TWO EXAMPLES CONCERNING EXISTENTIAL UNDECIDABILITY IN FIELDS

PHILIP DITTMANN

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 [Shl09]. 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 [AF16, AJ21, ADF22, Kar22] 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 $Ev$ 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.

In order to prove this theorem, 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 Thangagopal’s thesis [Tha18], where an example was given in characteristic $0$. We modify the construction given there, based on Ershov’s theory of fields with a strong local-global principle presented in [Ersh01].

**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.

2. A USEFUL FAMILY OF VARIETIES

Let $p$ be a prime number, $q > 1$ 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 $\frac{q^2}{2}$ with $g \equiv -1 \pmod{p}$, so $\frac{q^2}{2} < g \leq \frac{q^2}{2} + p$. By [BG13, 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 $q^n + 1 - 2g\sqrt{q^m} \geq q^n + 1 - (q-3+2p)q^{m/2}$ 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 [Yeh07].

Proof of the proposition. Let $C/\mathbb{F}_q$ be a curve as in the lemma, so that $C(\mathbb{F}_q^m) = \emptyset$ but $C(\mathbb{F}_q^m) \neq \emptyset$ 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 $C/\mathbb{F}_q$ is so: Indeed, by [CGP15, Proposition A.5.9] $V$ is smooth and geometrically connected (hence geometrically integral), and by [CGP15, Proposition A.5.8] and [BLR90, 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 $C(\mathbb{F}_q^m \otimes_{\mathbb{F}_q} \mathbb{F}_q^m)$. For $m \mid n$ we have $C(\mathbb{F}_q^m \otimes_{\mathbb{F}_q} \mathbb{F}_q^m) = C(\mathbb{F}_q^m) = C(\mathbb{F}_q^m)^n = \emptyset$.

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

Remark 2.4. For given $q$ and $m$, a variety $V$ as in the proposition can be effectively determined, simply by enumerating varieties, testing for points over small fields, and using the Hasse–Weil bound.

3. The construction

Fix again a prime $p$. We find an extension field $K$ 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 ring in the usual sense of commutative algebra. We do not distinguish between valuations and their valuation rings, so in particular we identify equivalent valuations. 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 $K/\mathbb{F}_p(t)$ together with a family $\mathcal{V}$ of discrete valuations such that the following hold:

1. For every $v \in \mathcal{V}$, the restriction of $v$ to $\mathbb{F}_p(t)$ is again a discrete valuation, which lies above $\mathbb{F}_p[t]$. Further, the extension $(K,v)/(\mathbb{F}_p(t),v|_{\mathbb{F}_p(t)})$ is immediate, i.e. the residue fields $K/v$ 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 $v \in \mathcal{V}$ prolonging $v_0$. 

(3) Any $x \in K$ is in the valuation ring of all but finitely many $v \in V$.
(4) If a geometrically integral variety $X/K$ has a smooth $K_v$-point for every $v \in V$ (where $K_v$ is the henselisation), then it has a $K$-point.

Proof. This is a consequence of [Ersh01, Theorem 3.6.3], as we now explain.
Let $V_0$ be the family of discrete valuation rings of $F_p(t)$ above $F_p[t]$. Then any two distinct members of $V_0$ are independent; $V_0$ is a near Boolean family in Ershov’s sense since $F_p[t]$ is an “NB-ring” [Ersh01, Remark 2.5.1] and the valuation rings of the valuations in $V_0$ are precisely the localisations of $F_p[t]$ at its maximal ideals [Ersh01, Proposition 2.5.3]; and the residue fields of $V_0$ are “regularly closed at infinity” [Ersh01, 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 [Poo17, Theorem 7.7.1(iv)].

Thus by [Ersh01, Theorem 3.6.3], there exists a countable regular extension $K/F_p(t)$ 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 $(K, v)/(F_p(t), v_0)$ is immediate. In particular every $v \in V$ is discrete, and conditions (1) and (2) are satisfied.

The bijection $V \to V_0$ is furthermore a homeomorphism with respect to the Zariski topologies on $V$ and $V_0$ (see [Ersh01, Section 2.2]), which means that for all $x \in K$ 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 $F_p(t)$. However, we cannot have $C_x = V$, since otherwise for a suitable element $b \in F_p(t)^\times$ (a high power of a uniformiser for some valuation in $V_0$) the set $C_x b$ would be infinite but strictly contained in $V$, violating the homeomorphism property. Therefore the set $C_x$ is finite for all $x \in K$. This gives condition (3).

In addition, the family $V$ satisfies Ershov’s “arithmetic local-global principle” $\text{LG}_A$, and therefore also the “geometric local-global principle” $\text{LG}_G$ [Ersh01, Proposition 3.2.5], which gives our condition (4) for geometrically integral affine varieties $X/K$. Now take an arbitrary geometrically integral variety $X/K$, and let $X_0/K$ be an affine dense open subvariety. If $X$ has a smooth $K_v$-point for every $v \in V$, then the same holds for $X_0$: This is the ampleness of the henselian field $K_v$ (see [Ersh01, Corollary 3.1.6] and the surrounding discussion). Hence we have $\emptyset \neq X_0(K) \subseteq X(K)$ by the affine case, proving (4) in full generality. \qed

Remarks 3.2.

(1) Fields $K$ as in the proposition are weak analogues of the “surprising extensions of $Q$” considered in [Ersh00] (also variously translated as “wonderful” or “amazing” extensions). Note, however, that there also the place at infinity, i.e. the real place of $Q$, is included.
(2) Since it plays no role in the sequel, we have not imposed the condition which is called maximality in [Ersh00], i.e. that for every proper separable algebraic extension $L/K$, some valuation in $V$ has no immediate extension to $L$. This condition can however always be added, see [Ersh01, Proposition 4.4.3, Remark 4.4.3, Proposition 4.4.4].
(3) Any non-trivial valuation $v$ of $K$ not in $V$ always has separably closed henselisation, and hence poses no obstruction to the existence of rational points on varieties. This follows from [Ersh01, 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 $K$.
(4) Instead of starting with the discrete valuations of $F_p(t)$ above $F_p[t]$, we could have worked with the coordinate ring of any irreducible smooth affine curve over $F_p$ and its function field.

We henceforth fix a field $K$ as in the proposition.
Lemma 3.3. Let $L/K$ be a finite separable extension. Let $X/F_p$ 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 $Lv$.

Proof. Let $W$ be the family of prolongations of valuations in $V$ to $L$. By [Ersh01, 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 $L_w$, $w \in W$.

Let $w \in W$. If $X$ has a point over the henselisation $L_w$, then it has a point over the residue field $Lv$, using that $X$ is projective (given homogenous coordinates of an $L_w$-point of $X$, clear denominators and reduce). Conversely, if $X$ has a point over the residue field $Lv$, then it has a point over the henselisation $L_w$ since there exists an embedding $Lw \hookrightarrow L$ (apply Hensel’s Lemma to the minimal polynomial of a primitive element of $Lw$ over $F_p$). Together with the local-global principle, this proves the statement. □

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

Lemma 3.4. Let $S_1, S_2$ be two disjoint finite sets of prime numbers greater than 4. There exists a cyclic extension $L_0/F_p(t)$ of degree 4 such that:

1. For every $l \in S_1$, there exists a discrete valuation of $L_0$ above $F_p[t]$ with residue field $F_{p'}$.
2. For every $l \in S_2$ and every $F_{pm}$ occurring as the residue field of a valuation of $L_0$, we have $\text{lcm}(l, m) \geq 4l$.

Proof. Let $L_0/F_p(t)$ be a cyclic extension of degree 4 in which each of the (non-zero) finitely many discrete valuations of $F_p(t)$ with residue field $F_{p'}$, $l \in S_1$, is completely split, and each of the finitely many discrete valuations of $F_p(t)$ with residue field $F_{pm}$, $S_1 \cap n \leq 4 \max(S_2)$, is inert. The existence of such an extension follows from the Grunwald–Wang Theorem [NSW07, Theorem 9.2.8], which allows the construction of abelian extensions of $F_p(t)$ in which the decomposition behaviour of finitely many places is prescribed. The field $L_0$ satisfies the required properties. □

Lemma 3.5. Let $S_1, S_2$ be two disjoint finite sets of prime numbers greater than 4. Then there exists a cyclic extension $L/K$ of degree 4 such that conditions (1) and (2) from Lemma 3.4 hold for $L$ (in place of $L_0$).

Proof. Take $L_0/F_p(t)$ as in Lemma 3.4, and let $L = K L_0$ (free compositum, equivalently the tensor product $K \otimes_{F_p(t)} L_0$). 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 $L_0 w \subset L v$. Thus condition (2) transfers from $L_0$ to $L$: Indeed, if $m_0 = [L_0 w : F_p]$ and $m = [L v : F_p]$, we have $m_0 | m$ 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 $F_p[t]$, the restriction $v_0$ to $F_p(t)$ is again discrete, and the defining property of $K$ affords a discrete valuation $v$ on $K$ such that $(K, v)/(F_p(t), v_0)$ is immediate. In particular, $K$ embeds into the completion $\widehat{F_p(t)}_{v_0}$ over $F_p(t)$. Thus $L$ embeds into the completion $\widehat{L_0 w}$ over $F_p(t)$ since both $K$ and $L_0$ have such an embedding and are linearly disjoint over $F_p(t)$. Therefore $L$ carries a discrete valuation above $F_p(t)$ with residue field $L_0 w$. Thus condition (1) transfers from $L_0$ to $L$. □

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

Recall (see for instance [Soa16, 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 $f : \mathbb{N} \to \mathbb{N}$ 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

\footnote{Using the valuative criterion of properness, it would suffice to assume that $X$ is proper instead of projective.}
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 3.6.** 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 \( 4 < l \leq 1 \) and \( V_l(L) \neq \emptyset \) for \( 4 < l \in S_2 \). This problem is solved by Lemma 3.5: Indeed, the field \( L \) produced there satisfies the condition by Lemma 3.3 and the construction of the \( V_l \).

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

**Remark 3.7.** 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 \( l \)-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 \( \mathbb{F}_p(s)_s \) at the \( s \)-adic valuation, since the fields \( \mathbb{F}_p((s)) \) and \( \mathbb{F}_p(s)_s \) have the same existential theory by [AF16, Corollary 7.2] (or by [Kuh16, Theorem 5.9]). Therefore \( X \) has a rational point over the henselisation \( \mathbb{K}_v \) for every \( v \), since every such henselisation embeds \( \mathbb{F}_p(s)_s \) (sending \( s \) to a uniformiser). Now \( X(\mathbb{K}) \neq \emptyset \) follows from the local-global principle. \( \square \)

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 $L_{\text{ring}}(F)$-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 $f_1, \ldots, f_k \in F[X_1, \ldots, X_n]$, 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 [GW10, 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 [EGA IV$_2$, Proposition 6.7.4], integral [GW10, Corollary 5.56(3)], but not geometrically integral, and therefore they have no rational points (see for instance [Poo09, Lemma 10.1]).

Thus let us assume that $X$ is geometrically integral. Then the smooth locus $X_{\text{sm}} \subseteq X$ is dense open [GW10, Theorem 6.19, Remark 6.20(ii)]. Any $E_1$-rational point on $X$ is necessarily smooth [EGA IV$_4$, Proposition 17.15.1], i.e. is an $E_1$-rational point on the geometrically integral smooth variety $X_{\text{sm}}$. By the assumption applied to the open affine subvarieties of $X_{\text{sm}}$, we must then also have an $E_2$-rational point on $X_{\text{sm}}$ 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. \hfill \Box

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 $F = \mathbb{F}_p$, $E_1 = \mathbb{K}$, $E_2 = \mathbb{F}_p((s))$). The “in particular” is [AF16, Corollary 7.5]. \hfill \Box

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 $K^*$ be an $\mathbb{R}_0$-saturated elementary extension of $\mathbb{K}$, and let $L/\mathbb{K}^*$ be a cyclic extension of degree 4 which is existentially undecidable (Theorem 3.6). 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. \hfill \Box

This proves Theorem 1.2 from the introduction. As mentioned previously, the analogue in characteristic 0 was established in [Tha18, 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 $L_{\text{ring}}(\mathbb{F}_p(t))$. 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 $L_{\text{ring}}(\mathbb{F}_p(t))$-formulae with natural numbers. Since every element of $\mathbb{F}_p(t)$ is quantifier-freely $L_{\text{ring}}(\mathbb{F}_p(t))$-definable in terms of the constant $t$, instead of $L_{\text{ring}}(\mathbb{F}_p(t))$ we could equivalently work in the expansion of $L_{\text{ring}}$ by a single constant symbol for $t$. 
Lemma 4.5. Assume the consequence (R4) of local uniformisation from [ADF22]. Then there is an algorithm which, given as input $k, n > 0$ and polynomials $f_1, \ldots, f_k \in \mathbb{F}_p[t][X_1, \ldots, X_n]$ 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 [Poo17, 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 $\hat{\mathbb{F}}_p(t)_v$, and therefore in the henselisation $\mathbb{F}_p(t)_v$ since $\mathbb{F}_p(t)_v$ is existentially closed in $\hat{\mathbb{F}}_p(t)_v$ [Kuh16, 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 $\mathbb{K}_v$ 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 [ADF22, Theorem 4.12]. Indeed, for each such $v$, the henselisation $\mathbb{K}_v$ (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. □

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 $f_1, \ldots, f_k \in \mathbb{F}_p(t)[X_1, \ldots, X_n]$ 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 $\mathbb{K} \models T$. □

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 char $E = 0$, 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 $F_p$ 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 [AJ21, 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 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 $Ev = Fv = K$, 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 $m_v$ 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

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

Therefore the residue field $L$ is (parameter-freely) existentially interpretable in $E(\sqrt{p})$ (i.e. we have an interpretation satisfying the property of [Hod93, Theorem 5.3.2, Remark 3]), so the existential $\mathcal{L}_{\text{ring}}$-theory of $E(\sqrt{p})$ is undecidable. (See [Hod93, Theorem 5.3.2, 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 $Q_p \subseteq F$ (given as the topological closure of the subfield $Q$). Since the relative algebraic closure of $F_p$ in $Fv = K$ is finite and $(F, v)$ has uniformiser $p$, the fundamental equality for algebraic extensions of $Q_p$ (see for instance [Ersh01, Proposition 1.4.6]) shows that the relative algebraic closure of $Q_p$ in $F$ is a finite extension of $Q_p$, 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 [PR84, Corollary 5.3], so in particular it is decidable whether a given polynomial in $Q[X]$ has a zero in $E$.  

Remark 5.2. The condition that the set of polynomials in $Q[X]$ 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 $Q$ 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 $E \cap \overline{Q}$ 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 [PR84, Theorem 3.4 and Theorem 5.1].

Remark 5.3. In [AF16, 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 [Hod93,
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 [Kar21, 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 [AK16, Corollary 1.6] and [AF16, Remark 7.4]. Our theorem shows that the obvious attempt to repair the failure of the decidability statement [AF16, 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 \( \mathbb{Z} \).

References

[ADF22] S. Anscoume, Ph. Dittmann and A. Fehm. Axiomatizing the existential theory of \( \mathbb{F}_q(\!(\ell)\!) \). arXiv:2205.05438 [math.LO], 2022. 1, 4, 5

[AF16] S. Anscoume and A. Fehm. The existential theory of equicharacteristic henselian valued fields. Algebra \& Number Theory, 10(3):665–683, 2016. 1, 4, 5, 3

[AJ21] S. Anscoume and F. Jahnke. The model theory of Cohen rings. arXiv:1904.08297v3 [math.LO], 2021. 1, 5

[AK16] S. Anscoume and F.-V. Kuhlmann. Notes on extremal and tame valued fields. J. Symbolic Logic, 81(2):400–416, 2016. 5, 3

[BG13] R. Becker and D. Glass. Pointless hyperelliptic curves. Finite fields appl. 21:30–57, 2013. 2

[BLR90] S. Bosch, W. Lütkebohmert and M. Raynaud. Néron models. Springer, 1990. 2

[CGP15] B. Conrad, O. Gabber and G. Prasad. Pseudo-reductive groups. 2nd edition, Cambridge University Press, 2015. 2

[EGA IV\textsubscript{2}] A. Grothendieck. Éléments de géométrie algébrique: IV. Étude locale des schémas et des morphismes de schémas, Seconde partie. Publ. math. IHES, 24:5–231, 1965. 4

[EGA IV\textsubscript{4}] A. Grothendieck. Éléments de géométrie algébrique: IV. Étude locale des schémas et des morphismes de schémas, Quatrième partie. Publ. math. IHES, 32:5–361, 1967. 4

[Ersh00] Yu. L. Ershov. Ob удивительных расширениях поля рациональных чисел. Dokl. Akad. Nauk, 373(1):15–16, 2000. Translated as: On surprising extensions of the field of rationals. Doklady Mathematics, 62(1):8–9, 2000. 1, 2

[Ersh01] Yu. L. Ershov. Multi-Valued Fields. Springer, 2001. 1, 3, 2, 3, 5

[GW10] U. Görtz and T. Wedhorn. Algebraic Geometry I. Vieweg+Teubner, 2010. 4

[Hod93] W. Hodges. Model theory. Cambridge University Press, 1993. 5, 5.3

[Kar21] K. Kartas. Decidability via the tilting correspondence. arXiv:2001.04424v4 [math.LO], 2021. 5, 3

[Kar22] K. Kartas. Diophantine problems over tamely ramified fields. arXiv:2103.14646v3 [math.AG], 2022. 1

[Kuh16] F.-V. Kuhlmann. The algebra and model theory of tame valued fields. J. reine angew. Math., 719:1–43, 2016. 4, 4

[NSW07] J. Neukirch, A. Schmidt, and K. Wingberg. Cohomology of Number Fields. Springer, second edition, 2007. 3

[Poo09] B. Poonen. Existence of rational points on smooth projective varieties. J. Eur. Math. Soc. 11(3):529–543, 2009. 4

[Poo17] B. Poonen. Rational points on varieties. American Mathematical Society, 2017. 3, 4

[PR84] A. Prestel and P. Roquette. Formally p-adic fields. Springer, 1984. 5, 5.2

[Shi09] A. Shlapentokh. Hilbert’s Tenth Problem. Diophantine Classes and Extensions to Global Fields. Cambridge University Press, 2009. 1

[Soa16] R. I. Soare. Turing computability. Springer, 2016. 3

[Tha18] Kesavan Thanagopal. On the decidability of finite extensions of decidable fields. Doctoral thesis, University of Oxford, 2018. https://ora.ox.ac.uk/objects/uuid:c5b04608-c6ff-4b15-b332-36cadf56144e 1, 4

[Yekh07] S. Yekhanin. A note on plane pointless curves. Finite fields appl. 13(2):418–422, 2007. 2, 3

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

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