PROCEEDINGS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 150, Number 8, August 2022, Pages 3335–3343
https://doi.org/10.1090/proc/15920
Article electronically published on April 1, 2022

ODONI'S CONJECTURE ON ARBOREAL GALOIS REPRESENTATIONS IS FALSE

PHILIP DITTMANN AND BORYS KADETS

(Communicated by Rachel Pries)

ABSTRACT. Suppose $f \in K[x]$ is a polynomial. The absolute Galois group of K acts on the preimage tree T of 0 under f. The resulting homomorphism $\phi_f \colon \mathrm{Gal}_K \to \mathrm{Aut}\,\mathrm{T}$ is called the arboreal Galois representation. Odoni conjectured that for all Hilbertian fields K there exists a polynomial f for which ϕ_f is surjective. We show that this conjecture is false.

1. INTRODUCTION

Suppose that K is a field and $f \in K[x]$ is a polynomial of degree d. Suppose additionally that f and all of its iterates $f^{\circ k}(x) := f \circ f \circ \cdots \circ f$ are separable. To f we can associate the arboreal Galois representation – a natural dynamical analogue of the Tate module – as follows. Define a graph structure on the set of vertices $V := \bigsqcup_{k \geqslant 0} \left(f^{\circ k}\right)^{-1}(0)$ by drawing an edge from α to β whenever $f(\alpha) = \beta$. The resulting graph is a complete rooted d-ary tree $\mathrm{T}_\infty(d)$, see Figure 1. The Galois group Gal_K acts on the roots of the polynomials $f^{\circ k}$ and preserves the tree structure; this defines a morphism $\phi_f \colon \mathrm{Gal}_K \to \mathrm{Aut}\,\mathrm{T}_\infty(d)$ known as the arboreal representation attached to f.

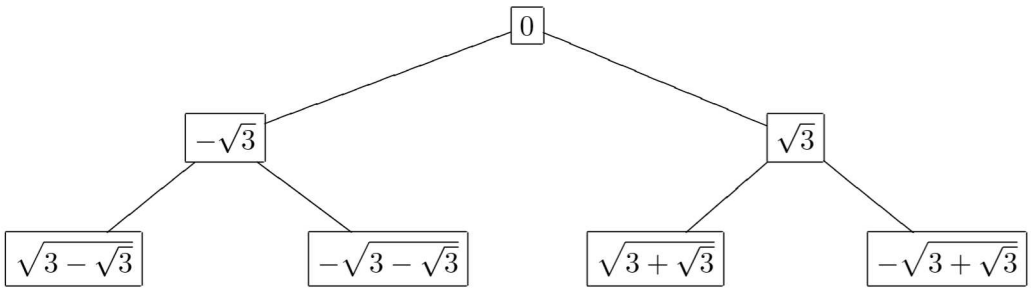

FIGURE 1. First two levels of the tree $\mathrm{T}_\infty(2)$ associated with the polynomial $f = x^2 - 3$

This definition is analogous to that of the Tate module of an elliptic curve, where the polynomial f is replaced by the multiplication-by-p morphism. However,

Received by the editors February 8, 2021, and, in revised form, September 13, 2021, and November 22, 2021.

2020 *Mathematics Subject Classification.* Primary 12F10, 12E25.

This material is based upon work supported by the National Science Foundation under Grant No. DMS-1928930 while the authors participated in a program hosted by the Mathematical Sciences Research Institute in Berkeley, California, during the Fall 2020 semester.

in contrast to the case of Tate modules, arboreal representations are rather poorly understood. In particular, the images of arboreal representations are often expected to be large (see [Jon13] for a survey), even though describing these images is out of reach even for some quadratic polynomials.

In [Odo85] Odoni proves that for the generic polynomial the associated arboreal representation is surjective. Therefore, over fields in which Hilbert's irreducibility theorem holds – the so-called Hilbertian fields – for every integer k the Galois group of $f^{\circ k}$ is maximal for infinitely many polynomials f. He then asks if the same holds for the whole arboreal representation.

Conjecture 1.1 ([Odo85, Conjecture 7.5.])**.** *Suppose K is a Hilbertian field of characteristic zero, and $d > 1$ is an integer. Then there exists a degree d monic polynomial $f \in K[x]$ such that the associated arboreal representation $\phi_f \colon \mathrm{Gal}_k \to \mathrm{Aut}\, \mathrm{T}_\infty(d)$ is surjective.*

Most of the work on arboreal representations focuses on the cases when K is a number field or a function field. For example, Odoni's conjecture is known to be true for all number fields; this was proved in varying degrees of generality in [Spe18], [BJ19], [Kad20]. The goal of this paper is to disprove Odoni's conjecture.

Theorem 1.2. *Suppose k is a countable Hilbertian field of characteristic zero. There exists a Hilbertian algebraic field extension F/k such that for every $f \in F[x]$ of degree $d \geqslant 2$ the image of the associated arboreal representation has infinite index in $\mathrm{Aut}\, \mathrm{T}_\infty(d)$.*

We give two separate proofs for Theorem 1.2. The first proof involves a very explicit general construction applicable to countable collections of special field extensions, of which finite index arboreal representations are a special case. To state the more general result we need Definition 1.3.

Definition 1.3. An algebraic field extension L/K is called *vast* if $L \neq K$ and for every finite extension F/K there exists a subfield $M \supsetneq K$ of L such that M and F are linearly disjoint over K.

The general result that will be used to prove Theorem 1.2 is Theorem 1.4.

Theorem 1.4. *Let k denote a countable Hilbertian field of characteristic 0. Suppose $\mathcal{A}$ is a countable collection of vast extensions L/K, such that for every $L/K \in \mathcal{A}$ the field K is a finite extension of k. Then there exists an algebraic Hilbertian field extension F/k such that:*

1. *the degree $[F : k]$ divides the product of degrees of the extensions from $\mathcal{A}$ (as supernatural numbers);*
2. *for every subextension K/k of F/k and every extension L/K from $\mathcal{A}$ the extensions F/K and L/K are not linearly disjoint.*

From Theorem 1.4 it is easy to deduce Theorem 1.2, with a field F/k whose degree (as a supernatural number) is a power of two.

In Section 3, we give a second proof of Theorem 1.2 using model-theoretic techniques. The counterexamples to Odoni's conjecture constructed there are of a very special kind, as they are pseudo-algebraically closed. The argument crucially relies on the fact that the class of Hilbertian pseudo-algebraically closed fields is model-theoretically well understood. However, the result obtained in this way through an abstract existence theorem is slightly weaker than what is given by the first proof,

see Remark 3.3. In particular, weaker control on the degree of F/k is obtained in the second proof, see Remark 3.2; for instance when $k = \mathbb{Q}$ the degree of F over $\mathbb{Q}$ obtained in this way is divisible by every natural number. Nevertheless the second proof seems to be of independent interest due to the techniques used.

2. An explicit construction of a counterexample

Throughout the paper we assume that all fields have characteristic zero. We begin by recalling the definition of a Hilbertian field.

Definition 2.1. A characteristic zero field K is called *Hilbertian* if for every smooth geometrically integral curve X/K and any nonconstant morphism $f\colon X \to \mathbb{P}^1_K$ of degree at least 2, there are infinitely many points $x \in \mathbb{P}^1(K)$ such that $f^{-1}(x)$ is integral.

Over such fields Hilbert's irreducibility theorem holds; hence the name. See [FJ08, Chapters 12, 13] for a detailed discussion of Hilbertian fields.

Remark 2.2. There are a few (equivalent) definitions of a Hilbertian field in the literature; the equivalence of Definition 2.1 with other commonly used definitions is proved in [BS08, Theorem 1.1]. Note that [BS08, Theorem 1.1] writes the main results in terms of polynomials. We now explain why the two definitions are equivalent. To disambiguate the notational conflicts with [BS08], we write the notation from [BS08] in bold. To arrive at Definition 2.1 in the notation of [BS08] take the curve X of Definition 2.1 to be the normalization of the projective closure of $\mathbf{f}(T, X) = 0$ in [BS08] and the morphism f of Definition 2.1 to be the $\mathbf{T}$ coordinate on $\mathbf{f}(T, X) = 0$. Definition 2.1 is not more general than the one from [BS08], since every X, f from definition 2.1 has a birational model of the form $\mathbf{f}(T, X) = 0$ with the map f given by the $\mathbf{T}$-coordinate map.

Before proving Theorem 1.4, we need the following simple property of vast extensions.

Lemma 2.3. *Let L/K be a vast extension. Suppose K'/K is a finite extension linearly disjoint from L/K. Then LK'/K' is vast.*

Proof. Suppose F/K' is a finite extension. We need to construct a finite subextension of LK'/K' linearly disjoint from F. Consider the extension F/K. Since L/K is vast, there exists a finite subextension M/K of L/K linearly disjoint from F/K. The compositum FM/K of F and M has degree $[F : K][M : K]$. Since $K' \subset F \subset FM$, the extension M/K is linearly disjoint from K'/K and the degree of FM over K' is

$$[FM : K'] = [F : K][M : K][K' : K]^{-1} = [F : K'][M : K] = [F : K'][K'M : K'].$$

Since FM/K' is the compositum of F/K' and $K'M/K'$, the degree formula above implies that F/K' and $K'M/K'$ are linearly disjoint. Thus $K'M/K'$ is a subfield of LK'/K' linearly disjoint from F/K'. □

Proof of Theorem 1.4. By Lemma 2.3, without loss of generality, we can assume that if L/K is an element of $\mathcal{A}$ and K'/K is a finite extension linearly disjoint from L, then LK'/K' is also an element of $\mathcal{A}$. We can also assume that no finite extension F/k satisfies the conclusion of the theorem.

The idea of the proof is to carefully construct a tower of extensions $k = F_1 \subset F_2 \subset \dots$ such that all elements of $\mathcal{A}$ defined over a finite subextension of $F = \bigcup F_n$ are not linearly disjoint from F, and yet F is Hilbertian. This is achieved by a "diagonal argument": we inductively produce extensions F_{n+1}/F_n that are not linearly disjoint from a smallest element of $\mathcal{A}$ in a certain ordering, while at the same time keeping fibers of finitely many coverings integral when base changed to F_n to eventually force F to be Hilbertian.

Fix an ordering of all elements of $\mathcal{A}$ by natural numbers. Let $\mathcal{B}$ be a list of all covers of smooth geometrically integral curves $f\colon X \to \mathbb{P}^1$, $\deg f \geqslant 2$ defined over some finite extension of k, with every covering repeated in $\mathcal{B}$ infinitely many times. We now produce sequences of fields $F_1 \subset F_2 \subset \dots \subset F_n \subset \dots$, coverings $f_n \in \mathcal{B}, f_n\colon X_n \to \mathbb{P}^1$, points $c_n \in \mathbb{P}^1$, and extensions $L_n/K_n \in \mathcal{A}$, indexed by natural numbers, with the following properties, that depend on a parameter $m \in \mathbb{N}$.

- (1_m) The point c_m belongs to $\mathbb{P}^1(F_m)$ and does not coincide with c_i for $i < m$.
- (2_m) For every $i \leqslant m$ the scheme $f_i^{-1}(c_i)$ is integral, and the function field $F_i(f_i^{-1}(c_i))$ of $f_i^{-1}(c_i)$ is linearly disjoint from F_m/F_i.
- (3_m) The covering $f_m \in \mathcal{B}$ is the first element of $\mathcal{B} \setminus \{f_1, \dots, f_{m-1}\}$ defined over F_m.
- (4_m) The extension L_m/K_m is the first element of $\mathcal{A}\setminus\{L_{m-1}/K_{m-1}, \dots, L_1/K_1\}$ such that K_m is a subfield of F_m and the extensions F_m/K_m and L_m/K_m are linearly disjoint.
- (5_m) The extension F_m/F_{m-1} is a nontrivial finite subextension of $L_{m-1}F_{m-1}/F_{m-1}$.

We do so inductively. Set $F_1 = k$. Let $f_1 \in \mathcal{B}$ be the first element defined over k. Let L_1/K_1 be the first element of $\mathcal{A}$ with $K = k$; if no such element exists, then $F = k$ is a finite extension satisfying the conclusions of the theorem, which we assumed in the beginning to not exist. Choose a point $c_1 \in \mathbb{P}^1(k)$ such that $f_1^{-1}(c_1)$ is integral; such a point exists because k is Hilbertian. The properties (1_m)–(4_m) are satisfied for $m = 1$, while the property (5_m) for $m = 1$ is vacuous.

Suppose a sequence $F_m, f_m, c_m, L_m/K_m$ is defined for $m < n$ and satisfies (1_m)–(5_m). We start by constructing the field F_n. Let M denote the compositum of $F_{n-1}(f_i^{-1}(c_i))$ for all $i < n$; it is a finite extension of F_{n-1}. Let L denote the compositum $F_{n-1}L_{n-1}$. By Lemma 2.3 and property (4_m) applied for $m = n-1$, the field extension L/F_{n-1} is vast. Since L/F_{n-1} is vast and M is finite, we can choose a subextension F_n of L/F_{n-1} linearly disjoint from M. Let $f_n \in \mathcal{B}$ be the element defined by condition (3_m) for $m = n$. Let $L_n/K_n \in \mathcal{A}$ be defined by (4_m) for $m = n$; if no such element exists then by property (5_m) for $m < n$, the finite extension F_n/k satisfies the conclusion of the theorem, which does not happen by assumption. Since F_n is a finite extension of a Hilbertian field it itself is Hilbertian. Therefore there exists a point $c_n \in \mathbb{P}^1(F_n)$ distinct from c_i for $i < n$ and such that $f_n^{-1}(c_n)$ is integral. With these choices conditions (1_m)–(5_m) are satisfied for all $m < n + 1$.

Let F denote the union $\bigcup_n F_n$. We claim that F is Hilbertian. Indeed, suppose we are given a covering of $f\colon X \to \mathbb{P}^1$ defined over F, with X a smooth geometrically integral curve and $\deg f \geqslant 2$. Since a covering is defined by finitely many equations, f will be defined over F_n for some n. By condition (3_m) and the definition of $\mathcal{B}$ infinitely many of the coverings f_m are equal to f. Let $c_{n_1}, c_{n_2}, \dots \in \mathbb{P}^1(F)$ be the corresponding sequence of points. By condition (2_m) the schemes $f^{-1}(c_{n_i})$ are

integral over F. Therefore F is Hilbertian. On the other hand, conditions (4_m) and (5_m) ensure that there is no vast extension L/K in $\mathcal{A}$ such that L is linearly disjoint from F over K. Finally, by condition (5_m) the degree of F divides the product of degrees of extensions from $\mathcal{A}$. □

Before proving Theorem 1.2 we recall some group-theoretic properties of the profinite group $\operatorname{Aut} \mathrm{T}_\infty(d)$. Consider the action of $\operatorname{Aut} \mathrm{T}_\infty(d)$ on the n-th level of the tree. The sign of this action defines a homomorphism $\sigma_n \colon \operatorname{Aut} \mathrm{T}_\infty(d) \to \mathbb{Z}/2\mathbb{Z}$. Note that a simple transposition on the n-th level of the tree lifted arbitrarily to an element $g \in \operatorname{Aut} \mathrm{T}_\infty(d)$ satisfies $\sigma_m(g) = 0$ for $m < n$ and $\sigma_n(g) = 1$, therefore the homomorphisms σ_n are linearly independent in the $\mathbb{F}_2$-vector space $\operatorname{Hom}(\operatorname{Aut} \mathrm{T}_\infty(d), \mathbb{Z}/2\mathbb{Z})$. Thus the collection of all sign homomorphisms defines a homomorphism $\sigma \colon \operatorname{Aut} \mathrm{T}_\infty(d) \to \prod_{n=1}^{\infty} \mathbb{Z}/2\mathbb{Z}$ whose image is dense in the product topology. Since σ is a continuous homomorphism of profinite groups, it is then surjective. We use ϕ_n to denote the homomorphism $\phi_n := (\sigma_n, \sigma_{n+1}, \dots) \colon \operatorname{Aut} \mathrm{T}_\infty(d) \to \prod_{k=n}^{\infty} \mathbb{Z}/2\mathbb{Z}$.

Definition 2.4. Suppose K is a field and $f \in K[x]$ a monic polynomial of degree $d \geqslant 2$ such that $\phi_f \colon \operatorname{Gal}_K \to \operatorname{Aut} \mathrm{T}_\infty(d)$ has image of finite index. The n-th *discriminant extension* K_n of K attached to f is the algebraic extension of K corresponding to the kernel of $\phi_n \circ \phi_f$ in Gal_K.

Remark 2.5. The homomorphism $\phi_n \circ \phi_f$ of Definition 2.4 is not necessarily surjective. However, since the image of ϕ_f has finite index in $\operatorname{Aut} \mathrm{T}_\infty(d)$ by assumption, the image of $\phi_n \circ \phi_f$ has finite index in $\prod_{k=1}^{\infty} \mathbb{Z}/2\mathbb{Z}$, and so $\operatorname{im} \phi_n \circ \phi_f = \operatorname{Gal} K_n/K \simeq \prod_{i=1}^{\infty} \mathbb{Z}/2\mathbb{Z}$.

Remark 2.6. The term "discriminant extension" comes from the relation between the sign homomorphism and discriminants of polynomials; see [Cox12, Section 7.4.A].

Proof of Theorem 1.2. Consider the set S consisting of pairs (K, f), where K/k is a finite extension and $f \in K[X]$ is a monic polynomial of degree at least 2 such that the image of $\phi_f \colon \operatorname{Gal}_K \to \operatorname{Aut} \mathrm{T}_\infty(\deg f)$ has finite index. Let

$$\mathcal{A} := \{K_n/K \colon (K, f) \in S, \\ K_n \text{ is the } n\text{-th discriminant extension of } K \text{ attached to } f \text{ for some } n\}.$$

Since every $\prod_{n=1}^{\infty} \mathbb{Z}/2\mathbb{Z}$-extension is vast, the collection $\mathcal{A}$ satisfies the assumptions of Theorem 1.4. Therefore there exists a Hilbertian extension F/k of 2-power degree such that F is not linearly disjoint from any $K_n/K \in \mathcal{A}$ with $K \subset F$.

We wish to show that F is as desired, so suppose for a contradiction that $f \in F[X]$ is a monic polynomial of degree at least 2 with finite index arboreal representation over F. We can choose $K \subset F$ finite over k with $f \in K[X]$, so that $(K, f) \in S$. The fields K_n attached to f (over K) are nested $K_1 \supset K_2 \supset \dots$ and $\bigcap_n K_n = K$. Since F/K is not linearly disjoint from K_n for any n, $F \cap K_1$ is an infinite extension of K. Therefore the arboreal representation of f over F has infinite index in $\operatorname{Aut} \mathrm{T}_\infty(\deg f)$, giving the desired contradiction. □

3. A model-theoretic construction of a counterexample

The iterative construction from Theorem 1.4, constructing an algebraic extension which step-by-step forces all polynomials to induce arboreal representations

with image of infinite index, can also naturally be understood model-theoretically using the Omitting Types Theorem. In this section we will therefore give another construction of counterexamples to Conjecture 1.1, using standard tools from field arithmetic.

Theorem 3.1. *Let K be a countable field of characteristic zero. There exists a Hilbertian pseudo-algebraically closed extension field L of K such that every monic polynomial over L of degree $d \geqslant 2$ induces an arboreal representation whose image has infinite index in* $\operatorname{Aut} \mathrm{T}_\infty(d)$. *If K is Hilbertian, we can choose L to be algebraic over K.*

Remark 3.2. The fact that the resulting field L is pseudo-algebraically closed should be seen as an artefact of the construction. In particular, this forces L to have projective absolute Galois group (see [FJ08, Theorem 11.6.2]). If K is a number field and L/K is algebraic, this means that the degree of L/K as a supernatural number must be divisible infinitely many times by every prime number for reasons of cohomological dimension (see [NSW08, Proposition 3.3.5]), in contrast to the construction in the previous section.

Remark 3.3. Let K be a countable field of characteristic zero. If K is not Hilbertian, replace it by its Hilbertian extension $K(t)$. Then K has an algebraic extension K' which is Hilbertian and pseudo-algebraically closed (see [FJ08, Theorem 27.4.8]), and the proof in the previous section yields an algebraic extension L/K' in which every monic polynomial of any degree $d \geqslant 2$ induces an arboreal representation whose image has infinite index in $\operatorname{Aut} \mathrm{T}_\infty(d)$. This field L is then pseudo-algebraically closed as an algebraic extension of K' [FJ08, Corollary 11.2.5]. Therefore the proof in the previous section yields Theorem 3.1 as a corollary. We nevertheless think that the separate proof below is interesting in its own right.

We use basic model-theoretic terminology, with [Hod97] as our general reference, although other textbooks such as [Mar02] also contain all necessary results.

We work in the first-order language of rings, i.e. with symbols $+, -, \cdot, 0, 1$, later expanded by constants. Let us introduce some terminology for sets $p(\underline{x})$ consisting of formulae with free variables among the (finite) tuple of variables $\underline{x}$. We say that a tuple $\underline{a}$ in a structure $\mathfrak{M}$ *realises* p if $\mathfrak{M} \models \varphi(\underline{a})$ for all $\varphi \in p$. Following [Hod97, Section 6.2], we say that a formula $\varphi(\underline{x})$ *supports* the set $p(\underline{x})$ in a theory T if $T \cup \{\exists \underline{x} \varphi\}$ has a model, and for every $\psi \in p$, $T \models \forall \underline{x}(\varphi \to \psi)$.[1] We say that the set $p(\underline{x})$ is supported in T if there exists a formula which supports it.

Lemma 3.4. *Fix $d \geqslant 2$, $n \geqslant 1$. There is a set $p_{d,n}(x_1, \dots, x_d)$ of formulae (in the language of rings) such that a tuple $(a_1, \dots, a_d)$ in a field L realises $p_{d,n}$ if and only if the arboreal representation $\phi_f \colon \operatorname{Gal}_L \to \operatorname{Aut} \mathrm{T}_\infty(d)$ associated to $f = X^d + a_1 X^{d-1} + \cdots + a_d$ has image of index at most n in* $\operatorname{Aut} \mathrm{T}_\infty(d)$.

Proof. For every $k \geqslant 1$, let us write $\mathrm{T}_k(d)$ for the part of $\mathrm{T}_\infty(d)$ up to level k. The image of ϕ_f has index at most n if and only if the image of the finite stages $\operatorname{Gal}_L \to \operatorname{Aut} \mathrm{T}_k(d)$ has index at most n, for all k. Equivalently, the splitting field of $f^{\circ k}$ has degree at least $|\operatorname{Aut} \mathrm{T}_k(d)|/n$. Since the coefficients of $f^{\circ k}$ are polynomials

[1] In [Mar02, Definition 4.2.1] the terminology for this property is that $\varphi(\underline{x})$ *isolates* $p(\underline{x})$, but there it is required throughout that $T \cup p(\underline{x})$ be consistent (which is true in all interesting situations).

in the a_i, this property is expressed by a first-order formula in the language of rings. Collecting these formulae for all k yields the desired $p_{d,n}$. □

Let us now fix a countable field K of characteristic zero, and work in the language $\mathcal{L}$ which is the language of rings together with constant symbols for each element of K. Consider the $\mathcal{L}$-theory T which consists of the theory of Hilbertian pseudo-algebraically closed fields (see [FJ08, Chapter 27]) and the diagram of K (see [Hod97, Section 1.4]). In this way, models of T correspond to field extensions L/K such that L is Hilbertian and pseudo-algebraically closed. For pseudo-algebraically closed fields, being Hilbertian is equivalent to the absolute Galois group satisfying a certain group-theoretic condition, called *ω-freeness*, see [Jar11, Theorem 5.10.3].

Proving Theorem 3.1 now means showing that there exists a model L of T in which none of the sets $p_{d,n}$ from Lemma 3.4 is realised by any tuple. (Let us ignore the additional condition that L/K be algebraic if K is Hilbertian for the moment.) We will apply the following standard tool from model theory, which applies to any consistent theory T in a countable language $\mathcal{L}$, thus in particular in our setting:

Theorem 3.5 (Omitting types, [Hod97, Theorem 6.2.1]; see also [Mar02, Theorem 4.2.4])**.** *For each $i \in \mathbb{N}$, let p_i be a set of $\mathcal{L}$-formulae in free variables $x_1, \dots, x_{n_i}$, such that no p_i is supported in T. Then there exists a model of T realising none of the p_i, i.e. the p_i are* omitted*.*

We thus wish to show that none of the sets $p_{d,n}$ from Lemma 3.4 are supported in T. We first isolate two important properties of T from [FJ08, Theorem 27.2.3], rephrasing the model-theoretic terminology there in more elementary terms.

Lemma 3.6. *Let $\varphi(\underline{x})$ be an $\mathcal{L}$-formula. Then φ is equivalent modulo T to a formula of the form $\exists \underline{y}(\psi(\underline{x}, \underline{y}))$, where ψ is a positive boolean combination of polynomial equalities and formulae of the form $\forall z(z^m + t_1 z^{m-1} + \cdots + t_m \neq 0)$, where the t_i are polynomial expressions in $\underline{x}, \underline{y}$ with coefficients from K.*

Proof. This is a relatively straightforward translation of the model completeness part of [FJ08, Theorem 27.2.3]. Let us explain this in detail.

The theorem cited works in an extended language $\mathcal{L}'$ for fields, containing not only symbols $+, -$ and $\cdot$, but also an additional n-ary predicate R_n for every $n \geqslant 2$, and states in particular that the theory T' consisting of T and the additional axioms

$$\forall x_1, \dots, x_n \big(R_n(x_1, \dots, x_n) \leftrightarrow \exists z(z^n + x_1 z^{n-1} + \cdots + x_n = 0) \big)$$

for all n (specifying the intended interpretation for R_n) is *model complete*.

By [Hod97, Theorem 7.3.1], this implies that the formula $\neg\varphi(\underline{x})$ is equivalent modulo T' to a universal $\mathcal{L}'$-formula $\theta_0(\underline{x})$, i.e. a formula built by universal quantification, $\wedge$ and $\vee$ from atomic formulae and their negations. Here atomic formulae are equations between terms (i.e. polynomial expressions in the variables and constants), as well as formulae of the form $R_n(t_1, \dots, t_n)$ with terms t_i.

Taking negations, $\varphi(\underline{x})$ is equivalent modulo T' to $\neg\theta_0(\underline{x})$, which in turn is equivalent to an existential formula $\theta_1(\underline{x})$, i.e. one built from atomic formulae and their negations using existential quantification, $\wedge$ and $\vee$. We may eliminate all negated equalities $t_1 \neq t_2$ between terms by rewriting them as $\exists z(zt_1 = zt_2 + 1)$. Now replace all occurrences of $\neg R_n(t_1, \dots, t_n)$ in ψ_1 by $\forall z(z^n + x_1 z^{n-1} + \cdots + x_n \neq 0)$ and all occurrences of $R_n(t_1, \dots, t_n)$ by $\exists z(z^n + x_1 z^{n-1} + \cdots + x_n = 0)$ to obtain an $\mathcal{L}$-formula $\theta_2(\underline{x})$. Moving all existential quantifiers to the front of the formula, θ_2 is equivalent to an $\mathcal{L}$-formula $\theta_3 = \exists \underline{y}(\psi(\underline{x}, \underline{y}))$ with ψ of the required shape.

We have seen that φ is equivalent to θ_3 modulo T'. Since T' is a so-called definitional expansion of T, i.e. only adds axioms specifying the interpretation of additional relation symbols, φ and θ_3 are actually already equivalent modulo T, since any model of T in which they are not equivalent could be expanded to a model of T' [Hod97, Theorem 2.6.4(a)]. □

Lemma 3.7. *For every extension L/K there exists a regular extension F/L with $F \models T$.*

Proof. This is a translation of another part of [FJ08, Theorem 27.2.3], as we now explain. By the statement about model companions given there, L embeds into a model F of T such that the embedding $L \hookrightarrow F$ not only preserves addition and multiplication, but also embeds L as a relatively algebraically closed subfield of F; see [FJ08, top of p. 660]. Identifying the embedding with an inclusion, this means that F/L is regular since the characteristic is zero. □

We now prove the key technical statements for the proof of Theorem 3.1.

Lemma 3.8. *For any fixed $d \geqslant 2$ and n, the set $p_{d,n}$ from Lemma 3.4 is not supported in T.*

Proof. Let $\varphi(\underline{x})$ be an arbitrary $\mathcal{L}$-formula such that $T \cup \{\exists \underline{x}(\varphi(\underline{x}))\}$ is consistent; we show that φ does not support $p_{d,n}$ in T. We may assume that $\varphi = \exists \underline{y}(\psi(\underline{x}, \underline{y}))$ as in Lemma 3.6. Since $T \cup \{\exists \underline{x}\varphi\}$ is consistent, there is a Hilbertian pseudo-algebraically closed field L/K with elements $\underline{x}, \underline{y}$ such that $L \models \psi(\underline{x}, \underline{y})$. We can choose an algebraic extension L'/L, with $\mathrm{Gal}_{L'}$ finitely generated, such that $L' \models \psi(\underline{x}, \underline{y})$, since we only need to ensure that the finitely many polynomials $Z^m + t_1 Z^{m-1} + \cdots + t_m$ mentioned in ψ which have no root in L do not have any root in L'. Then the arboreal representation $\phi_f \colon \mathrm{Gal}_{L'} \to \mathrm{Aut}\, \mathrm{T}_\infty(d)$ associated to $f = X^d + x_1 X^{d-1} + \cdots + x_m$ has image of infinite index, since $\mathrm{Aut}\, \mathrm{T}_\infty(d)$ is not finitely generated because of the surjective homomorphism $\mathrm{Aut}\, \mathrm{T}_\infty(d) \to \prod_{k=1}^{\infty} \mathbb{Z}/2\mathbb{Z}$.

By Lemma 3.7, there exists a regular extension F/L' with $F \models T$. Since the representation $\mathrm{Gal}_F \to \mathrm{Aut}\, \mathrm{T}_\infty(d)$ associated to f factors through $\mathrm{Gal}_{L'}$, its image has infinite index, so the tuple $\underline{x}$ does not realise $p_{d,n}$ in F. As $F \models \varphi(\underline{x})$ by construction, φ does not support $p_{d,n}$. □

Lemma 3.9. *Assume in addition that the fixed countable field K is Hilbertian. Let $p(x)$ be the set of formulae in one variable which assert that x satisfies no nontrivial polynomial relation over K. Then p is not supported in T.*

Proof. Suppose $\varphi(x)$ is a formula supporting p. In particular, there exists an extension L/K with $L \models T \cup \{\exists x \varphi(x)\}$. By the downward Löwenheim-Skolem theorem, we may assume that L is countable. By [FJ08, Proposition 23.2.4], L is elementarily equivalent over K to an ultraproduct $L' = \prod_{n=1}^{\infty} L_n/\mathcal{D}$, where $\mathcal{D}$ is an ultrafilter on $\mathbb{N}$ and each L_n is an algebraic extension of K which is PAC and satisfies $\mathrm{Gal}_{L_n} \cong \mathrm{Gal}_L$, so in particular every L_n is ω-free. Since $L' \equiv L \models \exists x \varphi(x)$, by Łoś's theorem on ultraproducts [FJ08, Corollary 7.7.2] there exists an n such that $L_n \models \exists x \varphi(x)$. Now L_n contains no element realising p, but has an element satisfying φ, so we deduce that φ does not support p. □

Proof of Theorem 3.1. The theorem follows immediately from Theorem 3.5 with Lemma 3.8, by simultaneously omitting the sets $p_{n,d}$ for all n and d, and additionally omitting the set p from Lemma 3.9 if K is Hilbertian. □

Acknowledgments

We thank Padmavathi Srinivasan for useful comments that improved the exposition. We thank the anonymous referees for many helpful suggestions.

References

[BS08] Lior Bary-Soroker, *On the characterization of Hilbertian fields*, Int. Math. Res. Not. IMRN, posted on 2008, Art. ID rnn 089, 10, DOI 10.1093/imrn/rnn089. MR2439555 ↑3337

[BJ19] Robert L. Benedetto and Jamie Juul, *Odoni's conjecture for number fields*, Bull. Lond. Math. Soc. **51** (2019), no. 2, 237–250, DOI 10.1112/blms.12225. MR3937585 ↑3336

[Cox12] David A. Cox, *Galois theory*, 2nd ed., Pure and Applied Mathematics (Hoboken), John Wiley & Sons, Inc., Hoboken, NJ, 2012, DOI 10.1002/9781118218457. MR2919975 ↑3339

[FJ08] Michael D. Fried and Moshe Jarden, *Field arithmetic*, 3rd ed., Ergebnisse der Mathematik und ihrer Grenzgebiete. 3. Folge. A Series of Modern Surveys in Mathematics [Results in Mathematics and Related Areas. 3rd Series. A Series of Modern Surveys in Mathematics], vol. 11, Springer-Verlag, Berlin, 2008. Revised by Jarden. MR2445111 ↑3337, 3340, 3341, 3342

[Hod97] Wilfrid Hodges, *A shorter model theory*, Cambridge University Press, Cambridge, 1997. MR1462612 ↑3340, 3341, 3342

[Jar11] Moshe Jarden, *Algebraic patching*, Springer Monographs in Mathematics, Springer, Heidelberg, 2011, DOI 10.1007/978-3-642-15128-6. MR2768285 ↑3341

[Jon13] Rafe Jones, *Galois representations from pre-image trees: an arboreal survey* (English, with English and French summaries), Actes de la Conférence "Théorie des Nombres et Applications", Publ. Math. Besançon Algèbre Théorie Nr., vol. 2013, Presses Univ. Franche-Comté, Besançon, 2013, pp. 107–136. MR3220023 ↑3336

[Kad20] Borys Kadets, *Large arboreal Galois representations*, J. Number Theory **210** (2020), 416–430, DOI 10.1016/j.jnt.2019.09.021. MR4057534 ↑3336

[Mar02] David Marker, *Model theory*, Graduate Texts in Mathematics, vol. 217, Springer-Verlag, New York, 2002. An introduction. MR1924282 ↑3340, 3341

[NSW08] Jürgen Neukirch, Alexander Schmidt, and Kay Wingberg, *Cohomology of number fields*, 2nd ed., Grundlehren der mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences], vol. 323, Springer-Verlag, Berlin, 2008, DOI 10.1007/978-3-540-37889-1. MR2392026 ↑3340

[Odo85] R. W. K. Odoni, *The Galois theory of iterates and composites of polynomials*, Proc. London Math. Soc. (3) **51** (1985), no. 3, 385–414, DOI 10.1112/plms/s3-51.3.385. MR805714 ↑3336

[Spe18] Joel Specter, *Polynomials with surjective arboreal Galois representation exist in every degree*, Preprint, `arXiv:1803.00434v2`, 2018. ↑3336

Technische Universität Dresden, Fakultät Mathematik, Institut für Algebra, 01062 Dresden, Germany

Email address: `philip.dittmann@tu-dresden.de`

Mathematical Sciences Research Institute, 17 Gauss Way, Berkeley, California 94720-5070

Email address: `kadets.math@gmail.com`

URL: `http://bkadets.github.io`