugate within the given copy of $\tilde{\mathbb{Q}}$ or the theory can be undecidable for a different arithmetic reason. In the first case it is tempting to say that the theory is *trivially* undecidable. A simple example of a field with a trivially undecidable existential theory is a Galois extension of $\mathbb{Q}$ which is not recursive as a subset of $\tilde{\mathbb{Q}}$.

THEOREM B. *For each positive integer e there are infinitely many e-tuples $\boldsymbol{\sigma} \in \mathrm{Gal}(\mathbb{Q})^e$ such that the field $\tilde{\mathbb{Q}}(\boldsymbol{\sigma})$ is primitive recursive in $\tilde{\mathbb{Q}}$ and its elementary theory is primitive recursively decidable. Moreover, $\tilde{\mathbb{Q}}(\boldsymbol{\sigma})$ is PAC and $\mathrm{Gal}(\tilde{\mathbb{Q}}(\boldsymbol{\sigma}))$ is isomorphic to the free profinite group on e generators.*

Both theorems make sense, because we can list the elements of $\tilde{\mathbb{Q}}$ in a primitive recursive sequence. The proof of Theorem A depends on our ability to perform the basic field theoretic operations including the factorization of polynomials over given number fields and even over $\tilde{\mathbb{Q}}$ in a primitive recursive way. The proof of Theorem B uses in addition an effective version of Hilbert irreducibility theorem (Lemma 2.2) and the method of Galois stratification.

All of these operations can be carried out over each given finitely generated infinite field (over its prime field). In the terminology of [4, Chapter 19], these fields have "elimination theory". So, actually we prove Theorems A and B for fields with elimination theory that are "effectively Hilbertian". In particular, they hold for each "presented infinite finitely generated field".

§1. Recursive subfields of $\tilde{K}$. We consider a presented field K in the sense of [4, p. 410, Definition 19.2.8]. This is a field which is explicitly constructed from the ring $\mathbb{Z}$ of integers, one has "effective recipes" to add and multiply given elements and to "effectively compute" the inverse of each given nonzero element. In particular, K is countable. An element z of a field extension F of K is *presented over K* if either z is algebraic over K and $\mathrm{irr}(z, K)$ is explicitly given or it is known that z is transcendental over K. An n-tuple $(z_1, \ldots, z_n)$ of elements of F is *presented over K* if z_i is presented over $K(z_1, \ldots, z_{i-1})$ for $i = 1, \ldots, n$. Similarly, a sequence $z_1, z_2, z_3, \ldots$ of elements of $\tilde{K}$ is said to be *presented over K* if the function $n \mapsto \mathrm{irr}(z_n, K(z_1, \ldots, z_{n-1}))$ is primitive recursive. In these cases we say that the field $K(z_1, \ldots, z_n)$ (resp. $K(z_1, z_2, z_3, \ldots)$) is *presented over K*, alternatively, that $K(z_1, \ldots, z_n)$ (resp. $K(z_1, z_2, z_3, \ldots)$) is a *presented extension* of K.

We say that K has a *splitting algorithm* if K has an effective algorithm for factoring each polynomial in $K[X]$ into a product of irreducible factors. By [4, p. 409, Lemma 19.2.4], every presented finitely generated separable field extension of a field K with a splitting algorithm has a splitting algorithm.

If every presented finitely generated extension of K has a splitting algorithm, we say that K has *elimination theory*. By [4, p. 411, Corollary 19.2.10], if K_0 is a presented perfect field with a splitting algorithm, then K_0 has elimination theory.

https://doi.org/10.1017/jsl.2017.10 Published online by Cambridge University Press

In particular, since each of the fields $\mathbb{Q}$ and $\mathbb{F}_p$ (where p is a prime number) has a splitting algorithm, every presented finitely generated field extension K of its prime field has elimination theory.

All of these notions and algorithms are rigorously defined, explained, and proved in [4, Sections 19.1 and 19.2]. Moreover, it is proved there that the above algorithms are *primitive recursive* in the usual sense (e.g., as defined in [4, Section 8.4]). Hence, they are also recursive. It is further proved in [4, Section 19.4] that both the separable closure K_s and the algebraic closure $\tilde{K}$ of K can be presented, and then have elimination theory.

Having done so, we say that a subfield M of $\tilde{K}$ is *recursive* (resp. *primitive recursive*), if M is a recursive (resp. primitive recursive) subset of $\tilde{K}$ (e.g., [4, Section 8.5]). Since addition, multiplication, and taking inverse of elements of $\tilde{K}$ are primitive recursive, these operations in M are also recursive (resp. primitive recursive). For example, K_s is a primitive recursive subfield of $\tilde{K}$.

Independently of the question whether M is a recursive subfield of $\tilde{K}$ or not, we consider the theory $\mathrm{Th}(M)$ (resp. the existential theory $\mathrm{Ex}(M)$) of M in the language $\mathcal{L}(\mathrm{ring}, K)$ of rings with a constant symbol for each element of K. Then, we may say that $\mathrm{Th}(M)$ is *decidable* (resp. *primitively decidable*) if there exists an algorithm (resp. primitive recursive algorithm) to decide whether a given sentence of $\mathcal{L}(\mathrm{ring}, K)$ holds in M or not. Similar definitions apply to $\mathrm{Ex}(M)$.

Note that $\mathcal{L}(\mathrm{ring}, K)$ has only constant symbols for the elements of K but not for the elements of $\tilde{K} \smallsetminus K$. Thus, the question whether M is a recursive subfield of $\tilde{K}$ is independent of the question whether $\mathrm{Th}(M)$ is decidable. Indeed, even if $\mathrm{Th}(M)$ is decidable, M may have uncountably many K-conjugates in $\tilde{K}$ (Example 1.6). Since K is countable, so is the language $\mathcal{L}(\mathrm{ring}, K)$. Hence, there are only countably many algorithms for the language $\mathcal{L}(\mathrm{ring}, K)$. It follows that at most countably many of the K-conjugates of M in $\tilde{K}$ may have decidable theories. All the others have undecidable theories.

However, we prove in this section that if M is a field extension of K in $\tilde{K}$ and $\mathrm{Ex}(M)$ is decidable (resp. primitive recursively decidable), then M has a K-conjugate M' which is recursive (resp. primitive recursive) in $\tilde{K}$. In particular, $\mathrm{Ex}(M') = \mathrm{Ex}(M)$, so $\mathrm{Ex}(M')$ is in addition decidable (resp. primitive recursively decidable). It follows that the analogous statements with $\mathrm{Th}(M)$ replacing $\mathrm{Ex}(M)$ are also true.

The statements of this section deal with an extension M of K in $\tilde{K}$. We assume that $\mathrm{Ex}(M)$ is decidable (resp. primitive recursively decidable) and construct elements of K_s and finite extensions of K using that assumption and the effective field theoretic constructions that appear in [4, Sections 19.1–19.4]. Since the latter are effective, our constructions are recursive (resp. primitive recursive). Hence, whenever we use the assumption on M and the effectiveness of the field theoretic constructions, we get recursive (resp. primitive recursive) constructions. Elements of $\tilde{K}$ and field extensions of K in $\tilde{K}$ constructed in this way will be referred to as *recursive* (resp. *primitive recursive*) over K.

In order to simplify our language, we omit the adverb "recursively" (resp. "primitive recursively") that should appear before the verbs "decompose", "construct", "compute", and "find" in the proofs.

https://doi.org/10.1017/jsl.2017.10 Published online by Cambridge University Press

In contrast, when we say that an object (like an embedding of fields over K) "exists" it means in particular that we don't know whether it is presentable over K.

LEMMA 1.1. *Let K be a presented field with elimination theory. Let M be a subfield of $\tilde{K}$ that contains K such that* $\mathrm{Ex}(M)$ *is decidable (resp. primitive recursively decidable). Suppose L is a recursive (resp. primitive recursive) finite separable extension of K and p is a given monic separable polynomial in $K[Z]$.*

Let P be the set of roots of p in K_s. Then, we can perform exactly one of the following two tasks:

(a) *Recursively (resp. primitive recursively) find out whether there exists no embedding of $L(z)$ into M with $z \in P \setminus L$.*
(b) *Recursively (resp. primitive recursively) find $z \in P \setminus L$ and prove the existence of a K-embedding $\phi' \colon L(z) \to M$.*

PROOF. By our assumptions of K and L we can decompose $p(Z)$ into a product of monic irreducible factors over L,

$$p(Z) = (Z - a_1) \cdots (Z - a_l) h_1(Z) \cdots h_m(Z)$$

such that $a_1, \ldots, a_l \in L$ and $\deg(h_i) \geq 2$ for $i = 1, \ldots, m$ [4, p. 407, Lemma 19.2.2]. If $m = 0$, then $P \subseteq L$, so there is no embedding of $L(z)$ into M with $z \in P \setminus L$.

Otherwise, we construct a primitive element y for L/K, compute $f = \mathrm{irr}(y, K)$, and set $d = \deg(f)$. For each $1 \leq i \leq m$ we set $d_i = \deg(h_i)$. Then, we compute for each $0 \leq j \leq d_i$ the unique polynomial g_{ij} in $K[Y]$ of degree at most $d - 1$ such that $h_i(Z) = \sum_{j=0}^{d_i} g_{ij}(y) Z^j$. We set $g_i(Y, Z) = \sum_{j=0}^{d_i} g_{ij}(Y) Z^j$ and observe that $g_i \in K[Y, Z]$ and $g_i(y, Z) = h_i(Z)$. Then, we denote the existential sentence

$$(\exists Y, Z)[f(Y) = 0 \wedge g_i(Y, Z) = 0]$$

of $\mathcal{L}(\mathrm{ring}, K)$ by θ_i.

Since $\mathrm{Ex}(M)$ is decidable (resp. primitive recursively decidable) in the language $\mathcal{L}(\mathrm{ring}, K)$, we may check the truth of each θ_i in M. If none of the sentences $\theta_1, \ldots, \theta_m$ is true in M, then there exists no K-embedding $\phi' \colon L(z) \to M$ with $z \in P \setminus L$.

Indeed, if such z and ϕ' exist, we write $y' = \phi'(y)$ and $z' = \phi'(z)$. Then, $z \in P \setminus \{a_1, \ldots, a_l\}$, so there exists an $1 \leq i \leq m$ with $h_i(z) = 0$. Hence, $g_i(y, z) = 0$. Applying ϕ', we see that $f(y') = 0$ and $g_i(y', z') = 0$, with $y', z' \in M$. Thus, θ_i holds in M, in contrast to our assumption.

Finally suppose that one of the sentences $\theta_1, \ldots, \theta_m$, say θ_1, is true in M. Thus, there exist $y', z' \in M$ with $f(y') = 0$ and $g_1(y', z') = 0$. Since f is irreducible over K, the map $y \mapsto y'$ extends to a K-isomorphism ϕ_0' of $L = K(y)$ onto $K(y')$. Since $g_1(y, Z) = h_1(Z)$ is irreducible over $K(y) = L$, the polynomial $g_1(y', Z)$ is irreducible over $K(y')$. Since z' is a root of the latter polynomial, there exists a root z of $g_1(y, Z)$ such that ϕ_0' extends to an isomorphism $\phi' \colon K(y, z) \to K(y', z')$ with $\phi'(z) = z'$, as desired. ⊣

LEMMA 1.2. *Let K be a presented field with elimination theory. Let M be a subfield of $\tilde{K}$ that contains K such that* $\mathrm{Ex}(M)$ *is decidable (resp. primitive recursively decidable). Suppose L is a recursive (resp. primitive recursive) finite separable extension of K and p is an explicitly given monic separable polynomial in $K[Z]$. Suppose in*

https://doi.org/10.1017/jsl.2017.10 Published online by Cambridge University Press

addition, that there exists a K-embedding $\phi\colon L \to M$. Let P be the set of roots of p in K_s.

Then, we can recursively (resp. primitive recursively) find a subset I of P for which there exists a K-embedding $\psi\colon L(I) \to M$ such that $I = P \cap L(I)$ and $\psi(I) = P \cap M$.

PROOF. We set $L' = \phi(L)$. By Lemma 1.1, we may decide which of the two cases below holds.

CASE A: *There is no K-embedding $L(z) \to M$ with $z \in P \setminus L$.* Then, we set $I = P \cap L$ and $\psi = \phi$. Hence, $L(I) = L$, so $I = P \cap L(I)$. Then, $L' = \phi(L)$ satisfies $\psi(P \cap L) = P \cap L'$.

Now note that $\psi(I) = \psi(P \cap L) \subseteq P \cap M$. If there exists $z' \in P \cap M \setminus \psi(I)$, then by the preceding paragraph, $z' \in M \setminus L'$. Thus, there exists $z \in K_s$ and an extension of ψ to an isomorphism $\psi'\colon L(z) \to L'(z')$ such that $\psi'(z) = z'$. Hence, $z \in P \setminus L$, in contrast to our assumption.

It follows from this contradiction that $\psi(I) = P \cap M$.

CASE B: *Case A does not occur and we may find $z \in P \setminus L$ for which there exists a K-embedding $\phi'\colon L(z) \to M$.* Then, $|P \setminus L(z)| < |P \setminus L|$, so by induction, we may find a subset I of P for which there exists a K-embedding ψ of $L(z, I)$ into M such that $I = P \cap L(z, I)$ and $\psi(I) = P \cap M$. In particular, since $z \in P$, we have $z \in I$. Thus, $L(I, z) = L(I)$ and $I = P \cap L(I)$. ⊣

We denote the maximal purely inseparable extension of a field F by F_{ins}.

LEMMA 1.3. *Let K be a presented field with elimination theory. Let F be a recursive (resp. primitive recursive) subfield of K_s that contains K. Suppose that we can decide (resp. primitive recursively decide) for each monic separable polynomial $f \in K[X]$ whether f has a root in F. Then, F_{ins} is also a recursive (resp. primitive recursive) subfield of $\tilde{K}$ and we can decide (resp. primitive recursively decide) for each monic polynomial $f \in K[X]$ whether f has a root in F_{ins}.*

PROOF. It suffices to consider the case where $p = \text{char}(K) > 0$. By our assumption on K, we are able to factor each monic $f \in K[X]$ into irreducible polynomials over K. Hence, in order to decide whether f has a root in F_{ins}, we may assume that f is irreducible. In this case we present $f(X)$ as $f(X) = g(X^q)$, where g is an irreducible separable polynomial in $K[X]$ and q is a power of p. If y is a root of g in F and $z^q = y$ with $z \in \tilde{K}$, then $f(z) = 0$ and $z \in F_{\text{ins}}$. On the other hand, if $z \in F_{\text{ins}}$ and $f(z) = 0$, we get for $y = z^q$ that $g(y) = f(z) = 0$ and $y \in K_s \cap F_{\text{ins}} = F$. By our assumptions on F, we may decide whether g has a root in F. Hence, we may decide whether f has a root in F_{ins}.

Consider $x \in \tilde{K}$ and compute $f(X) = \text{irr}(x, K)$. Then, we write $f(X) = g(X^q)$, where $g \in K[X]$ is separable and q is a power of p. Then, $x^q \in K_s$ and we can check whether $x^q \in F$. This is the case if and only if $x \in F_{\text{ins}}$. ⊣

THEOREM 1.4. *Let K be a presented field with elimination theory. Let M be a perfect subfield of $\tilde{K}$ that contains K. Suppose that* $\text{Ex}(M)$ *is decidable (resp. primitive recursively decidable). Then, $\tilde{K}$ has a recursive (resp. primitive recursive) subfield M' that contains K and is K-isomorphic to M.*

https://doi.org/10.1017/jsl.2017.10 Published online by Cambridge University Press

PROOF. We make a primitive recursive list, $p_1, p_2, p_3, \ldots$, of all monic separable irreducible polynomials in $K[Z]$. For each positive integer j we compute the set P_j of all roots of p_j in K_s. Since $p_1, p_2, p_3, \ldots$ are distinct irreducible polynomials,

(1) the sets $P_1, P_2, P_3, \ldots$ are disjoint.

Using Lemma 1.2, we inductively construct a recursive (resp. primitive recursive) ascending tower $L_0 \subseteq L_1 \subseteq L_2 \subseteq \cdots$ of finite extensions of K in K_s with $L_0 = K$. For each positive integer j we prove the existence of a K-embedding $\psi_j : L_j \to M$ such that

(2) $\psi_j(P_j \cap L_j) = P_j \cap M$.

Then, we consider the subfield $L_\infty = \bigcup_{j=1}^{\infty} L_j$ of K_s and set $M_\infty = M \cap K_s$.

For each positive integer j we denote the set of all K-embeddings $\psi : L_j \to M$ such that $\psi(P_j \cap L_j) = P_j \cap M$ by $\mathcal{P}_j$. The set $\mathcal{P}_j$ is nonempty (because $\psi_j \in \mathcal{P}_j$) and finite (because $[L_j : K] < \infty$). Moreover, if $\phi \in \mathcal{P}_{j+1}$, then $\phi|_{L_j} \in \mathcal{P}_j$. Thus, $\mathcal{P}_1, \mathcal{P}_2, \mathcal{P}_3, \ldots$ form an inverse system of finite sets. Hence, by [4, p. 3, Corollary 1.1.4], there exists a K-embedding $\phi : L_\infty \to M$ such that $\phi|_{L_j} \in \mathcal{P}_j$, i.e.,

(3) $\phi(P_j \cap L_j) = P_j \cap M$

for each positive integer j.

CLAIM A: *ϕ maps L_∞ isomorphically onto M_∞*. Indeed, since $L_\infty \subseteq K_s$, we have $\phi(L_\infty) \subseteq M_\infty$. Conversely, let $y \in M_\infty$. By definition, $K_s = \bigcup_{j=1}^{\infty} P_j$. Hence, there exists a positive integer j such that $y \in P_j$. By (3), there exists $x \in P_j \cap L_j$ (hence, $x \in L_\infty$) such that $\phi(x) = y$. Thus, $\phi(L_\infty) = M_\infty$. Since ϕ is injective, ϕ maps L_∞ isomorphically onto M_∞.

CLAIM B: $L_\infty = \bigcup_{j=1}^{\infty} P_j \cap L_j$. Indeed, by definition, the right hand side is contained in the left hand side. Conversely, let $x \in L_\infty$. Then, there exists a positive integer j with $x \in P_j$. Thus, $\phi(x) \in P_j \cap M$. By (3), $x \in P_j \cap L_j$, as claimed.

CLAIM C: *The field L_∞ is recursive (resp. primitive recursive) in K_s*. Indeed, given $x \in K_s$ we can find a positive integer j with $p_j(x) = 0$. This means that $x \in P_j$. Then, we check if $x \in L_j$. If this is the case, then $x \in L_\infty$. Otherwise (i.e., $x \notin L_j$), $x \notin L_\infty$.

Indeed, if $x \in L_\infty$, then by Claim B, there exists j' such that $x \in P_{j'} \cap L_{j'}$. It follows by (1) that $j' = j$, so $x \in L_j$. This contradicts our assumption.

CONCLUSION OF THE PROOF. Since M is perfect and $M_\infty = M \cap K_s$, the field M is the maximal purely inseparable extension of M_∞. Let M' be the maximal purely inseparable extension of L_∞. Then, by Claim A, ϕ has a unique extension to an isomorphism $\phi' : M' \to M$. By Claim C and Lemma 1.3, M' is a recursive (resp. primitive recursive) subfield of $\tilde{K}$. ⊣

REMARK 1.5. Note that we do not claim nor do we prove that the K-isomorphism $\phi' : M' \to M$ mentioned in Theorem 1.4 is recursive. Indeed, let $\mathcal{M}$ be a K-conjugacy class of fields with a decidable theory. Only countably many of them are recursive subfields of $\tilde{K}$. For each of them there are only countably many recursive K-embeddings into $\tilde{K}$. Thus, all but countably many fields in $\mathcal{M}$ are not images of those embeddings. If M is not one of those countably many fields, M is not the image of a recursive K-isomorphism of a recursive subfield of $\tilde{K}$. ⊣

https://doi.org/10.1017/jsl.2017.10 Published online by Cambridge University Press

Each of the fields that occur in the following example is considered as a structure for the language of rings $\mathcal{L}(\text{ring}, \mathbb{Z})$ [4, Example 7.3.1].

EXAMPLE 1.6. Let R be a real closure of $\mathbb{Q}$. Then, R is elementarily equivalent to the field $\mathbb{R}$ of real numbers [11, p. 51, Corollary 5.3]. By Tarski [14, p. 42, Theorem 37], $\text{Th}(\mathbb{R})$ is primitive recursively decidable, hence so is $\text{Th}(R)$. Similarly, for each positive integer p let $\mathbb{Q}_p$ be a Henselian closure of $\mathbb{Q}$ with respect to the p-adic valuation of $\mathbb{Q}$. Then, $\mathbb{Q}_p$ is elementary equivalent to the field $\hat{\mathbb{Q}}_p$ of all p-adic numbers [12, p. 86, Theorem 5.1]. We know that $\text{Th}(\hat{\mathbb{Q}}_p)$ is decidable [10, p. 97, Corollary 3.3.16], and even primitive recursively decidable [16]. Hence, so is $\text{Th}(\mathbb{Q}_p)$.

By E. Artin, $\text{Aut}(R)$ is trivial [9, p. 455, Theorem XI.2.9]. By F. K. Schmidt [13], the same is true for $\text{Aut}(\mathbb{Q}_p)$ (see also [7, Proposition 14.5]). Since $\text{Gal}(\mathbb{Q})$ is uncountable, the fields R and $\mathbb{Q}_p$ have uncountable many $\mathbb{Q}$-conjugates. It follows from Theorem 1.4 that there exists a primitive recursive subfield L of $\tilde{\mathbb{Q}}$ which is isomorphic to R (resp. to $\mathbb{Q}_p$).

§2. Decidable large fields. We consider a presented field K with elimination theory. As in Section 1. We say that a finitely generated extension L of K (resp. an element of L) is *recursively presented* if it emerges from a recursive procedure over K (but not necessarily from a primitive recursive procedure, nor L is explicitly given in the sense of the first paragraph of Section 1). In particular, L has a recursive splitting algorithm. In addition to the field operations discussed in Section 1, we note that all of the standard operations on Galois extensions of K and on their Galois groups can be carried out in a recursive way, as in [4, pp. 411–412, Section 19.3]. The same holds for every recursively presented finitely generated extension of K.

In addition, using [4, p. 413, Lemma 19.4.1], we effectively construct a sequence $z_1, z_2, z_3, \ldots$ of elements that presents K_s over K. Thus, $K_s = K(z_1, z_2, z_3, \ldots)$. We recall that by the above mentioned lemma, both K_s and $\tilde{K}$ have elimination theory.

Throughout this section we use the language $\mathcal{L}(\text{ring}, K)$. All of the procedures that appear in the lemmas, proposition, and theorem of this section will be recursive and will be stated as those. However, as in the first section, we omit the adverb "recursively" before the verbs "construct", "find", "find out", "choose", "compute", "embed", "gives", "check" from the proofs, keeping them only in the proclaims.

NOTATION 2.1. *We consider variables $T_1, \ldots, T_r, X$ over K and abbreviate $(T_1, \ldots, T_r)$ by $\mathbf{T}$. Let $f_1, \ldots, f_m$ be irreducible and separable polynomials in $K(\mathbf{T})[X]$ and let g be a nonzero polynomial in $K[\mathbf{T}]$. Following* [4, *Section* 12.1], *we write $H_K(f_1, \ldots, f_m; g)$ for the set of all $\mathbf{a} \in K^r$ such that $f_1(\mathbf{a}, X), \ldots, f_m(\mathbf{a}, X)$ are defined, irreducible, and separable in $K[X]$. In addition, $g(\mathbf{a}) \neq 0$. Then, we call $H_K(f_1, \ldots, f_m; g)$ a separable Hilbert subset of K^r. A separable Hilbert set of K is a separable Hilbert subset of K^r for some positive integer r. We say that K is Hilbertian if each separable Hilbert set of K is nonempty.*

LEMMA 2.2. *Let K be a presented field with elimination theory. Suppose that K is Hilbertian. Then, for each presented separable Hilbert subset H of K^r we can recursively find $(a_1, \ldots, a_r) \in H$.*

PROOF. Using Cantor's first diagonal method, we can write down a list $(\mathbf{a}_1, \mathbf{a}_2, \mathbf{a}_3, \ldots)$, with $\mathbf{a}_i = (a_{i1}, \ldots, a_{ir})$, of all elements of K^r. Let $H = H_K(f_1, \ldots, f_m; g)$ be as in Notation 2.1.

https://doi.org/10.1017/jsl.2017.10 Published online by Cambridge University Press

Since K has the splitting algorithm, we may check the irreducibility of the polynomials $f_1(\mathbf{a}_i, X), \dots, f_m(\mathbf{a}_i, X)$ over K, their separability, and the condition $g(\mathbf{a}_i) \neq 0$ for $i = 1, 2, 3, \dots$. Since K is Hilbertian, we will certainly hit an i such that $f_1(\mathbf{a}_i, X), \dots, \mathbf{f}_m(\mathbf{a}_i, X)$ are irreducible and separable over K, and $g(\mathbf{a}_i) \neq 0$, as needed.

This gives us a recursive procedure (but not a primitive recursive procedure) to find $\mathbf{a}$ in H. ⊣

LEMMA 2.3. *Let K be a presented field with elimination theory which is Hilbertian, let L be a recursively presented finite separable extension of K, and let H be a recursively presented separable Hilbert subset of L^r. Then, we can recursively find a separable Hilbert subset H_K of K^r which is contained in H.*

PROOF. Let $H = H_L(f_1, \dots, f_m; g)$, where $f_1, \dots, f_m$ are recursively presented irreducible separable polynomials in $L(\mathbf{T})[X]$ and g is a recursively presented nonzero polynomial in $L[\mathbf{T}]$. Without loss we may assume that the coefficients of $f_1, \dots, f_m$ are in $L[\mathbf{T}]$. The proof of [4, p. 224, Lemma 12.2.2] uses the proof of [4, p. 223, Lemma 12.2.1] with $L(\mathbf{T})$ replacing L in the latter lemma to recursively produce a nonzero polynomial $h \in K[\mathbf{T}]$ and irreducible separable polynomials $p_1, \dots, p_m$ in $K(\mathbf{T})[X]$ with the following property: If $\mathbf{a} \in K^r$, $h(\mathbf{a}) \neq 0$, and the $p_i(\mathbf{a}, X)$'s are defined, irreducible, and separable in $K[X]$, then $f_1(\mathbf{a}, X), \dots, f_m(\mathbf{a}, X)$ are defined, irreducible, and separable in $L[X]$, and $g(\mathbf{a}) \neq 0$. Replacing h by the product of all its K-conjugates (an effective operation), $H_K(p_1, \dots, p_m; h)$ is a separable Hilbert subset of K^r which is contained in H. ⊣

Recall that a field M is *PAC* if every absolutely integral variety over M has an M-rational point. We denote the free profinite group on e generators by $\hat{F}_e$ [4, p. 349, first paragraph]. We also denote the absolute Galois group of a field F by $\mathrm{Gal}(F)$.

LEMMA 2.4. *Let K be a presented field with elimination theory. Let M be an extension of K in $\tilde{K}$. Suppose that M is perfect, PAC, and* $\mathrm{Gal}(M) \cong \hat{F}_e$, *Further suppose that the set* $\mathrm{Root}(M)$ *of all monic polynomials in $K[X]$ that have roots in M is recursive. Then,* $\mathrm{Th}(M)$ *is decidable.*

PROOF. Let $\mathrm{Ax}(K, e)$ be the set of axioms in the language $\mathcal{L}(\mathrm{ring}, K)$ given in [4, p. 437, Proposition 20.4.4] for the field extensions of K that are perfect, PAC, and with absolute Galois group isomorphic to $\hat{F}_e$. Let $\mathrm{Ax}(K, M)$ be the union of $\mathrm{Ax}(K, e)$ and the axioms that say that each $f \in \mathrm{Root}(M)$ has a root in M and each monic $f \in K[X] \setminus \mathrm{Root}(M)$ does not have a root in M. In particular, $M \models \mathrm{Ax}(K, M)$.

Conversely, if a field F is a model of $\mathrm{Ax}(K, M)$, then a monic polynomial $f \in K[X]$ has a root in F if and only if f has a root in M. By [4, p. 441, Lemma 20.6.3(b)], $F \cap \tilde{K} \cong_K M$. Hence, by [4, p. 436, Corollary 20.4.2], F is elementarily equivalent to M as a structure of $\mathcal{L}(\mathrm{ring}, K)$.

It follows from Gödel completeness theorem [4, p. 154, Corollary 8.2.6] that $\mathrm{Th}(M)$ is decidable. ⊣

PROPOSITION 2.5. *Let K be a presented field with elimination theory. Suppose that K is Hilbertian and let z_0 be a recursively presented element of K_s. Then, we can for every positive integer e recursively construct a decidable perfect PAC algebraic extension M of K with $z_0 \in M$ and* $\mathrm{Gal}(M) \cong \hat{F}_e$ *which is recursive in $\tilde{K}$.*

https://doi.org/10.1017/jsl.2017.10 Published online by Cambridge University Press

PROOF. We construct a primitive recursive list $(G_1, G_2, G_3, \ldots)$ of all finite non-trivial groups that are generated by e elements. By the first paragraph of this section, $\tilde{K}$ has the splitting algorithm. Hence, by [4, p. 405, Lemma 19.1.3(c)] applied to $\tilde{K}$ rather than to K, we may find out whether a given polynomial $f \in K[T, X]$ is irreducible over $\tilde{K}$. We use this test to build a recursive list $(f_1, f_2, f_3, \ldots)$ of all absolutely irreducible polynomials in $K[T, X]$ that are monic and separable in X. The rest of the proof breaks up into several parts.

PART A: *The induction plan.* By induction we construct an ascending sequence $(N_0, N_1, N_2, \ldots)$ of finite Galois extensions of K in K_s and for each $n \geq 0$ an extension M_n of K in N_n such that

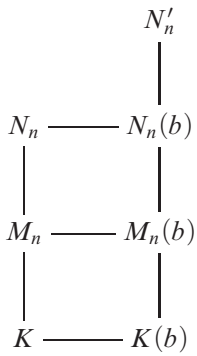
(1) $z_0 \in M_0$ and $\mathrm{Gal}(N_0/M_0)$ is generated by e elements, and for each $n \geq 1$ we have:
(2a) $z_n \in N_n$ (where, as in the beginning of this section, $z_1, z_2, z_3, \ldots$ present K_s over K).
(2b) There exist $a \in K$ and $b \in M_n$ such that $f_n(a, b) = 0$.
(2c) The group $\mathrm{Gal}(N_n/M_n)$ is generated by e elements, it has G_n as a quotient, and $N_{n-1} \cap M_n = M_{n-1}$.

PART B: *The field* N_n'. Let N_0 be the Galois closure of $K(z_0)/K$ and set $M_0 = N_0$. Then, (1) holds. Next we consider $n \geq 1$ and assume that $N_0, \ldots, N_n$ and $M_0, \ldots, M_n$ have already been constructed such that (2) holds with n replaced by m for $m = 0, \ldots, n$.

Since f_{n+1} is absolutely irreducible, f_{n+1} is irreducible over N_n. Hence, we can use Lemma 2.3 to construct a separable Hilbert subset H of K such that $f_{n+1}(a, X)$ is irreducible over N_n for each $a \in H$. Then, we use Lemma 2.2 to choose $a \in K$ such that $a \in H$. In the next step we choose $b \in K_s$ with $f_{n+1}(a, b) = 0$. Hence, N_n and $K(b)$ are linearly disjoint over K, so $N_n \cap M_n(b) = M_n$. Therefore,

(3) res: $\mathrm{Gal}(N_n(b)/M_n(b)) \to \mathrm{Gal}(N_n/M_n)$ is an isomorphism.

We use [4, p. 412, Lemma 19.3.2] to construct the Galois closure N_n' of $N_n(b, z_{n+1})/K$.



PART C: *Construction of* N_{n+1}. We compute the order r of G_{n+1} and embed G_{n+1} into the symmetric group S_r. For every field F, the Galois group of the general polynomial $X^r + T_1 X^{r-1} + \cdots + T_r$ over $F(T_1, \ldots, T_r)$ is the symmetric group S_r [9, p. 272, Example VI.2.2]. The proof of [4, p. 231, Lemma 13.3.1] gives a

https://doi.org/10.1017/jsl.2017.10 Published online by Cambridge University Press

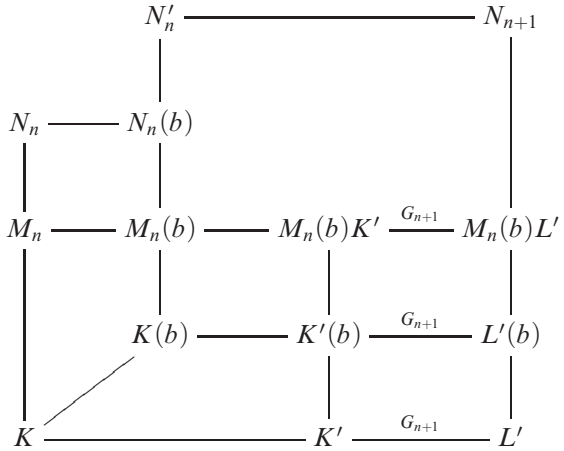
separable Hilbert subset H of F^r such that $\mathrm{Gal}(X^r + a_1 X^{r-1} + \cdots + a_r, F) \cong S_r$ for each $\mathbf{a} \in H$.

By Lemma 2.3 applied to the general polynomial of degree r and to the field N_n' rather than the field L, we can recursively find a Galois extension L' of K with Galois group S_r such that $N_n' \cap L' = K$. We set $N_{n+1} = N_n' L'$.

PART D: *Construction of* M_{n+1}. By the preceding paragraph,

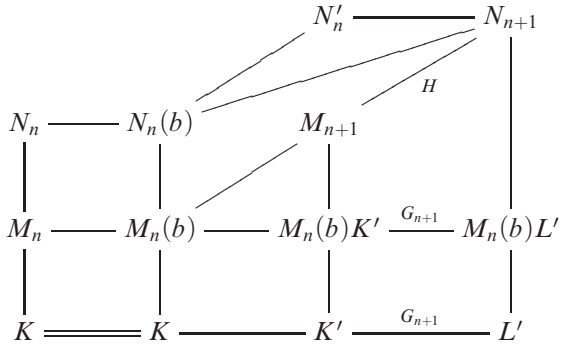
$$\mathrm{Gal}(N_{n+1}/M_n(b)) \cong \mathrm{Gal}(N_n'/M_n(b)) \times \mathrm{Gal}(M_n(b)L'/M_n(b)). \tag{4}$$

In addition, $M_n(b)$ is linearly disjoint from L' over K. We find $\tau_1, \ldots, \tau_e$ in $\mathrm{Gal}(L'/K)$ that generate a subgroup which is isomorphic to G_{n+1} [4, p. 412, Lemma 19.3.2] and set K' to be the fixed field of $\tau_1, \ldots, \tau_e$ in L'. Then, $\mathrm{Gal}(M_n(b)L'/M_n(b)K') \cong \mathrm{Gal}(L'/K') \cong G_{n+1}$.



By (2c) and (3), we find $\sigma_{n,1}, \ldots, \sigma_{n,e}$ in $\mathrm{Gal}(N_n'/M_n(b))$ whose restriction to $N_n(b)$ generate $\mathrm{Gal}(N_n(b)/M_n(b))$, so their restrictions to N_n generate $\mathrm{Gal}(N_n/M_n)$. By (4), we can find $\sigma_{n+1,1}, \ldots, \sigma_{n+1,e}$ in $\mathrm{Gal}(N_{n+1}/M_n(b))$ whose restrictions to N_n' are $\sigma_{n,1}, \ldots, \sigma_{n,e}$, respectively, and whose restrictions to L' are $\tau_1, \ldots, \tau_e$, respectively. Now consider the subgroup $H = \langle \sigma_{n+1,1}, \ldots, \sigma_{n+1,e} \rangle$ of $\mathrm{Gal}(N_{n+1}/M_n(b))$. Then, the restriction of H to L' is G_{n+1} and the restriction of H to N_n is $\mathrm{Gal}(N_n/M_n)$. Let M_{n+1} be the fixed field of H in N_{n+1}. Then, G_{n+1} is a quotient of $\mathrm{Gal}(N_{n+1}/M_{n+1})$, and $N_n \cap M_{n+1} = M_n$. This concludes the $(n+1)$th step of the induction.

We put all of the fields mentioned above in the following diagram:



https://doi.org/10.1017/jsl.2017.10 Published online by Cambridge University Press

PART E: *The field* M_∞. By the defining property of $z_1, z_2, z_3, \ldots$ and by (2a), $\bigcup_{n=1}^{\infty} N_n = K_s$. By Part A, $M_\infty = \bigcup_{n=1}^{\infty} M_n$ is a recursive extension of K in K_s. Moreover, for $n' > n$, (2c) and induction on $n' - n$ imply that $M_{n'} \cap N_n = M_n$. Hence, $M_\infty \cap N_n = M_n$ for each positive integer n. Also, $\mathrm{Gal}(M_\infty)$ is the inverse limit of the groups $\mathrm{Gal}(N_n/M_n)$. Since each of these groups is generated by e elements, so is $\mathrm{Gal}(M_\infty)$ (as a profinite group). In addition, since G_n is a quotient of $\mathrm{Gal}(N_n/M_n)$, each finite group which is generated by e elements is a quotient of $\mathrm{Gal}(M_\infty)$. Hence, $\mathrm{Gal}(M_\infty) \cong \hat{F}_e$ [4, p. 360, Lemma 17.7.1]. Finally, by (2b), each absolutely irreducible polynomial in two variables with coefficients in K has a zero in M_∞. Therefore, by [4, p. 195, Theorem 11.2.3], M_∞ is PAC.

PART F: *The field* M_∞ *is recursive in* K_s. Next we show how to decide whether a given monic separable polynomial $f \in K[X]$ of degree ≥ 1 has a root in M_∞. Since K has the splitting algorithm, we may assume that f is irreducible. Moreover, since K_s has the splitting algorithm, we may find a root z of f in K_s and identify z as z_n for some positive integer n. By (2a), $z \in N_n$ and so f totally splits in N_n. We check whether $\mathrm{Gal}(N_n/M_n)$ fixes any of the roots of f (by [4, p. 412, Lemma 19.3.2]). This will be the case if and only if f has a root in M_n. Since, by Part E, $N_n \cap M_\infty = M_n$, this will be the case if and only if f has a root in M_∞.

In the situation of the preceding paragraph, we may check whether G_n fixes z, hence whether $z \in M_\infty$. This proves that M_∞ is recursive in K_s.

PART G: *Conclusion of the proof*. Finally, let M be the maximal purely inseparable extension of M_∞ in $\tilde{K}$. Then, M is recursive in $\tilde{K}$ (Lemma 1.3), M is PAC [4, p. 196, Corollary 11.2.5], and $\mathrm{Gal}(M) \cong \mathrm{Gal}(M_\infty) \cong \hat{F}_e$. It follows from Lemma 2.4 that M is decidable. ⊣

We are now in a position to prove a stronger version of Theorem B of the introduction.

THEOREM 2.6. *Let K be a presented field with elimination theory. Suppose that K is Hilbertian. Then, we can for every positive integer e construct an infinite sequence of decidable PAC perfect fields which are recursive in $\tilde{K}$, each with absolute Galois group isomorphic to $\hat{F}_e$.*

PROOF. Let n be a non-negative number and assume that we have already constructed n distinct decidable PAC perfect fields $M^{(1)}, \ldots, M^{(n)}$ with absolute Galois groups isomorphic to $\hat{F}_e$ and which are recursive in $\tilde{K}$. In particular, $M^{(1)}, \ldots, M^{(n)}$ are proper K-vector-subspaces of $\tilde{K}$. Hence, $\bigcup_{i=1}^{n} M^{(i)}$ is a proper subset of $\tilde{K}$ [6, p. 11, A 1.1.c]. Since each $M^{(i)}$ is a recursive subset of $\tilde{K}$, we may find $z \in \tilde{K} \smallsetminus \bigcup_{i=1}^{n} M^{(i)}$.

By Proposition 2.5, $K(z)$ has an extension $M^{(n+1)}$ which is perfect, PAC, decidable, $\mathrm{Gal}(M^{(n+1)}) \cong \hat{F}_e$, and is a recursive subfield of $\tilde{K}$. Finally note that the condition $z \in M^{(n+1)}$ implies that $M^{(n+1)} \neq M^{(i)}$ for $i = 1, \ldots, n$. This concludes the induction. ⊣

REMARK 2.7. If N is a Galois extension of K and $\mathrm{Ex}(N)$ is decidable (resp. primitive recursively decidable), then N is also a recursive (resp. primitive recursive) subfield of K_s, hence also of $\tilde{K}$. Indeed, if $z \in K_s$, we construct $\mathrm{irr}(z, K)$ and check whether $\mathrm{irr}(z, K)$ has a root in N. This is the case if and only if all of the roots of $\mathrm{irr}(z, K)$ belong to N, hence if and only if $z \in N$.

https://doi.org/10.1017/jsl.2017.10 Published online by Cambridge University Press

For example, the field $\mathbb{Q}_{\mathrm{tr}}$ of all totally real algebraic numbers is a Galois extension of $\mathbb{Q}$ and $\mathrm{Th}(\mathbb{Q}_{\mathrm{tr}})$ is primitive recursively decidable [3, p. 90, Theorem 10.1]. If S is a finite number of prime numbers, then the field $\mathbb{Q}_{\mathrm{tot},S}$ of all totally S-adic numbers is decidable, by [1]. By the preceding paragraph, $\mathbb{Q}_{\mathrm{tot},S}$ is recursive in $\tilde{\mathbb{Q}}$.

§3. Primitive recursively decidable fields. The goal of this section is to explain how to strengthen Theorem 2.6 in the case where the base field K is a presented field with elimination theory which is "effectively Hilbertian".

To this end we say that K is *effectively Hilbertian* if there is an effective procedure (in the sense of [4, Chapter 19]) to check for each given separable Hilbert set H if H is nonempty. In particular, that procedure is primitive recursive.

With that notion, the proof of Lemma 2.3 proves mutatis mutandis the following result:

LEMMA 3.1. *Let K be a presented field with elimination theory which is effectively Hilbertian. Let L be a presented finite separable extension of K and let H be a presented separable Hilbert subset of L^r. Then, we can effectively find a separable Hilbert subset H_K of K^r which is contained in H. In particular, L is also effectively Hilbertian.*

EXAMPLE 3.2. We claim that every presented infinite finitely generated field (over its prime field) is effectively Hilbertian.

That $\mathbb{Q}$ is effectively Hilbertian follows from a strong result of Yann Walkowiak [15, p. 345, Theorem 2]. That result says that if f is a primitive polynomial in $\mathbb{Z}[X, Y]$ of total degree d, of degree $n \geq 2$ in Y, if m is the maximum of the absolute values of the coefficients of f and the number e^e (where e is the basis of the natural logarithm), and if s is a positive integer, then there exist s positive integers $x_1, \ldots, x_s$ less than $\bar{m} = (s + 2^{88} d^{45} \log^{19}(m))^4$ such that each $f(x_i, Y)$ is irreducible in $\mathbb{Q}[Y]$. Given a nonzero polynomial $g \in \mathbb{Q}[X]$ of degree less than s, we may use the splitting algorithm of $\mathbb{Q}$ to check whether $f(x, Y)$ is irreducible in $\mathbb{Q}[Y]$ for $x = 1, \ldots, \bar{m}$ in order to find x such that $f(x, Y)$ is irreducible and $g(x) \neq 0$. Thus, $\mathbb{Q}$ is effectively Hilbertian.

By Lemma 3.1, each presented number field is also effectively Hilbertian.

The proof of our claim in all other cases needs more space and would go beyond the scope of this work. So, we restrict ourselves to some hints for the proofs.

In order to prove that a presented finitely generated infinite field K is effectively Hilbertian, it suffices by Lemma 3.1, to prove it only in the cases where K is either $K_0(t)$, where K_0 is an infinite finitely generated field and t is indeterminate, or $K = \mathbb{F}_p(t)$.

In the first case, we notice that the proof of [4, p. 236, Proposition 13.2.1] reduces the effective Hilbertianity to the primitive recursiveness of $\mathrm{Th}(\tilde{K}_0)$, using [4, p. 170, Proposition 9.4.3].

The case where $K = \mathbb{F}_p(t)$ (and actually where $K = \mathbb{Q}$) involves effective operations in $\mathbb{Z}$ like factoring polynomials into products of irreducible polynomials in $\mathbb{F}_p[t]$ (and positive integers into products of prime numbers) and an effective Chebotarev density theorem. All of this appear in the proof of Theorem 13.3.5 of [4] and the lemmata that proceed it in Chapter 13 of [4].

https://doi.org/10.1017/jsl.2017.10 Published online by Cambridge University Press

Another new ingredient that enters our proof is the following "primitive recursive invariant" of Lemma 2.4. To this end recall that a profinite group G is said to have the *embedding property* if for every epimorphism $\alpha\colon B \to A$ of finite groups such that B is a quotient of G and every epimorphism $\phi\colon G \to A$ there exists an epimorphism $\gamma\colon G \to B$ with $\alpha \circ \gamma = \phi$ [4, p. 564, Definition 24.1.2]. We denote the set of all finite quotients of G by $\mathrm{Im}(G)$.

LEMMA 3.3. *Let K be a presented field with elimination theory. Let M be an extension of K in $\tilde{K}$. Suppose that M is perfect and PAC,* $\mathrm{Gal}(M)$ *has the embedding property, and* $\mathrm{Im}(\mathrm{Gal}(M))$ *is primitive recursive. Further suppose that the set* $\mathrm{Root}(M)$ *is primitive recursive. Then,* $\mathrm{Th}(M)$ *is primitive recursively decidable.*

PROOF. We assume in this proof that the reader is acquainted with the methods of Galois Stratification, as presented in [4, Chapter 30]. Following the text that precedes Theorem 30.6.2 of [4] let θ be an effectively given sentence of $\mathcal{L}(\mathrm{ring}, K)$.

The Galois stratification procedure, in particular Lemmas 30.4.1 and 30.4.2 of [4] effectively gives a finite Galois extension L of K and a conjugacy domain Con of subgroups of $\mathrm{Gal}(L/K)$ such that $M \models \theta$ if and only if $\mathrm{Gal}(L/L \cap M) \in \mathrm{Con}$. We effectively compute $z_1, \ldots, z_n$ in L such that $K(z_1), \ldots, K(z_n)$ are all of the subfields of L that contain K. Since $\mathrm{Root}(M)$ is primitive recursive, we can effectively check for each $1 \leq i \leq n$ whether the polynomial $\mathrm{irr}(z_i, K)$ has a root in M, that is whether $K(z_i)$ has a K-embedding into M. Doing that, we effectively find $1 \leq j \leq n$ such that $K(z_j)$ has a K-embedding into M but no proper extension of $K(z_j)$ in L has a K-embedding into M. Thus, $K(z_j)$ is K-conjugate to $L \cap M$. Finally we effectively check whether $\mathrm{Gal}(L/K(z_j))$ belongs to Con, hence whether $\mathrm{Gal}(L/L \cap M)$ belongs to Con in order to primitive recursively decide whether $M \models \theta$. ⊣

Now we consider the case where G is the free profinite group $\hat{F}_e$ of e generators for some positive integer e. By [4, p. 361, Proposition 17.7.3], $\hat{F}_e$ has the embedding property. Also, the set $\mathrm{Im}(\hat{F}_e)$ consists of all finite groups that are generated by e elements. Thus, $\mathrm{Im}(\hat{F}_e)$ is a primitive recursive set of finite groups. Therefore, the following result is a special case of Lemma 3.3.

LEMMA 3.4. *Let K be a presented field with elimination theory. Let M be an extension of K in $\tilde{K}$. Suppose that M is perfect, PAC, and* $\mathrm{Gal}(M) \cong \hat{F}_e$, *Further suppose that the set* $\mathrm{Root}(M)$ *is primitive recursive. Then,* $\mathrm{Th}(M)$ *is primitive recursively decidable.*

Having Lemma 3.4 at our disposal, we can follow the proofs of Proposition 2.5 and Theorem 2.6 mutatis mutandis in order to prove the following result:

THEOREM 3.5. *Let K be a presented field with elimination theory. Suppose that K is effectively Hilbertian. Then, we can for every positive integer e construct an infinite sequence of primitive recursively decidable perfect PAC fields each of which is primitive recursive in $\tilde{K}$ with absolute Galois group isomorphic to $\hat{F}_e$.*

§4. Appendix. We prove in this appendix a statement made in the introduction.

For each field K, every positive integer e, and every $\boldsymbol{\sigma} \in \mathrm{Gal}(K)^e$ we denote the maximal purely inseparable extension of $K_s(\boldsymbol{\sigma})$ by $\tilde{K}(\boldsymbol{\sigma})$.

https://doi.org/10.1017/jsl.2017.10 Published online by Cambridge University Press

PROPOSITION 4.1. *Let K be a Hilbertian field and let e be a positive integer. Then, there are uncountably many elementary equivalence classes (in the language $\mathcal{L}(\mathrm{ring}, K)$) of fields of the form $\tilde{K}(\boldsymbol{\sigma})$ with $\boldsymbol{\sigma} \in \mathrm{Gal}(K)^e$.*

Moreover, the Haar measure of the set of pairs $(\boldsymbol{\sigma}, \boldsymbol{\sigma}') \in \mathrm{Gal}(K)^{2e}$ such that $K_s(\boldsymbol{\sigma})$ and $K_s(\boldsymbol{\sigma}')$ are not equivalent as structures of the language $\mathcal{L}(\mathrm{ring}, K)$ is 1.

PROOF. Using the assumption that K is Hilbertian, we construct, by induction, a linearly disjoint sequence $K_1, K_2, K_3, \ldots$ of quadratic separable extensions of K [4, p. 297, Corollary 16.2.7(b)] (if $\mathrm{char}(K) = 2$, one has to use [4, p. 296, Example 16.2.5(c) and p. 297, Lemma 16.2.6]). Let L be the compositum of all these extensions. Then, $\mathrm{Gal}(L/K)$ is an infinite profinite group of exponent 2. In particular, the closed subgroup generated by every finite subset of $\mathrm{Gal}(L/K)$ is finite, hence has Haar measure 0 in $\mathrm{Gal}(L/K)$.

We denote the normalized Haar measure of $\mathrm{Gal}(L/K)$ by μ. For each $\boldsymbol{\sigma} = (\sigma_1, \ldots, \sigma_e) \in \mathrm{Gal}(L/K)^e$ we denote the fixed field of $\sigma_1, \ldots, \sigma_e$ in L by $L(\boldsymbol{\sigma})$ and let $\langle \boldsymbol{\sigma} \rangle = \mathrm{Gal}(L/L(\boldsymbol{\sigma}))$ be the closed subgroup of $\mathrm{Gal}(L/K)$ generated by $\sigma_1, \ldots, \sigma_e$.

If there are only countably many fields $L(\boldsymbol{\sigma}^{(1)}), L(\boldsymbol{\sigma}^{(2)}), L(\boldsymbol{\sigma}^{(3)}), \ldots$ with $\boldsymbol{\sigma}^{(i)} \in \mathrm{Gal}(L/K)^e$, then $\mathrm{Gal}(L/K) = \bigcup_{i=1}^{\infty} \langle \boldsymbol{\sigma}^{(i)} \rangle$, so $1 = \mu(\mathrm{Gal}(L/K)) \leq \sum_{i=1}^{\infty} \mu(\langle \boldsymbol{\sigma}^{(i)} \rangle) = 0$, which is a contradiction. Hence, there is an uncountable subset S of $\mathrm{Gal}(L/K)^e$ such that $L(\boldsymbol{\sigma}) \neq L(\boldsymbol{\sigma}')$ for every distinct elements $\boldsymbol{\sigma}$ and $\boldsymbol{\sigma}'$ of S.

We extend each $\boldsymbol{\sigma} \in S$ to an element $\tilde{\boldsymbol{\sigma}}$ of $\mathrm{Gal}(K)^e$. If $\boldsymbol{\sigma}' \in S$ and $\boldsymbol{\sigma}' \neq \boldsymbol{\sigma}$, then $K_s(\tilde{\boldsymbol{\sigma}})$ is not K-conjugate to $K_s(\widetilde{\boldsymbol{\sigma}'})$, otherwise $L(\boldsymbol{\sigma})$ and $L(\boldsymbol{\sigma}')$ are K-conjugate, hence equal, because $\mathrm{Gal}(L/K)$ is abelian. It follows from [4, p. 441, Lemma 20.6.3(b)] that $\tilde{K}(\tilde{\boldsymbol{\sigma}})$ and $\tilde{K}(\widetilde{\boldsymbol{\sigma}'})$ are not elementarily equivalent as structures of $\mathcal{L}(\mathrm{ring}, K)$. This proves the first statement of the proposition.

The proof of the second statement of the proposition is based on the observation that the diagonal D of $\mathrm{Gal}(L/K)^e$ has Haar measure 0 in $\mathrm{Gal}(L/K)^{2e}$. This is so, because $\mathrm{Gal}(L/K)^e$ is an infinite profinite group and for every finite group G, the proportion of the diagonal $\{(g, g) \in G^2 \mid g \in G\}$ in G^2 is $\frac{1}{|G|}$. It follows from [5, p. 279, Theorem C] that the set $\tilde{D} = \{(\boldsymbol{\sigma}, \boldsymbol{\sigma}') \in \mathrm{Gal}(K)^{2e} \mid \boldsymbol{\sigma}|_L \neq \boldsymbol{\sigma}'|_L\}$ has Haar measure 1. By the preceding paragraph, $K_s(\boldsymbol{\sigma})$ is not elementarily equivalent to $K_s(\boldsymbol{\sigma}')$ for all $(\boldsymbol{\sigma}, \boldsymbol{\sigma}') \in \tilde{D}$. ⊣

§5. Acknowledgments. The first author was supported by the Minkowski Center for Geometry at Tel Aviv University, established by the Minerva Foundation. The second author was partially supported by a National Science Foundation Grant DMS-1161456. The authors are indebted to Aharon Razon for critically reading a draft of this work. We are also indebted to the anonymous referee for helpful observations.

REFERENCES

[1] Y. L. ERSHOV, *Nice local-global fields I.* ***Algebra and Logic***, vol. 35 (1996), pp. 229–235.

[2] M. FRIED, D. HARAN, and M. JARDEN, *Galois stratification over Frobenius fields.* ***Advances of Mathematics***, vol. 51 (1984), pp. 1–35.

[3] M. D. FRIED, D. HARAN, and H. VÖLKLEIN, *Real hilbertianity and the field of totally real numbers.* ***Contemporary Mathematics***, vol. 174 (1994), pp. 1–34.

[4] M. D. Fried and M. Jarden, ***Field Arithmetic***, third ed., revised by Moshe Jarden, Ergebnisse der Mathematik (3), vol. 11, Springer, Heidelberg, 2008.

[5] P. R. Halmos, ***Measure Theory,*** D. Van Nostrand Company, Princeton, 1968.

[6] B. Huppert, ***Angewandte Linear Algebra,*** de Gruyter, Berlin, 1990.

[7] M. Jarden, *Intersection of local algebraic extensions of a Hilbertian field,* ***Generators and Relations in Groups and Geometries*** (A. Barlotti, E. W. Ellers, P. Plaumann and K. Strambach, editors), NATO ASI Series C, vol. 333, Kluwer, Dordrecht, 1991, pp. 343–405.

[8] M. Jarden and U. Kiehne, *The elementary theory of algebraic fields of finite corank.* ***Inventiones Mathematicae***, vol. 30 (1975), pp. 275–294.

[9] S. Lang, ***Algebra***, third ed., Addison-Wesley, Reading, 1993.

[10] D. Marker, ***Model Theory: An Introduction,*** Springer, New York, 2002.

[11] A. Prestel, *Pseudo real closed fields,* ***Set Theory and Model Theory***, Lecture Notes, vol. 872, Springer, Berlin-New York, 1981, pp. 127–156.

[12] A. Prestel and P. Roquette, ***Formally p-adic Fields,*** Lecture Notes in Mathematics, vol. 1050, Springer, Berlin, 1984.

[13] F. K. Schmidt, *Mehrfach perfekte Körper.* ***Mathematische Annalen***, vol. 108 (1933), pp. 1–25.

[14] A. Tarski, ***A decision Method for Elementary Algebra and Geometry,*** The RAND Corporation, Santa Monica, 1948. Available at http://www.rand.org/content/dam/rand/pubs/reports/2008/R109.pdf.

[15] Y. Walkowiak, *Théorème d'irréductibilité de Hilbert effectif.* ***Acta Arithmetica***, vol. 116 (2005), pp. 343–362.

[16] V. Weispfenning, *Quantifier elimination and decision procedures for valued fields,* ***Models and Sets***, Lecture Notes in Mathematics, vol. 1103, Springer, Berlin, 1984, pp. 419–472.

SCHOOL OF MATHEMATICS
TEL AVIV UNIVERSITY
RAMAT AVIV
TEL AVIV 6139001, ISRAEL
E-mail: jarden@post.tau.ac.il

DEPARTMENT OF MATHEMATICS
EAST CAROLINA UNIVERSITY
UNIVERSITY GREENVILLE
NC 27858-4353, USA
E-mail: shlapentokha@ecu.edu