

TWO EXAMPLES CONCERNING EXISTENTIAL UNDECIDABILITY IN FIELDS

PHILIP DITTMANN 

Abstract. We construct an existentially undecidable complete discretely valued field of mixed characteristic with existentially decidable residue field and decidable algebraic part, answering a question by Anscombe–Fehm in a strong way. Along the way, we construct an existentially decidable field of positive characteristic with an existentially undecidable finite extension, modifying a construction due to Kesavan Thanagopal.

§1. Introduction. Given a field K , one may ask whether there is an algorithm to decide which multivariable polynomials with coefficients in the prime field have zeroes in K —in short, whether K is *existentially decidable*. Motivated by Hilbert’s Tenth Problem, much research has been done on this question in particular in global fields and function fields (see for instance the monograph [24]). On the other hand, this question is also of interest in henselian valued fields, where it is the first step of a good model-theoretic understanding of the full first-order theory. See in particular [1, 3, 4, 17] for recent related work.

The chief aim of this note is to prove the following theorem, giving an interesting example of existential undecidability.

THEOREM 1.1. *Let p be a prime number. There exists a complete discretely valued field (E, v) of characteristic 0 and residue characteristic p such that the residue field E_v is existentially decidable, the set of polynomials in $\mathbb{Q}[X]$ with a zero in E is decidable, but the field E is existentially undecidable.*

This answers a question by Anscombe–Fehm in a strong way (see Remark 5.3 for a discussion). The existential theories of complete discretely valued fields of mixed characteristic (or more generally finitely ramified henselian valued fields) are further explored in [2].

In order to prove Theorem 1.1, we use an example of a different phenomenon in existential decidability, which seems interesting in its own right.

THEOREM 1.2. *Let p be a prime number. There exists an existentially decidable field of characteristic p with an existentially undecidable quadratic extension.*

A variant of this problem was first considered in Kesavan Thanagopal’s thesis [26], where an example was given in characteristic 0. We modify the construction

Received December 2, 2022.

2020 *Mathematics Subject Classification.* Primary 03C60, 12L05.

Key words and phrases. undecidable, existential theory, complete discretely valued field.

© The Author(s), 2023. Published by Cambridge University Press on behalf of The Association for Symbolic Logic. This is an Open Access article, distributed under the terms of the Creative Commons Attribution licence (<https://creativecommons.org/licenses/by/4.0/>), which permits unrestricted re-use, distribution, and reproduction in any medium, provided the original work is properly cited.

0022-4812/00/0000-0000

DOI:10.1017/jsl.2023.87



given there, based on Ershov’s theory of fields with a strong local–global principle presented in [10].

§2. A useful family of varieties. Let p be a prime number, and $q > 1$ a power of p . In this section we prove the following proposition, which will be useful later.

PROPOSITION 2.1. *Let $n \geq 1$. There exists a smooth projective geometrically integral variety V/\mathbb{F}_q such that for any $m \geq 1$ we have:*

- if $m \mid n$, then $V(\mathbb{F}_{q^m}) = \emptyset$;
- if $\text{lcm}(m, n) \geq 4n$, then $V(\mathbb{F}_{q^m}) \neq \emptyset$.

For definiteness, in this article we take a *variety* (over a specified base field) to be a separated scheme of finite type, although almost all varieties occurring will be quasi-projective and geometrically integral.

The proof of Proposition 2.1 relies on the following lemma.

LEMMA 2.2. *There exists a smooth projective geometrically integral curve C/\mathbb{F}_q such that $C(\mathbb{F}_q) = \emptyset$, but $C(k) \neq \emptyset$ for any field extension k/\mathbb{F}_q with $4 \leq [k : \mathbb{F}_q] < \infty$.*

PROOF. Let g be the smallest integer bigger than $\frac{q-3}{2}$ with $g \equiv -1 \pmod{p}$, so $\frac{q-3}{2} < g \leq \frac{q-3}{2} + p$. By [6, Lemma 2.2], there exists a hyperelliptic curve C/\mathbb{F}_q of genus g with $C(\mathbb{F}_q) = \emptyset$.

The number of \mathbb{F}_{q^m} -rational points of C is at least $q^m + 1 - 2g\sqrt{q^m} \geq q^m + 1 - (q - 3 + 2p)q^{m/2}$ by the Hasse–Weil bound. This is positive if $q - 3 + 2p \leq q^{m/2}$, which is the case if $m \geq 4$. –

REMARK 2.3. The situation would be neater if we could strengthen the lemma to say that $C(k) \neq \mathbb{F}_q$ for any proper finite extension k/\mathbb{F}_q , in which case we could also strengthen the proposition to say that $V(\mathbb{F}_{q^m}) = \emptyset$ if and only if $m \mid n$.

In order to improve the lemma in this way, one would need to improve the construction of Becker and Glass, finding a bound for the genus which is better than linear in q . This works at least for specific values for q in any characteristic $p > 3$ (see [27]).

PROOF OF THE PROPOSITION. Let C/\mathbb{F}_{q^n} be a curve as in the lemma, so that $C(\mathbb{F}_{q^n}) = \emptyset$, but $C(\mathbb{F}_{q^{nl}}) \neq \emptyset$ for $l \geq 4$. Let V/\mathbb{F}_q be the Weil restriction of C . It is a smooth projective geometrically integral variety over \mathbb{F}_q because C/\mathbb{F}_{q^n} is so: Indeed, by [8, Proposition A.5.9] V is smooth and geometrically connected (hence geometrically integral), and by [8, Proposition A.5.8] and [7, Proposition 7.6/5] V is quasi-projective and proper, hence projective.

By the defining property, for any m , the set $V(\mathbb{F}_{q^m})$ is in bijection to $C(\mathbb{F}_{q^m} \otimes_{\mathbb{F}_q} \mathbb{F}_{q^n})$. For $m \mid n$ we have $C(\mathbb{F}_{q^m} \otimes_{\mathbb{F}_q} \mathbb{F}_{q^n}) = C(\mathbb{F}_{q^n}^m) = C(\mathbb{F}_{q^n})^m = \emptyset$.

Now let $m \geq 1$ with $\text{lcm}(n, m) \geq 4n$. We have $\mathbb{F}_{q^m} \otimes_{\mathbb{F}_q} \mathbb{F}_{q^n} = \mathbb{F}_{q^{\text{lcm}(n,m)}}^{nm/\text{lcm}(n,m)}$. Then $C(\mathbb{F}_{q^m} \otimes_{\mathbb{F}_q} \mathbb{F}_{q^n}) = C(\mathbb{F}_{q^{\text{lcm}(n,m)}}^{nm/\text{lcm}(n,m)}) \neq \emptyset$ since $C(\mathbb{F}_{q^{\text{lcm}(n,m)}}) \neq \emptyset$ by the defining property of C . This proves the desired property of V . –

REMARK 2.4. It will be important for us later that for given q and m , a variety V as in the proposition can be effectively determined. This follows from the proofs, since both the construction of [6, Lemma 2.2] and Weil restriction as in the proof of

Proposition 2.1 are effective. On the other hand, this is also clear without going back into the proofs, merely using the existence statement: simply enumerate candidate varieties, test for points over small fields, and use the Hasse–Weil bound.

§3. The construction. Fix again a prime p . We find an extension field \mathbb{K} of $\mathbb{F}_p(t)$ satisfying a strong local–global principle, after Ershov.

We first fix some terminology. A *discrete valuation* is a Krull valuation whose value group is isomorphic to \mathbb{Z} , i.e., is given by a discrete valuation in the usual sense of commutative algebra. We do not distinguish between valuations and their valuation rings, so in particular we identify equivalent valuations. Given a valuation v on a field K , we write Kv for the residue field and K_v^h for the henselisation. A valuation of $\mathbb{F}_p(t)$ is said to be *above* $\mathbb{F}_p[t]$ if its valuation ring contains $\mathbb{F}_p[t]$, i.e., if it is not the degree valuation of $\mathbb{F}_p(t)$.

PROPOSITION 3.1. *There exists a countable regular field extension $\mathbb{K}/\mathbb{F}_p(t)$ together with a family V of discrete valuations such that the following hold:*

- (1) *For every $v \in V$, the restriction of v to $\mathbb{F}_p(t)$ is again a discrete valuation, which lies above $\mathbb{F}_p[t]$. Further, the extension $(\mathbb{K}, v)/(\mathbb{F}_p(t), v|_{\mathbb{F}_p(t)})$ is immediate, i.e., the residue fields $\mathbb{K}v$ and $\mathbb{F}_p(t)v|_{\mathbb{F}_p(t)}$ agree and a uniformiser for $v|_{\mathbb{F}_p(t)}$ remains a uniformiser for v .*
- (2) *For every discrete valuation v_0 of $\mathbb{F}_p(t)$ above $\mathbb{F}_p[t]$ there is precisely one $v \in V$ prolonging v_0 .*
- (3) *Any $x \in \mathbb{K}$ is in the valuation ring of all but finitely many $v \in V$.*
- (4) *If a geometrically integral variety X/\mathbb{K} has a smooth \mathbb{K}_v^h -point for every $v \in V$, then it has a \mathbb{K} -point.*

PROOF. This is a consequence of [10, Theorem 3.6.3], as we now explain.

Let V_0 be the family of discrete valuation rings of $\mathbb{F}_p(t)$ above $\mathbb{F}_p[t]$. Then any two distinct members of V_0 are independent; V_0 is a near Boolean family in Ershov’s sense since $\mathbb{F}_p[t]$ is an “NB-ring” [10, Remark 2.5.1] and the valuation rings of the valuations in V_0 are precisely the localisations of $\mathbb{F}_p[t]$ at its maximal ideals [10, Proposition 2.5.3]; and the residue fields of V_0 are “regularly closed at infinity” [10, Section 3.4, p. 172], as they are finite fields with only finitely many of cardinality lower than a given bound, and so the desired property follows from the Lang–Weil bounds [21, Theorem 7.7.1 (iv)].

Thus by [10, Theorem 3.6.3], there exists a countable regular extension $\mathbb{K}/\mathbb{F}_p(t)$ with a family of valuation rings V such that every valuation $v \in V$ lies over a valuation $v_0 \in V_0$, this induces a bijection between V and V_0 , and the extension of valued fields $(\mathbb{K}, v)/(\mathbb{F}_p(t), v_0)$ is immediate. In particular every $v \in V$ is discrete, and conditions (1) and (2) are satisfied.

The bijection $V \rightarrow V_0$ is furthermore a homeomorphism with respect to the Zariski topologies on V and V_0 (see [10, Section 2.2]), which means that for all $x \in \mathbb{K}$ the (“Zariski closed”) set $C_x := \{v \in V : v(x) < 0\}$ is either finite or all of V since the analogous statement holds in $\mathbb{F}_p(t)$. However, we cannot have $C_x = V$, since otherwise for a suitable element $b \in \mathbb{F}_p(t)^\times$ (a high power of a uniformiser for some valuation in V_0) the set C_{xb} would be infinite but strictly contained in V ,

violating the homeomorphism property. Therefore the set C_x is finite for all $x \in \mathbb{K}$. This gives condition (3).

In addition, the family V satisfies Ershov's "arithmetic local–global principle" LG_A , and therefore also the "geometric local–global principle" LG_G [10, Proposition 3.2.5], which gives our condition (4) for geometrically integral affine varieties X/\mathbb{K} . Now take an arbitrary geometrically integral variety X/\mathbb{K} , and let X_0/\mathbb{K} be an affine dense open subvariety. If X has a smooth \mathbb{K}_v^h -point for every $v \in V$, then the same holds for X_0 : This is the ampleness of the henselian field \mathbb{K}_v^h (see [10, Corollary 3.1.6] and the surrounding discussion). Hence we have $\emptyset \neq X_0(\mathbb{K}) \subseteq X(\mathbb{K})$ by the affine case, proving (4) in full generality. \dashv

REMARKS 3.2. (1) Fields \mathbb{K} as in the proposition are weak analogues of the "surprising extensions of \mathbb{Q} " considered in [9] (also variously translated as "wonderful" or "amazing" extensions). Note, however, that there also the place at infinity, i.e., the real place of \mathbb{Q} , is included.

(2) Since it plays no role in the sequel, we have not imposed the condition which is called maximality in [9], i.e., that for every proper separable algebraic extension L/\mathbb{K} , some valuation in V has no immediate extension to L . This condition can, however, always be added (see [10, Proposition 4.4.3, Remark 4.4.3, and Proposition 4.4.4]).

(3) Any non-trivial valuation v of \mathbb{K} not in V always has separably closed henselisation, and hence poses no obstruction to the existence of rational points on varieties. This follows from [10, Corollary 3.5.4] (there stated for Boolean families of valuations, but the same proof works for near-Boolean families with residue fields regularly closed at infinity). In particular, the family V simply consists of all discrete valuations of \mathbb{K} .

(4) Instead of starting with the discrete valuations of $\mathbb{F}_p(t)$ above $\mathbb{F}_p[t]$, we could have worked with the coordinate ring of any irreducible smooth affine curve over \mathbb{F}_p and its function field.

We henceforth fix a field \mathbb{K} as in the proposition.

LEMMA 3.3. *Let L/\mathbb{K} be a finite separable extension. Let X/\mathbb{F}_p be a smooth projective geometrically integral variety. Then $X(L) \neq \emptyset$ if and only if for every $v \in V$ and every prolongation w of v to L , X has a point over the residue field Lw .*

PROOF. Let W be the family of prolongations of valuations in V to L . By [10, Proposition 3.4.1] (a Weil restriction argument), the same local–global principle as for V holds for W . In particular, $X(L) \neq \emptyset$ if and only if X has a point over all henselisations L_w^h , $w \in W$.

Let $w \in W$. If X has a point over the henselisation L_w^h , then it has a point over the residue field Lw , using that X is projective (given homogenous coordinates of an L_w^h -point of X , clear denominators and reduce).¹ Conversely, if X has a point over the residue field Lw , then it has a point over the henselisation L_w^h since there exists an embedding $Lw \hookrightarrow L_w^h$ (apply Hensel's Lemma to the minimal polynomial

¹Using the valuative criterion of properness, it would suffice to assume that X is proper instead of projective.

of a primitive element of Lw over \mathbb{F}_p). Together with the local–global principle, this proves the statement. \dashv

REMARK 3.4. None of the hypotheses of smoothness, projectivity, and geometric integrality can be omitted in Lemma 3.3. This explains why these hypotheses, in particular smoothness and geometric integrality, recur throughout this article. We sketch a few examples to demonstrate this.

For the variety X which is the affine line \mathbb{A}^1 punctured at each of its \mathbb{F}_p -points—equivalently, X is the plane curve described by the equation $yx(x-1)\cdots(x-(p-1))=1$ —we have $X(\mathbb{K}) \neq \emptyset$, but for the residue field \mathbb{F}_p of the unique valuation $v \in V$ above the t -adic valuation of $\mathbb{F}_p(t)$ we have $X(\mathbb{F}_p) = \emptyset$ by construction. Thus one direction of the lemma fails for $L = \mathbb{K}$ with the non-projective smooth geometrically integral variety X .

In the other direction, both smoothness and geometric integrality are needed in general for Ershov’s local–global principle to apply. Consider a finite extension $L_0/\mathbb{F}_p(t)$ which is the function field of a smooth projective geometrically integral \mathbb{F}_p -curve without rational points and set $L = L_0\mathbb{K}$. Then L is regular over \mathbb{F}_p , but carries no valuation with residue field \mathbb{F}_p . Let \mathbb{F}_q be a finite field which occurs as the residue field of some discrete valuation on L . Let C/\mathbb{F}_q be a smooth projective geometrically integral curve without \mathbb{F}_q -points. Then C has no L -point, but it has an Lw -point for all but finitely many discrete valuations w on L by the Hasse–Weil bound. For a suitable list $\mathbb{F}^{(1)}, \dots, \mathbb{F}^{(n)}$ of proper finite extensions of \mathbb{F}_p , the \mathbb{F}_p -variety $C' := C \amalg \text{Spec}(\mathbb{F}^{(1)}) \amalg \dots \amalg \text{Spec}(\mathbb{F}^{(n)})$ has an Lv -point for all discrete valuations v on L , but no L -point (since none of its connected components has an L -point by construction). Thus C' is a reducible smooth projective \mathbb{F}_p -variety for which the statement of the lemma does not hold.

To find a projective non-smooth geometrically integral example, one can again start with L and C as above, and construct a curve C'' from C not by adding finitely many points, but by a pinching construction (see for instance [23, Section 1.3] for an explanation in principle, but only for curves over algebraically closed fields, and [11] for the generality needed here): thus C will be the normalisation of C'' , and by wisely choosing the pinching data, one forces C'' to have rational points over all residue fields of L , but none over L itself. We omit the details.

We next wish to find finite extensions L/\mathbb{K} such that the discrete valuations of L have prescribed residue fields. This is achieved by the following lemmas.

LEMMA 3.5. *Let S_1, S_2 be two disjoint finite sets of prime numbers greater than 4. There exists a cyclic extension $L_0/\mathbb{F}_p(t)$ of degree 4 such that:*

- (1) *For every $l \in S_1$, there exists a discrete valuation of L_0 above $\mathbb{F}_p[t]$ with residue field \mathbb{F}_{p^l} .*
- (2) *For every $l \in S_2$ and every \mathbb{F}_{p^m} occurring as the residue field of a valuation of L_0 , we have $\text{lcm}(l, m) \geq 4l$.*

PROOF. Let $L_0/\mathbb{F}_p(t)$ be a cyclic extension of degree 4 in which each of the (non-zero) finitely many discrete valuations of $\mathbb{F}_p(t)$ with residue field \mathbb{F}_{p^l} , $l \in S_1$, is completely split, and each of the finitely many discrete valuations of $\mathbb{F}_p(t)$ with residue field \mathbb{F}_{p^n} , $S_1 \not\ni n \leq 4 \max(S_2)$, is inert. The existence of such an extension

follows from the Grunwald–Wang Theorem [19, Theorem 9.2.8], which allows the construction of abelian extensions of $\mathbb{F}_p(t)$ in which the decomposition behaviour of finitely many places is prescribed. The field L_0 satisfies the required properties. \dashv

LEMMA 3.6. *Let S_1, S_2 be two disjoint finite sets of prime numbers greater than 4. Then there exists a cyclic extension L/\mathbb{K} of degree 4 such that conditions (1) and (2) from Lemma 3.5 hold for L (in place of L_0).*

PROOF. Take $L_0/\mathbb{F}_p(t)$ as in Lemma 3.5, and let $L = \mathbb{K}L_0$ (free compositum, equivalently the tensor product $\mathbb{K} \otimes_{\mathbb{F}_p(t)} L_0$). For any discrete valuation v of L , the restriction w to L_0 is also a discrete valuation and we have the inclusion of residue fields $L_0w \subseteq Lv$. Thus condition (2) transfers from L_0 to L : Indeed, if $m_0 = [L_0w : \mathbb{F}_p]$ and $m = [Lv : \mathbb{F}_p]$, we have $m_0 \mid m$ and thus $4l \leq \text{lcm}(l, m_0) \mid \text{lcm}(l, m)$.

On the other hand, for every discrete valuation w of L_0 above $\mathbb{F}_p[t]$, the restriction v_0 to $\mathbb{F}_p(t)$ is again discrete, and the defining property of \mathbb{K} affords a discrete valuation v on \mathbb{K} such that $(\mathbb{K}, v)/(\mathbb{F}_p(t), v_0)$ is immediate. In particular, \mathbb{K} embeds into the completion $\widehat{\mathbb{F}_p(t)}_{v_0}$ over $\mathbb{F}_p(t)$. Thus L embeds into the completion $\widehat{L_0w}$ over $\mathbb{F}_p(t)$ since both \mathbb{K} and L_0 have such an embedding and are linearly disjoint over $\mathbb{F}_p(t)$. Therefore L carries a discrete valuation above $\mathbb{F}_p[t]$ with residue field L_0w . Thus condition (1) transfers from L_0 to L . \dashv

We can now show that \aleph_0 -saturated elementary extensions \mathbb{K}^* of \mathbb{K} have existentially undecidable finite extensions.

Recall (see for instance [25, Definition 1.6.8]) that a set of natural numbers A is *many-one reducible* to a set of natural numbers B if there exists a computable function $f : \mathbb{N} \rightarrow \mathbb{N}$ such that for any $x \in \mathbb{N}$ we have $f(x) \in B$ if and only if $x \in A$. This is a formalisation of the notion that membership in A is no harder to decide than membership in B . (A different formalisation is given by Turing reducibility, which is implied by many-one reducibility.)

By fixing a standard Gödel coding, we identify formulae of a given finite first-order language with natural numbers. In particular, computability-theoretic terms such as decidability and many-one reducibility make sense for sets of formulae. We generally work in the language of rings $\mathcal{L}_{\text{ring}} = \{+, -, \cdot, 0, 1\}$.

THEOREM 3.7. *Let S be a set of prime numbers. Then any \aleph_0 -saturated elementary extension \mathbb{K}^* of \mathbb{K} has a cyclic extension L/\mathbb{K}^* of degree 4 such that S is many-one reducible to the existential theory of L . In particular, there exist cyclic extensions L/\mathbb{K}^* of degree 4 with undecidable existential theory.*

PROOF. For every prime number l , let V_l/\mathbb{F}_p be a variety as in Proposition 2.1 (with $q = p, n = l$). We claim that we can choose L such that for all primes $l > 4$, we have $V_l(L) \neq \emptyset$ if and only if $l \in S$. Since V_l can be computed from l by Remark 2.4, and $V_l(L) \neq \emptyset$ is straightforwardly translated into an existential sentence, this L solves the problem.

It thus remains to find L satisfying the claim. Recasting the search for L as the search for the coefficients of an irreducible polynomial of degree 4 over \mathbb{K}^* with a root generating L , saturation reduces us to finding, for every finite set of primes S_1 disjoint from S and finite $S_2 \subseteq S$, an extension L/\mathbb{K} of degree 4 with $V_l(L) = \emptyset$ for $4 < l \in S_1$ and $V_l(L) \neq \emptyset$ for $4 < l \in S_2$. This problem is solved by Lemma 3.6:

Indeed, the field L produced there satisfies the condition by Lemma 3.3 and the construction of the V_j .

The “in particular” holds because if S is an undecidable set, then the existential theory of L cannot be decidable. \dashv

REMARK 3.8. The passage to an elementary extension of \mathbb{K} is due to the need to realise a certain type, given by the requirements for the coefficient tuple of an irreducible polynomial defining L . Given that this is only one type, a well-chosen countable elementary extension \mathbb{K}^* of \mathbb{K} (depending on S) would be sufficient in place of an \aleph_0 -saturated one.

§4. Existential decidability. Let again p be a prime number, $\mathbb{K}/\mathbb{F}_p(t)$ as in the last section. In this section we prove that the existential theory of \mathbb{K} is decidable.

LEMMA 4.1. *Let X/\mathbb{F}_p be a geometrically integral smooth affine variety. Then $X(\mathbb{K}) \neq \emptyset$ if and only if $X(\mathbb{F}_p((s))) \neq \emptyset$.*

PROOF. First observe that since \mathbb{K} carries a discrete valuation with residue field \mathbb{F}_p (for instance the prolongation in V of the t -adic valuation of $\mathbb{F}_p(t)$), \mathbb{K} embeds into $\mathbb{F}_p((s))$, and therefore the existence of a \mathbb{K} -rational point of X implies the existence of an $\mathbb{F}_p((s))$ -rational point.

Suppose conversely that X has an $\mathbb{F}_p((s))$ -rational point. Then it has a point over the henselisation $\mathbb{F}_p(s)_s^h$ at the s -adic valuation, since the fields $\mathbb{F}_p((s))$ and $\mathbb{F}_p(s)_s^h$ have the same existential theory by [3, Corollary 7.2] (or by [18, Theorem 5.9]). Therefore X has a rational point over the henselisation \mathbb{K}_v^h for every v , since every such henselisation embeds $\mathbb{F}_p(s)_s^h$ (sending s to a uniformiser). Now $X(\mathbb{K}) \neq \emptyset$ follows from the local–global principle. \dashv

The following general lemma reduces the existential theory of a field to information about which smooth affine varieties have rational points. This may well have appeared elsewhere in the literature, but I am unaware of a reference. As usual, given a field F , the language $\mathcal{L}_{\text{ring}}(F)$ is simply the expansion of $\mathcal{L}_{\text{ring}}$ by constants for the elements of F . In particular, every extension E/F is naturally an $\mathcal{L}_{\text{ring}}(F)$ -structure.

LEMMA 4.2. *Let F be a field, and $E_1/F, E_2/F$ two regular extensions. Assume that for every geometrically integral smooth affine F -variety X we have $X(E_1) \neq \emptyset$ if and only if $X(E_2) \neq \emptyset$. Then the existential $\mathcal{L}_{\text{ring}}(F)$ -theories of E_1 and E_2 agree.*

PROOF. By standard reductions (disjunctive normal form, elimination of inequalities) it suffices to show that for any $f_1, \dots, f_k \in F[X_1, \dots, X_n]$, the f_i have a common zero in E_1 if and only if they have a common zero in E_2 . In other words, we must show that for every affine F -variety X we have $X(E_1) \neq \emptyset$ if and only if $X(E_2) \neq \emptyset$.

By passing to the reduction of X is necessary, and using that for every reduced variety the regular locus is open and not empty [12, Corollary 12.52(2)], we can write X as a union of finitely many regular integral affine locally closed subvarieties. In other words, it suffices to consider integral regular affine X .

If X is not geometrically integral, then $X(E_1) = \emptyset = X(E_2)$: Indeed, the base-changed varieties X_{E_1}/E_1 and X_{E_2}/E_2 are regular [13, Proposition 6.7.4], integral

[12, Corollary 5.56(3)], but not geometrically integral, and therefore they have no rational points (see for instance [20, Lemma 10.1]).

Thus let us assume that X is geometrically integral. Then the smooth locus $X_{\text{sm}} \subseteq X$ is dense open [12, Theorem 6.19 and Remark 6.20(ii)]. Any E_1 -rational point on X is necessarily smooth [14, Proposition 17.15.1], i.e., is an E_1 -rational point on the geometrically integral smooth variety X_{sm} . By the assumption applied to the open affine subvarieties of X_{sm} , we must then also have an E_2 -rational point on X_{sm} and therefore on X . By symmetry, this shows that $X(E_1) \neq \emptyset$ if and only if $X(E_2) \neq \emptyset$, as desired. \dashv

PROPOSITION 4.3. *The existential theory of \mathbb{K} agrees with the existential theory of $\mathbb{F}_p((s))$. In particular, it is decidable.*

PROOF. The first statement follows from the two preceding lemmas (take $F = \mathbb{F}_p$, $E_1 = \mathbb{K}$, and $E_2 = \mathbb{F}_p((s))$). The “in particular” is [3, Corollary 7.5]. \dashv

COROLLARY 4.4. *There exists an existentially decidable field K of characteristic p with an existentially undecidable separable quadratic extension. We can choose K such that the relative algebraic closure of \mathbb{F}_p in K is finite.*

PROOF. Let \mathbb{K}^* be an \aleph_0 -saturated elementary extension of \mathbb{K} , and let L/\mathbb{K}^* be a cyclic extension of degree 4 which is existentially undecidable (Theorem 3.7). Let L_0/\mathbb{K}^* be the unique quadratic intermediate field. Since \mathbb{K} is regular over $\mathbb{F}_p(t)$, the prime field \mathbb{F}_p is relatively algebraically closed in \mathbb{K} and thus in \mathbb{K}^* . Hence the relative algebraic closure of \mathbb{F}_p in L is finite. Since \mathbb{K}^* is existentially decidable as \mathbb{K} is, either L_0/\mathbb{K}^* or L/L_0 is a pair of fields as desired. \dashv

This proves Theorem 1.2 from the introduction. As mentioned previously, the analogue in characteristic 0 was established in [26, Theorem 3.3.1], with a similar technique. There the full first-order theory of the base field is decidable, so the result is stronger than ours (inspection of the proof yields that the quadratic extension still has undecidable existential theory). Decidability of the full first-order theory seems out of reach in positive characteristic with the current method, as our understanding of the model theory of valued fields is insufficient.

Conditionally on a conjecture related to resolution of singularities, we can establish a slightly stronger decidability result in the language $\mathcal{L}_{\text{ring}}(\mathbb{F}_p(t))$. Here we fix a natural coding of $\mathbb{F}_p(t)$ (specifically, a coding witnessing the computability of the field $\mathbb{F}_p(t)$) to identify $\mathcal{L}_{\text{ring}}(\mathbb{F}_p(t))$ -formulae with natural numbers. Since every element of $\mathbb{F}_p(t)$ is quantifier-freely $\mathcal{L}_{\text{ring}}$ -definable in terms of the constant t , instead of $\mathcal{L}_{\text{ring}}(\mathbb{F}_p(t))$ we could equivalently work in the expansion of $\mathcal{L}_{\text{ring}}$ by a single constant symbol for t .

LEMMA 4.5. *Assume the consequence (R4) of local uniformisation from [1]. Then there is an algorithm which, given as input $k, n > 0$ and polynomials $f_1, \dots, f_k \in \mathbb{F}_p(t)[X_1, \dots, X_n]$ such that the affine variety described by the f_i is geometrically integral and smooth over $\mathbb{F}_p(t)$, decides whether the variety has a \mathbb{K} -rational point, i.e., whether the f_i have a common zero in \mathbb{K} .*

PROOF. Let V_0 be the set of discrete valuations of $\mathbb{F}_p(t)$ above $\mathbb{F}_p[t]$. By [21, Remark 7.7.3] (a combination of the Lang–Weil bounds and Hensel’s Lemma) one can effectively determine a finite subset $S \subseteq V_0$ such that for all $v \in V_0 \setminus S$ the f_i

have a common zero in the completion $\widehat{\mathbb{F}_p(t)}_v$, and therefore in the henselisation $\mathbb{F}_p(t)_v^h$ since $\mathbb{F}_p(t)_v^h$ is existentially closed in $\widehat{\mathbb{F}_p(t)}_v$ [18, Theorem 5.9].

In order to decide whether the f_i have a common zero in \mathbb{K} , by the local–global principle it therefore suffices to decide whether they have a common zero in the henselisation \mathbb{K}_v^h for each discrete valuation v of \mathbb{K} above one of the valuations in S . The decidability of this problem (under the assumption (R4)) follows from [1, Theorem 4.12]. Indeed, for each such v , the henselisation \mathbb{K}_v^h (with the canonical valuation) is an immediate extension of $\mathbb{F}_p(t)$ (with the restricted valuation), and therefore its universal/existential $\mathcal{L}_{\text{ring}}(\mathbb{F}_p(t))$ -theory is formally entailed by the first-order axioms expressing that it is a henselian valued field extending $(\mathbb{F}_p(t), v|_{\mathbb{F}_p(t)})$ with the same residue field and uniformiser. \dashv

PROPOSITION 4.6. *Assume (R4). Then the existential $\mathcal{L}_{\text{ring}}(\mathbb{F}_p(t))$ -theory of \mathbb{K} is decidable.*

PROOF. Consider the $\mathcal{L}_{\text{ring}}(\mathbb{F}_p(t))$ -theory T given by the following system of axioms:

- (1) the field axioms;
- (2) the quantifier-free diagram of $\mathbb{F}_p(t)$;
- (3) for each irreducible polynomial $f \in \mathbb{F}_p(t)[X]$ the sentence $\forall x(f(x) \neq 0)$;
- (4) for any finite list of polynomials $f_1, \dots, f_k \in \mathbb{F}_p(t)[X_1, \dots, X_n]$ describing a geometrically integral smooth affine $\mathbb{F}_p(t)$ -variety, an axiom asserting that the f_i have a common zero if this is the case in \mathbb{K} , and otherwise an axiom asserting that they do not have a common zero.

We claim that this system of axioms is computably enumerable. This is clear for the field axioms, follows from the computability of $\mathbb{F}_p(t)$ for the quantifier-free diagram, and from the existence of a splitting algorithm for $\mathbb{F}_p(t)$ for the third point. For the fourth point, this is essentially the preceding lemma and the observation that it is decidable whether a system of polynomials defines a geometrically integral smooth variety (for instance by Gröbner basis techniques and the Jacobian criterion).

The models of T are field extensions E of $\mathbb{F}_p(t)$ in which $\mathbb{F}_p(t)$ is relatively algebraically closed, i.e., which are regular over $\mathbb{F}_p(t)$, and such that the same geometrically integral smooth affine $\mathbb{F}_p(t)$ -varieties have rational points in E as in \mathbb{K} . By Lemma 4.2, the theory T is therefore complete for universal and existential $\mathbb{F}_p(t)$ -sentences, i.e., for any existential $\mathbb{F}_p(t)$ -sentence, T entails either the sentence or its negation. A proof calculus therefore gives a decision procedure for existential consequences of T , which proves the claim since $\mathbb{K} \models T$. \dashv

§5. An existentially undecidable complete valued field. Let p be a fixed prime. We prove the following (stated as Theorem 1.1 in the introduction):

THEOREM 5.1. *There exists a complete discretely valued field (E, v) with $\text{char } E = 0$, $\text{char } Ev = p$, such that the existential theory of Ev is decidable, but the existential theory of E is undecidable. We can furthermore choose E such that the set of one-variable polynomials in $\mathbb{Q}[X]$ with a zero in E is decidable.*

PROOF. By Corollary 4.4, we may select an existentially decidable field K of characteristic p with an existentially undecidable separable quadratic extension L , such that furthermore the relative algebraic closure of \mathbb{F}_p in K is finite.

There is an element $\alpha \in L$ with $L = K(\alpha)$ and $a := \alpha^2 - \alpha \in K$. (We use this equation instead of $a = \alpha^2$ to handle all characteristics simultaneously.)

Let (F, v) be the unique complete discretely valued field of characteristic 0 with residue field K and uniformiser p . (See for instance [4, Theorem 2.10 and Corollary 6.6] for the (classical) existence and uniqueness of such (F, v) in terms of the valuation ring, although we do not in fact need the uniqueness.) Let $b \in F$ be a lift of a , and set $E = F(\sqrt{p(1+4b)})$. We continue to write v for the unique prolongation to finite extensions of F , in particular to E .

We claim that (E, v) is as desired. Note first that $v(1+4b) = 0$: this is clear if $p = 2$, and holds for odd p since otherwise $a = -1/4$ and so the polynomial $X^2 - X - a$ would be reducible in K . Therefore the extension E is obtained by adjoining to F a square root of the uniformiser $p(1+4b)$, and is thus totally ramified. In particular $E_v = F_v = K$, which is existentially decidable.

On the other hand, the field $E(\sqrt{p})$ contains the element $\sqrt{1+4b}$, and therefore a root of the polynomial $X^2 - X - b$, so the residue field $E(\sqrt{p})_v$ must be $K(\alpha) = L$. In the complete discretely valued field $(E(\sqrt{p}), v)$ both the valuation ring \mathcal{O}_v and its maximal ideal \mathfrak{m}_v are existentially $\mathcal{L}_{\text{ring}}$ -definable (without parameters), since for a natural number $n > 2$ coprime to p a well-known application of Hensel's Lemma shows that

$$\mathcal{O}_v = \{x \in E(\sqrt{p}) : \exists y(1 + px^n = y^n)\}, \quad \mathfrak{m}_v = \{x \in E(\sqrt{p}) : \exists y(1 + x^n/p = y^n)\}.$$

Therefore the residue field L is (parameter-freely) existentially interpretable in $E(\sqrt{p})$ (i.e., we have an interpretation satisfying the property of [15, Theorem 5.3.2 and Remark 3]), so the existential $\mathcal{L}_{\text{ring}}$ -theory of $E(\sqrt{p})$ is undecidable. (See [15, Theorem 5.3.2 and Remark 4] for generalities on transfer of decidability under interpretations.) Consequently, the existential $\mathcal{L}_{\text{ring}}$ -theory of E is likewise undecidable, since $E(\sqrt{p})$ is quantifier-freely interpretable in E .

Lastly, consider the subfield $\mathbb{Q}_p \subseteq F$ (given as the topological closure of the subfield \mathbb{Q}). Since the relative algebraic closure of \mathbb{F}_p in $F_v = K$ is finite and (F, v) has uniformiser p , the fundamental equality for algebraic extensions of \mathbb{Q}_p (see for instance [10, Proposition 1.4.6]) shows that the relative algebraic closure of \mathbb{Q}_p in F is a finite extension of \mathbb{Q}_p , and therefore the same holds in E . Thus the algebraic part of E is the same as the algebraic part of a local field of characteristic zero. The local fields of characteristic zero have decidable first-order theory [22, Corollary 5.3], so in particular it is decidable whether a given polynomial in $\mathbb{Q}[X]$ has a zero in E . \dashv

REMARK 5.2. The condition that the set of polynomials in $\mathbb{Q}[X]$ with a zero in E be decidable is occasionally phrased as E having “decidable algebraic part,” in the sense that it allows to decide which elements of an algebraic closure of \mathbb{Q} lie in E (up to conjugacy). There is, however, a certain ambiguity in this expression, as it may also be understood to assert that the field $E \cap \overline{\mathbb{Q}}$ is decidable, i.e., has decidable full first-order theory, which is a stronger condition. Our proof of Theorem 5.1 shows that even this stronger condition is satisfied, since the algebraic part of a local field

is an elementary substructure and therefore shares its (decidable) first-order theory [22, Theorem 3.4 and Theorem 5.1].

REMARK 5.3. In [3, Remark 7.6] it was asked whether there exists an existentially undecidable henselian valued field of mixed characteristic with existentially decidable residue field and pointed value group (i.e., value group with a constant for the value of p). Theorem 5.1 provides an example for this phenomenon, as even the full first-order theory of the value group \mathbb{Z} is decidable [15, Theorem 3.3.8] (and expanding by a constant symbol for $v(p)$ does not change this, since any constant in \mathbb{Z} is definable).

It was previously pointed out that there must exist (non-discrete) examples of valued fields with the desired property in [16, Remark 3.6.9], using an inexplicit counting argument. However, the reason for existential undecidability of the examples there is due to it not being decidable which one-variable polynomials over \mathbb{Q} have roots, unlike in our example.

The algebraic part has been known for some time as an obstruction in the model theory of henselian valued fields of mixed characteristic (see for instance [5, Corollary 1.6] and [3, Remark 7.4]). Our theorem shows that the obvious attempt to repair the failure of the decidability statement [3, Corollary 7.5] in mixed characteristic, by requiring a decidable axiom scheme describing the algebraic part, still fails, even in the case of value group \mathbb{Z} .

In the case of finitely ramified fields (generalising the situation of value group \mathbb{Z} in mixed characteristic), a satisfactory replacement for [3, Corollary 7.5] is obtained in [2, Theorem 5.10]: here the obstruction from Theorem 5.1 is surmounted by considering the residue field in a certain expansion of the language of rings.

Acknowledgements. I became aware of the examples presented here some years ago. I would like to thank Arno Fehm for encouraging me to commit them to writing, as well as for comments on a draft version.

REFERENCES

- [1] S. ANSCOMBE, P. DITTMANN, and A. FEHM, *Axiomatizing the existential theory of $\mathbb{F}_q(t)$* . *Algebra & Number Theory*, vol. 17 (2023), no. 11, pp. 2013–2032.
- [2] S. ANSCOMBE, P. DITTMANN, and F. JAHNKE, *Ax–Kochen–Ershov principles for finitely ramified henselian fields*, preprint, 2023. [arXiv:2305.12145](https://arxiv.org/abs/2305.12145) [math.LO].
- [3] S. ANSCOMBE and A. FEHM, *The existential theory of equicharacteristic henselian valued fields*. *Algebra & Number Theory*, vol. 10 (2016), no. 3, pp. 665–683.
- [4] S. ANSCOMBE and F. JAHNKE, *The model theory of Cohen rings*. *Confluentes Mathematici*, vol. 14 (2022), no. 2, pp. 1–28.
- [5] S. ANSCOMBE and F.-V. KUHLMANN, *Notes on extremal and tame valued fields*, this JOURNAL, vol. 81 (2016), no. 2, pp. 400–416.
- [6] R. BECKER and D. GLASS, *Pointless hyperelliptic curves*. *Finite Fields and Their Applications*, vol. 21 (2013), pp. 50–57.
- [7] S. BOSCH, W. LÜTKEBOHMERT, and M. RAYNAUD, *Néron Models*, Springer, Berlin–Heidelberg, 1990.
- [8] B. CONRAD, O. GABBER, and G. PRASAD, *Pseudo-Reductive Groups*, second ed., Cambridge University Press, Cambridge, 2015.
- [9] Y. L. ERSHOV, *Об удивительных расширениях поля рациональных чисел*. *Doklady Akademii Nauk*, vol. 373 (2000), no. 1, pp. 15–16. Translated as: *On surprising extensions of the field of rationals*. *Doklady Mathematics*, vol. 62 (2000), no. 1, pp. 8–9.

- [10] ———, *Multi-Valued Fields*. Springer, New York, 2001.
- [11] D. FERRAND, *Conducteur, descente et pincement*. *Bulletin de la Société Mathématique de France*, vol. 131 (2003), no. 4, pp. 553–585.
- [12] U. GÖRTZ and T. WEDHORN, *Algebraic Geometry I*. Vieweg+Teubner, Wiesbaden, 2010.
- [13] A. GROTHENDIECK, *Éléments de géométrie algébrique: IV. Étude locale des schémas et des morphismes de schémas, Seconde partie*. *Publications Mathématiques de l'IHÉS*, vol. 24 (1965), pp. 5–231.
- [14] ———, *Éléments de géométrie algébrique: IV. Étude locale des schémas et des morphismes de schémas, Quatrième partie*. *Publications Mathématiques de l'IHÉS*, vol. 32 (1967), pp. 5–361.
- [15] W. HODGES, *Model Theory*. Cambridge University Press, Cambridge, 1993.
- [16] K. KARTAS, *Decidability via the tilting correspondence*. *Annals of Pure and Applied Logic*, vol. 174 (2023), no. 2, Article no. 103203.
- [17] ———, *Diophantine problems over tamely ramified fields*. *Journal of Algebra*, vol. 617 (2023), pp. 127–159.
- [18] F.-V. KUHLMANN, *The algebra and model theory of tame valued fields*. *Journal für die Reine und Angewandte Mathematik*, vol. 719 (2016), pp. 1–43.
- [19] J. NEUKIRCH, A. SCHMIDT, and K. WINGBERG, *Cohomology of Number Fields*, second ed., Springer, Berlin–Heidelberg, 2007.
- [20] B. POONEN, *Existence of rational points on smooth projective varieties*. *Journal of the European Mathematical Society*, vol. 11 (2009), no. 3, pp. 529–543.
- [21] ———, *Rational Points on Varieties*. American Mathematical Society, Providence, 2017.
- [22] A. PRESTEL and P. ROQUETTE, *Formally p -adic fields*. Springer, Berlin–Heidelberg, 1984.
- [23] J.-P. SERRE, *Groups algébriques et corps de classes*. Publications de l'Institut de Mathématique de l'Université de Nancago, vol. VII, Hermann, Paris, 1959.
- [24] A. SHLAPENTOKH, *Hilbert's Tenth Problem: Diophantine Classes and Extensions to Global Fields*. Cambridge University Press, Cambridge, 2009.
- [25] R. I. SOARE, *Turing Computability*. Springer, Berlin–Heidelberg, 2016.
- [26] K. THANAGOPAL, *On the decidability of finite extensions of decidable fields*, Ph.D. thesis, University of Oxford, 2018. Available at <https://ora.ox.ac.uk/objects/uuid:c5b04608-c6ff-4b15-b332-36cadf56144e>.
- [27] S. YEKHANIN, *A note on plane pointless curves*. *Finite Fields and Their Applications*, vol. 13 (2007), no. 2, pp. 418–422.

INSTITUT FÜR ALGEBRA
 TECHNISCHE UNIVERSITÄT DRESDEN
 01062 DRESDEN, GERMANY
 E-mail: philip.dittmann@tu-dresden.de