# UNIFORM FIRST-ORDER DEFINITIONS IN FINITELY GENERATED FIELDS

BJORN POONEN

ABSTRACT. We prove that there is a first-order sentence in the language of rings that is true for all finitely generated fields of characteristic 0 and false for all fields of characteristic $> 0$. We also prove that for each $n \in \mathbb{N}$, there is a first-order formula $\psi_n(x_1, \dots, x_n)$ that when interpreted in a finitely generated field $K$ is true for elements $x_1, \dots, x_n \in K$ if and only if the elements are algebraically dependent over the prime field in $K$.

## 1. INTRODUCTION

1.1. **Theorems for finitely generated fields.** It is important, especially when trying to transfer results from one structure to another, to know whether a property can be expressed by the truth of a first-order sentence. For example, it is a basic theorem of model theory that a first-order sentence in the language of rings true for one algebraically closed field of characteristic 0 is true for all algebraically closed fields of characteristic 0; it is because of this that many theorems proved for $\mathbb{C}$ using analytic methods are known to hold for arbitrary algebraically closed fields of characteristic 0.

But many properties have no such simple first-order characterizations. Characterizing characteristic 0 fields among all fields with a single sentence is a typical impossible task: compactness shows that for every sentence $\phi$ valid for an algebraically closed field of characteristic 0, there is a number $p_0$ such that $\phi$ holds also for every algebraically closed field of characteristic $\geq p_0$.

Similarly, one cannot detect whether elements $t_1, \dots, t_n$ are algebraically dependent over the prime subfield by means of a single formula with $n$ free variables. When $n = 1$, this would amount to defining the relative algebraic closure $k$ of the prime field in $K$ uniformly, but if $K = \mathbb{C}$, then every definable subset of $K$ is either finite or cofinite, while $k = \overline{\mathbb{Q}}$ is neither.

We focus our attention on finitely generated fields, i.e., fields that are finitely generated over the prime subfield. Our main theorems show that the arithmetic of these fields is rich enough that the previously impossible tasks become possible.

Before giving these theorems, we fix a few conventions. A **formula** is a first-order formula in the language of rings. If $\phi$ is a **sentence** (a formula with no free variables) and $K$ is a field, then $K \models \phi$ is the statement that $\phi$ is true for $K$. A **definable subset** is one defined by a formula *without constants*. The **prime subfield** $\mathbb{F}$ of a field $K$ is its minimal subfield (either

$\mathbb{Q}$ or $\mathbb{F}_p$ for some prime $p$). When discussing a finitely generated field $K$, we will always use $k$ to denote the **field of constants**, defined as the (relative) algebraic closure of $\mathbb{F}$ in $K$.

**Theorem 1.1.** *There is a sentence that is true for all finitely generated fields of characteristic $0$, and false for* all *fields of characteristic $> 0$.*

**Theorem 1.2.** *There exists a formula $\phi(t)$ that when interpreted in an* infinite *finitely generated field $K$ is true if and only if $t \in \mathbb{F}$.*

The hypothesis in Theorem 1.2 that $K$ is infinite is necessary, because there is no uniform definition of $\mathbb{F}_p$ in $\mathbb{F}_{p^2}$ [CvdDM92].

**Theorem 1.3.** *There exists a formula $\psi(t)$ that when interpreted in a finitely generated field $K$ is true if and only if $t \in k$.*

**Theorem 1.4.** *For each $n \in \mathbb{N}$, there exists a formula $\psi_n(t_1, \ldots, t_n)$ that when interpreted in a finitely generated field $K$ is true if and only if $t_1, \ldots, t_n$ are algebraically dependent over $k$ (or equivalently, over $\mathbb{F}$).*

*Remark* 1.5. The $n = 1$ case of Theorem 1.4 is Theorem 1.3.

*Remark* 1.6. Using different methods, it is possible to prove geometric analogues of these results, for function fields over algebraically closed and other "large" fields. These will appear in a future joint paper with F. Pop.

*Remark* 1.7. Our results give also a proof of the undecidability of the first-order theory of any infinite finitely generated field: see Remark 5.2.

1.2. **Questions about the richness of the arithmetic of finitely generated fields.**
The sentence of Theorem 1.1 defines the class of characteristic $0$ finitely generated fields among all finitely generated fields. Can any "reasonable" class of infinite finitely generated fields be distinguished by a single sentence?

E. Hrushovski suggested the following definition of "reasonable". Fix any natural bijection between the set of $(r, f_1, \ldots, f_m)$ with $r \in \mathbb{N}$ and $f_1, \ldots, f_m \in \mathbb{Z}[x_1, \ldots, x_r]$ and a recursive subset $A \subseteq \mathbb{N}$, such as the one sending $(r, f_1, \ldots, f_m)$ to the concatenation of the ASCII symbols of the characters in the TEX code for $(r, f_1, \ldots, f_m)$. There is an algorithm for testing whether an ideal $(f_1, \ldots, f_m) \subseteq \mathbb{Z}[x_1, \ldots, x_r]$ is prime [Asc04, p. 432] and of infinite index; i.e., the set of $a \in A$ corresponding to $(r, f_1, \ldots, f_m)$ with this property is a recursive subset $B$. We have a surjection

$$\kappa \colon B \to \{\text{isomorphism classes of infinite finitely generated fields}\}$$

sending an $a \in B$ corresponding to $(r, f_1, \ldots, f_m)$ to the fraction field of $\mathbb{Z}[x_1, \ldots, x_r]/(f_1, \ldots, f_m)$. Call a set $S$ of isomorphism classes of infinite finitely generated fields **reasonable** if $\{a \in B : \kappa(a) \in S\}$ is a first-order definable subset in $(\mathbb{N}, +, \cdot)$. If $\phi$ is a sentence, the set of isomorphism classes of infinite finitely generated fields $K$ such that $K \models \phi$ is a reasonable set.

**Question 1.8.** Does every reasonable set of isomorphism classes of infinite finitely generated fields arise from a sentence $\phi$ as above?

For example, the set of (isomorphism classes of) function fields of smooth projective $\mathbb{Q}$-varieties having a rational point is a reasonable set, so a positive answer to Question 1.8 would

say in particular that there is a sentence that is true for these infinite finitely generated fields and no others. Also, any single isomorphism class forms a reasonable set, so a positive answer to Question 1.8 would imply a positive answer to the following, which obviously holds for finite fields:

**Question 1.9.** Is it true that for every finitely generated field $K$, there is a sentence $\phi_K$ that is true for $K$ and false for all finitely generated fields $L \not\simeq K$?

The theory $\mathrm{Th}(K)$ of a field $K$ is the set of sentences $\phi$ such that $K \models \phi$. Fields $K$ and $L$ are elementarily equivalent (and we then write $K \equiv L$) if $\mathrm{Th}(K) = \mathrm{Th}(L)$. A positive answer to Question 1.9 would imply a positive answer to the following question, which was raised by G. Sabbagh in a special case and formulated explicitly by F. Pop [Pop02].

**Question 1.10.** Is it true that whenever $K$ and $L$ are finitely generated fields and $K \equiv L$, we have $K \simeq L$?

Note added: Thomas Scanlon has announced a positive answer to Question 1.9, by building on the results of this paper.

1.3. **Structure of this paper.** Section 2 describes earlier work that will be useful to us. Section 3 shows how to define the field of constants in a finitely generated field of characteristic 0. Section 4 shows how to define the family of relatively algebraically closed global function fields in a finitely generated field of characteristic $> 0$: this is by far the hardest part of the paper. Section 5 combines the results obtained so far to prove the main theorems. Finally, Section 6 shows that the formulas promised by the main theorems cannot be purely existential.

## 2. Previous work

**Definition 2.1.** The Kronecker dimension of a finitely generated field $K$ is

$$\mathrm{Krdim}\, K := \begin{cases} \mathrm{trdeg}(K/\mathbb{F}_p), & \text{if char } K = p > 0 \\ \mathrm{trdeg}(K/\mathbb{Q}) + 1, & \text{if char } K = 0. \end{cases}$$

A global field is a finitely generated field $K$ with $\mathrm{Krdim}\, K = 1$; such a field is either a number field (finite extension of $\mathbb{Q}$) or a global function field (function field of a curve over a finite field).

R. Rumely [Rum80], building on the work of J. Robinson, proved Theorems 1.1, 1.2 and 1.3 (and hence also Theorem 1.4) in the case of global fields. We record some of his results in the following theorem.

**Theorem 2.2.**
(1) *There is a sentence that is true for all number fields and false for all global function fields.*
(2) *There is a formula that for any global field defines the prime subfield.*
(3) *There is a formula that for any number field defines the subset $\mathbb{Z}$.*
(4) *There is a formula that for any number field defines the subset $\mathbb{N}$.*
(5) *There is a formula that for any global function field defines the constant field.*
(6) *There is a formula with a parameter $x$ that for all global function fields defines the ring $\mathbb{F}[x]$ in $K$. (See [Rum80, p. 211].)*

(7) *There is a formula with a parameter $x$ that for all global function fields defines the ring $k[x]$ in $K$.*

(8) *There are formulas with a parameter $x$ that for any global field $K$ and $x \in K - k$ defines a model of $(\mathbb{N}, +, \cdot)$ in $K$ consisting of the powers of $x$.*

We will also need the following result proved by Pop using the recently proved connection between isotropy of Pfister forms and cohomological dimension: see also Proposition A.3.

**Theorem 2.3** ([Pop02]). *For each $n \in \mathbb{N}$, there is a sentence $\sigma_n$ that for a finitely generated field $K$ holds if and only if $\mathrm{Krdim}\, K = n$.*

It follows from these results that Question 1.9 has a positive answer for any finitely generated $K$ with $\mathrm{Krdim}\, K \leq 1$.

The paper [Pop02] also answered Question 1.10 and its geometric analogue in the case where one of the finitely generated fields is a function field of general type.

## 3. Defining constants in characteristic 0

**Definition 3.1.** Suppose $P$ (the parameter space) is a definable subset of $K^N$, and $D$ is a definable subset of $K^M \times P$. For each $\vec{p} \in P$, we get a subset $S_{\vec{p}} := \{\vec{a} \in K^M : (\vec{a}, \vec{p}) \in D\}$. Any family of subsets of $K^M$ that equals $\{S_{\vec{p}} : \vec{p} \in P\}$ for some such $P$ and $D$ will be called a definable family of subsets.

If $X$ is a variety over a field $K$, and $L$ is a field extension of $K$, we let $X_L$ denote $X \times_K L$.

**Lemma 3.2.** *Given a finitely generated field $K$ of characteristic $0$, with field of constants $k$, there exists an elliptic curve $E$ over $\mathbb{Q}$ such that $E(\mathbb{Q})$ is infinite and $E(K) = E(k)$.*

*Proof.* This is a special case of [MB05, Lemma 11.1(i)]. $\square$

The idea behind the following two proofs is contained in the proof of [Den78, Lemma 3.4(iii)] and [KR95, Proposition 3]: see also [MB05, Lemma 11.1(ii)].

**Lemma 3.3.** *Let $E$ be an elliptic curve over $\mathbb{Q}_p$. Equip $E(\mathbb{Q}_p)$ with the $p$-adic topology. The closure of any infinite subgroup of $E(\mathbb{Q}_p)$ is an open neighborhood of the identity $O \in E(\mathbb{Q}_p)$.*

*Proof.* By the theory of formal groups, $E(\mathbb{Q}_p)$ contains a finite-index subgroup that is isomorphic as a topological group to $\mathbb{Z}_p$. The result for infinite subgroups of $E(\mathbb{Q}_p)$ now follows from the corresponding result for $\mathbb{Z}_p$. $\square$

**Lemma 3.4.** *There exists a definable family $\mathcal{F}_1$ of subsets of $K$, defined by a formula independent of $K$, such that if $K$ is a finitely generated field of characteristic $0$, some $S \in \mathcal{F}_1$ is a subset of $k$ such that for each finite prime $p$, the intersection $S \cap \mathbb{Q}$ is $p$-adically dense in $\mathbb{Q}_p$.*

*Proof.* For each $(a, b) \in K^2$, consider the subset

$$S_{a,b} := \{x/y : x \in K, \ y \in K^*, \ \text{and} \ y^2 = x^3 + ax + b\}.$$

of $K$. These subsets form a definable family $\mathcal{F}_0$.

Now suppose that $K$ is a finitely generated field of characteristic $0$. Let $a, b$ be the elements of $\mathbb{Q}$ defining the elliptic curve $E$ of Lemma 3.2. Then $E(K) = E(k)$, so $S_{a,b} \subseteq k$. Applying Lemma 3.3 to the infinite group $E(\mathbb{Q})$ shows that $E(\mathbb{Q})$ is $p$-adically dense in a neighborhood

4

of $O$ in $E(\mathbb{Q}_p)$. Since the rational function $x/y$ on $E$ is a uniformizing parameter at $O$, it is a local diffeomorphism between a neighborhood of $O$ in $E(\mathbb{Q}_p)$ and a neighborhood of $0$ in $\mathbb{Q}_p$. Thus the $p$-adic closure of $S_{a,b} \cap \mathbb{Q}$ contains a neighborhood of $0$ in $\mathbb{Q}_p$.

Finally, for each $(a,b)$, let $T_{a,b}$ be the set of ratios of nonzero elements of $S_{a,b}$. The subsets $T_{a,b}$ form a definable family $\mathcal{F}_1$ having the required property. □

**Lemma 3.5.** *Let $K$ be a finitely generated field of characteristic $0$ with $\sqrt{-1} \in K$. Let $S$ be as in Lemma 3.4. Then $k$ is the set of $t \in K$ such that for all $s_1, s_2, s_3 \in S$, the Pfister form $\langle\langle s_1, s_2, t - s_3 \rangle\rangle$ over $K$ represents $0$.*

*Proof.* Suppose $t \in k$ and $s_1, s_2, s_3 \in S$. Then $s_1, s_2, t - s_3 \in k$. The form $\langle\langle s_1, s_2, t - s_3 \rangle\rangle$ is of rank $> 4$, and $k$ is a totally complex number field, so $\langle\langle s_1, s_2, t - s_3 \rangle\rangle$ represents $0$ over $k$, and hence also over $K$.

Now suppose $t \notin k$. Let $V$ be an integral $k$-variety with function field $K$. Replacing $V$ by an open subset, we may assume $t$ is regular on $V$. Since $t \notin k$, the map $t \colon V \to \mathbb{A}^1_k$ is dominant. Since $\operatorname{char} k = 0$, we may shrink $V$ further to assume that $t$ is smooth. Since $t$ is dominant, some $s_3 \in S \subseteq \mathbb{A}^1(k)$ is in the image of $t$. Choose a closed point $v \in V$ at which $t - s_3$ vanishes. Then $t - s_3$ is part of a system of local parameters at $v$. Let $\ell$ be the residue field of $v$, so $\ell$ is a number field. Choose a prime $p$ of $\mathbb{Q}$ that splits completely in $\ell$. Choose $a, b \in \mathbb{Q}_p$ such that $\langle\langle a, b \rangle\rangle$ has no nontrivial zero. Approximate $a, b$ $p$-adically by $s_1, s_2 \in S \cap \mathbb{Q}$, closely enough that $\langle\langle s_1, s_2 \rangle\rangle$ still has no nontrivial zero over $\mathbb{Q}_p$. Since $\ell$ injects into $\mathbb{Q}_p$, $\langle\langle s_1, s_2 \rangle\rangle$ has no nontrivial zero over $\ell$. Lemma A.5 implies that $\langle\langle s_1, s_2, t - s_3 \rangle\rangle$ has no nontrivial zero over $K$. □

**Lemma 3.6.** *There exists a definable family $\mathcal{F}_2$ of subsets of $K$, defined by a formula independent of $K$, such that if $K$ is a finitely generated field of characteristic $0$, one of the subsets in $\mathcal{F}_2$ is the field of constants $k$.*

*Proof.* Let $\mathcal{F}_1$ be as in Lemma 3.4. For each $S \in \mathcal{F}_1$, consider

$$A_S := \{t \in K : (\forall s_1, s_2, s_3 \in S)\, \langle\langle s_1, s_2, t - s_3 \rangle\rangle \text{ represents } 0 \text{ over } K(\sqrt{-1})\}.$$

The family $\mathcal{F}_2$ of such subsets is a definable family defined by a formula independent of $K$.

Now suppose $K$ is a finitely generated field of characteristic $0$. If $S$ is the infinite subset of $k$ promised by Lemma 3.4, then Lemma 3.5 implies that

$$A_S = K \cap (\text{constant subfield of } K(\sqrt{-1})) = k.$$

□

**Lemma 3.7.** *There is a formula $\phi(x)$ that when interpreted in a finitely generated field of characteristic $0$ defines its field of constants, and that when interpreted in a finitely generated field of characteristic $> 0$ defines the empty set.*

*Proof.* Let $\mathcal{F}_2$ be as in Lemma 3.6, so $k \in \mathcal{F}_2$. We can find a definable subfamily $\mathcal{F}_3 \subseteq \mathcal{F}_2$ consisting of the sets in $\mathcal{F}_2$ that are fields. All these fields are finitely generated, so we may apply Theorem 2.3 with $n = 1$ and then Theorem 2.2(1) to find a definable subfamily $\mathcal{F}_4 \subseteq \mathcal{F}_3$ consisting of the sets of $\mathcal{F}_3$ that are number fields. The union $\ell$ of the sets in $\mathcal{F}_4$ is a subset of $K$ definable by a formula independent of $K$.

If $K$ is a finitely generated field of characteristic $0$, each set in $\mathcal{F}_4$ is a subfield of $k$, and $k \in \mathcal{F}_4$, so $\ell = k$. On the other hand, if $K$ is a finitely generated field of characteristic $p > 0$, then $\mathcal{F}_4$ is empty, so $\ell = \emptyset$. □

## 4. DEFINING SUBFIELDS OF TRANSCENDENCE DEGREE 1 OVER FINITE FIELDS

For this section, we fix the following notation:

- $K$ is a finitely generated field of characteristic $p > 0$.
- $k$ is the field of constants of $K$.
- $\mathcal{L}$ is the set of subfields $L \subseteq K$ such that $L$ is relatively algebraically closed in $K$ and $\mathrm{trdeg}(L/k) = 1$.

Moreover, we use the following notation for the rest of the paper: let $d = 3$ if char $k = 2$ and $d = 2$ otherwise.

Our goal in this section is to construct a definable family of subsets of $K$ consisting of the fields in $\mathcal{L}$. We will mainly try to follow the constructions of the previous section used to define the collection of number fields in $K$ in the characteristic 0 case, but more elaborate arguments will be needed, since certain steps fail. For instance, the analogue of Lemma 3.3 for local fields of characteristic $p$ is false.

### 4.1. Nearly prime generalized Mersenne numbers.
Let $E$ be an ordinary elliptic curve over a finite field $\mathbb{F}_q$. We would like to find primes $\ell$ such that $\#E(\mathbb{F}_{q^\ell})$ is close to being prime. Let $R = \mathrm{End}_{\mathbb{F}_q} E$. Let $N \colon R \otimes \mathbb{Q} \to \mathbb{Q}$ be the norm map. Let $F \in R$ be the $q$-power Frobenius endomorphism. Then $\#E(\mathbb{F}_{q^\ell}) = N(F^\ell - 1)$ (whereas Mersenne numbers are numbers of the form $2^\ell - 1$).

For an integer $n$, define $\Psi(n) := \sum_{p|n} \frac{1}{p}$, where the sum is over the distinct prime divisors $p$ of $n$. We consider $n$ to be nearly prime if $\Psi(n)$ is small. (Perhaps a better name would be "not too composite".)

**Lemma 4.1.** *For any ordinary elliptic curve $E$ over $\mathbb{F}_q$,*

$$\liminf_{\ell \to \infty} \Psi\left(\frac{\#E(\mathbb{F}_{q^\ell})}{\#E(\mathbb{F}_q)}\right) = 0.$$

*Proof.* Let $\mathcal{O}$ be the ring of integers of $R \otimes \mathbb{Q}$. Define

$$e_\ell := \frac{\#E(\mathbb{F}_{q^\ell})}{\#E(\mathbb{F}_q)} = N\left(\frac{F^\ell - 1}{F - 1}\right).$$

If $\ell$ and $m$ are distinct primes, then the ideal $(x^\ell - 1, x^m - 1)$ in $\mathbb{Z}[x]$ equals $(x - 1)$, since reducing one generator modulo the other iteratively amounts to running the Euclidean algorithm on the exponents. Thus the ideals $\left(\frac{F^\ell - 1}{F - 1}\right)$ and $\left(\frac{F^m - 1}{F - 1}\right)$ of $\mathcal{O}$ are coprime. There are at most two prime ideals of $\mathcal{O}$ above a given prime of $\mathbb{Z}$, so each prime of $\mathbb{Z}$ divides at most two of the $e_\ell$. Hence

$$(1) \qquad \sum_{\ell \leq B} \Psi(e_\ell) \leq 2\Psi\left(\prod_{\ell \leq B} e_\ell\right).$$

Since $e_\ell \leq \#E(\mathbb{F}_{q^\ell}) = q^\ell(1 + o(1))$ as $\ell \to \infty$, we have $\prod_{\ell \leq B} e_\ell = q^{O(B^2)}$ as $B \to \infty$. In particular $\prod_{\ell \leq B} e_\ell$ has at most $O(B^2)$ distinct prime factors. Thus

$$(2) \qquad \Psi\left(\prod_{\ell \leq B} e_\ell\right) \leq \sum_{j=1}^{O(B^2)} \frac{1}{j} = O(\log B).$$

6

Combining equations (1) and (2) yields

$$\sum_{\ell \leq B} \Psi(e_\ell) = O(\log B).$$

If $\pi(B)$ is the number of primes $\leq B$, then some term $\Psi(e_\ell)$ on the left is bounded by $O(\log B)/\pi(B)$, which tends to 0 as $B \to \infty$. $\square$

*Remark* 4.2. The conclusion of Lemma 4.1 holds also for supersingular $E$, but we do not need this.

**Lemma 4.3.** *Let $E$ be an ordinary elliptic curve over $\mathbb{F}_q$. Fix $\ell \in \mathbb{Z}_{\geq 1}$. The probability that a random element of $E(\mathbb{F}_{q^\ell})$ generates $E(\mathbb{F}_{q^\ell})/E(\mathbb{F}_q)$ as an $R$-module is at least $1 - 2\Psi(n)$ where $n := \#E(\mathbb{F}_{q^\ell})/\#E(\mathbb{F}_q)$.*

*Proof.* We continue to let $R = \mathrm{End}_{\mathbb{F}_q} E$. Since $E$ is ordinary, [Len96, Theorem 1(a)] gives an isomorphism of $R$-modules $\iota \colon E(\mathbb{F}_{q^\ell}) \to R/(F^\ell - 1)R$. If $P \in E(\mathbb{F}_{q^\ell})$ does not generate $E(\mathbb{F}_{q^\ell})/E(\mathbb{F}_q)$ as an $R$-module, then the $R$-submodule of $E(\mathbb{F}_{q^\ell})$ generated by $P$ and $E(\mathbb{F}_q)$ must correspond under $\iota$ to a proper ideal of $R' := R/(F^\ell - 1)R$, and hence be contained in a maximal ideal $\mathfrak{m}$ of $R'$ of residue characteristic dividing $n$. If $\mathfrak{m}_1, \ldots, \mathfrak{m}_r$ are the maximal ideals of residue characteristic $p$, then $\mathfrak{m}_1 \cap \cdots \cap \mathfrak{m}_r$ is of index at least $p^r$ in $R'$, but it contains $pR'$ which has index at most $(R : pR) = p^2$, so $r \leq 2$. The probability that $\iota(P)$ lies in a given $\mathfrak{m}$ of residue characteristic $p$ is at most $1/p$, so the probability that $\iota(P)$ lies in some $\mathfrak{m}$ of residue characteristic dividing $n$ is at most $\sum_{p|n} \frac{2}{p} = 2\Psi(n)$. $\square$

## 4.2. **More elliptic curve lemmas.**

**Lemma 4.4.** *For any finite field $k$, there exists an ordinary elliptic curve over $k$.*

*Proof.* Let $p = \mathrm{char}\, k$. If $p \geq 5$, then apart from 0 and 1, there are at most $(p-1)/2$ values of $\lambda \in \mathbb{F}_p$ for which $y^2 = x(x-1)(x-\lambda)$ is supersingular [Sil92, V.4.1(b)], so for some $\lambda \in \mathbb{F}_p$, this curve is ordinary. For $p = 3$, the curve $y^2 = x^3 + x^2 - x$ is ordinary. For $p = 2$, the curve $y^2 + xy = x^3 + 1$ is ordinary. $\square$

**Lemma 4.5.** *There is a universal constant $c \in \mathbb{R}_{>0}$ such that the following holds. Let $E$ be an elliptic curve over a finite field $\mathbb{F}_q$ in Weierstrass form. Let $z$ be the rational function $y/x$ on $E$. Let $G$ be a subgroup of $E(\mathbb{F}_q)$. If $(E(\mathbb{F}_q) : G) < cq^{1/2}$,*

$$\{z(g_1) + z(g_2) : g_i \in G - \{poles\ of\ z\}\} = \mathbb{F}_q.$$

*Proof.* Fix $t \in \mathbb{F}_q$, and define a curve

$$X := \{(P_1, P_2) \in (E - \{\text{poles of } z\})^2 : z(P_1) + z(P_2) = t\}.$$

Let $\overline{X}$ be the Zariski closure of $X$ in $E \times E$. Let $X^{\mathrm{smooth}}$ be the smooth locus of $X$, and $\overline{X}^{\mathrm{smooth}}$ the smooth locus of $\overline{X}$. If we use $w = 1/z$ as a uniformizer at the identity $O$ of $E$, then we obtain a system of local parameters $w_1, w_2$ at $(O, O) \in E \times E$, and the local equation of $X$ there is $1/w_1 + 1/w_2 = t$, which after clearing denominators is $w_2 + w_1 = tw_1w_2$; thus $(O, O) \in \overline{X}^{\mathrm{smooth}}$. Let $g \geq 1$ be a universal upper bound (independent of $q$, $E$, $t$) for the geometric genus of the geometric components of the normalization $\hat{X}$ of $\overline{X}$, and let $r$ be a universal upper bound for the number of $\overline{\mathbb{F}}_q$-points in $\hat{X} - X^{\mathrm{smooth}}$. Define $c := 1/(2g + r)$.

The separable isogeny $F - 1\colon E \to E$ factors through $E \twoheadrightarrow E' := E/G$ so we get the homomorphism $\phi$ in the commutative diagram

$$
\begin{array}{ccc}
E & \xrightarrow{\;F-1\;} & E \\
\downarrow & {\scriptstyle \phi} \nearrow & \downarrow \\
E' & \xrightarrow{\;F-1\;} & E'.
\end{array}
$$

The lower right triangle now shows that $G = \phi(E'(\mathbb{F}_q))$. Let $\delta := \deg \phi = (E(\mathbb{F}_q) : G) \le cq^{1/2}$.

Let $X' = (\phi, \phi)^{-1}(X) \subset E' \times E'$. Let $\overline{X}' = (\phi, \phi)^{-1}(\overline{X})$. Its smooth locus $(\overline{X}')^{\mathrm{smooth}}$ equals $(\phi, \phi)^{-1}(\overline{X}^{\mathrm{smooth}})$. Then $(O, O) \in (\overline{X}')^{\mathrm{smooth}}(\mathbb{F}_q)$, so the irreducible component of $\overline{X}'$ containing $(O, O)$ is geometrically irreducible. Thus the dense open subset $X'^{\mathrm{smooth}}$ of $\overline{X}'$ also has a geometrically irreducible component $C'$. Since $C'$ is finite étale of degree at most $\delta$ over $X^{\mathrm{smooth}}$, it is a curve of geometric genus at most $g' := \delta(g-1) + 1 \le cq^{1/2}g$ with at most $r' := \delta r \le cq^{1/2}r$ geometric points removed. By the Weil conjectures

$$\#C'(\mathbb{F}_q) \ge q + 1 - 2g'q^{1/2} - r' > q - 2cgq - crq^{1/2} \ge q(1 - (2g + r)c) = 0.$$

In particular, there exists a point $(P_1, P_2) \in C'(\mathbb{F}_q)$. For $i = 1, 2$, define $g_i := \phi(P_i) \in \phi(E'(\mathbb{F}_q)) = G$. By definition of $C'$, we have $z(g_1) + z(g_2) = t$. $\qquad\square$

**Lemma 4.6.** *Let $E$ be an ordinary elliptic curve over a finite field $\mathbb{F}_q$. Let $R = \mathrm{End}_{\mathbb{F}_q}(E)$. Let $W$ be a geometrically integral $\mathbb{F}_q$-variety with a smooth morphism $\pi = (\pi_1, \pi_2)\colon W \to \mathbb{A}^1 \times E$. For some prime $\ell > 3$, there exists $w \in W(\mathbb{F}_{q^\ell})$ such that $\pi_1(w) = z(Q_1) + z(Q_2)$ for some $Q_1, Q_2 \in R \cdot \pi_2(w)$.*

*Proof.* Let $S_1 := \pi(W(\mathbb{F}_{q^\ell}))$. Let $S_2$ be the set of $(t, P) \in (\mathbb{A}^1 \times E)(\mathbb{F}_{q^\ell})$ such that $t = z(Q_1) + z(Q_2)$ for some $Q_1, Q_2 \in R \cdot P$. We need to show that $S_1$ and $S_2$ intersect, so it will suffice to prove that

$$(3) \qquad\qquad \#S_1 + \#S_2 > \#(\mathbb{A}^1 \times E)(\mathbb{F}_{q^\ell})$$

for some prime $\ell > 3$.

By the Weil conjectures, $\#W(\mathbb{F}_{q^\ell}) = q^{\ell(\dim W)}(1 + o(1))$ as $\ell \to \infty$. Let $b$ be a bound on the number of components of the geometric fibers of $W \to \mathbb{A}^1 \times E$; then each fiber of $W(\mathbb{F}_{q^\ell}) \to (\mathbb{A}^1 \times E)(\mathbb{F}_{q^\ell})$ has size at most $(b + o(1))q^{\ell(\dim W - 2)}$. Dividing, we obtain

$$(4) \qquad\qquad \#S_1 \ge \left(\frac{1}{b} - o(1)\right) q^{2\ell}.$$

By Lemma 4.1, we can find infinitely many primes $\ell$ such that the integer $n := \#E(\mathbb{F}_{q^\ell})/\#E(\mathbb{F}_q)$ satisfies $\Psi(n) \le \frac{1}{4b}$; we assume from now on that $\ell$ satisfies this. By Lemma 4.3, the probability that a random $P \in E(\mathbb{F}_{q^\ell})$ generates $E(\mathbb{F}_{q^\ell})/E(\mathbb{F}_q)$ as an $R$-module is at least $1 - 2\Psi(n) \ge 1 - \frac{1}{2b}$. In this case, $G := R \cdot P$ has index at most $\#E(\mathbb{F}_q)$ in $E(\mathbb{F}_{q^\ell})$, so for $\ell \gg 1$, Lemma 4.5 applied to $E$ over $\mathbb{F}_{q^\ell}$ implies that

$$\{z(g_1) + z(g_2) : g_i \in G - \{\text{poles of } z\}\} = \mathbb{F}_{q^\ell}.$$

Thus

$$(5) \qquad\qquad \#S_2 \ge \left(1 - \frac{1}{2b}\right) \#E(\mathbb{F}_{q^\ell}) \cdot \#\mathbb{F}_{q^\ell} = \left(1 - \frac{1}{2b} - o(1)\right) q^{2\ell}.$$

Finally,

$$(6) \qquad \#(\mathbb{A}^1 \times E)(\mathbb{F}_{q^\ell}) = (1 + o(1)) \, q^{2\ell}.$$

Combining (4), (5), and (6) gives (3) if $\ell$ is large enough. $\qquad\qquad\square$

Suppose $L \in \mathcal{L}$. (Recall that $\mathcal{L}$ was defined at the beginning of Section 4.) Let $E$ be an elliptic curve over $k$ in Weierstrass form. For $u \in L - k$, define a degree-2 étale $L$-algebra $L_u := L \otimes_{k(u)} k(E)$ where the homomorphism $k(u) \to k(E)$ sends $u$ to the coordinate function $x \in k(E)$ for a fixed Weierstrass model, and let $E_u$ be the "quadratic twist" elliptic curve over $L$ obtained by twisting $E_L$ by the nontrivial automorphism of $L_u/L$ and the multiplication by $-1$ map $[-1]: E_L \to E_L$. (For instance, if char $k \neq 2$ and the Weierstrass model is $y^2 = f(x)$, then $E_u$ is $f(u)y^2 = f(x)$. The reason we do not restrict attention to such concrete models is that we want everything we say to hold whether or not char $k = 2$.) Define $K_u := K \otimes_{k(u)} k(E)$ similarly. So we have inclusions $k(E) \subseteq L_u \subseteq K_u$.

Let $\sigma$ be the nontrivial element of $\mathrm{Aut}(K_u/K)$. (We write Aut instead of Gal only because we do not know yet whether $K_u$ is a field.) The restriction of $\sigma$ to $k(E)$ is the nontrivial element of $\mathrm{Gal}(k(E)/k(u))$ induced by $[-1]: E \to E$. By definition of the twist $E_u$, we may identify $E_u(K)$ with

$$E(K_u)^{\sigma=-1} := \{P \in E(K_u) : {}^\sigma P = -P\}.$$

Because the $x$-coordinate map $E_L \to \mathbb{P}^1$ is invariant under the $[-1]$ map on $E_L$, it induces an $x$-coordinate on a Weierstrass model of $E_u$, and the inclusion $E_u(K) \hookrightarrow E(K_u)$ respects $x$-coordinates.

Restricting a morphism $\rho: E \to E$ to the generic point of $E$ gives a point $\bar{\rho} \in E(k(E)) \subseteq E(L_u) \subseteq E(K_u)$. If $\phi \in k(E)$, then $\phi(\bar{\rho})$ (if defined) is an element of $k(E)$ whose value at a point $P \in E(\bar{k})$ equals $\phi(\rho(P))$ (if both are defined). If moreover $\rho \in \mathrm{End}_k E$, then $\rho$ commutes with $[-1]$ on $E$, so $\sigma(\bar{\rho}) = -\bar{\rho}$, so

$$\bar{\rho} \in E(L_u)^{\sigma=-1} \subseteq E(K_u)^{\sigma=-1}.$$

**Lemma 4.7.** *For any $L \in \mathcal{L}$ and elliptic curve $E$ over $k$, there exists $u \in L - k$ such that $L_u$ and $K_u$ are fields and $E_u(K) = E_u(L)$.*

*Proof.* Let $V$ be an integral $L$-variety with function field $K$. Let $A$ be the Albanese variety of $V$. Let $A_1, \ldots, A_n$ be the distinct $L$-simple abelian varieties appearing in a decomposition of $A$ up to isogeny. Choose a nontrivial place $v$ of $L$ at which all the $A_i$ have good reduction, and choose $u$ so that $v(u) = -1$. Since $v(u)$ is negative and odd, $v$ totally ramifies in $L_u/L$; in particular $L_u$ is a field. Since $L$ is relatively algebraically closed in $K$, the algebra $K_u$ is a field too.

Now $E_u$ is a twist of $E$ by a quadratic extension $L_u/L$ in which $v$ ramifies, so $E_u$ has bad reduction at $v$. Hence $E_u$ is not isogenous to any $A_i$. Therefore every morphism $A \to E_u$ is constant. So every $L$-rational map $V \dashrightarrow E_u$ is constant. In other words, $E_u(K) = E_u(L)$. $\qquad\qquad\square$

### 4.3. **Defining subfields of transcendence degree** $1$.

**Lemma 4.8.** *Suppose $L \in \mathcal{L}$. Suppose that $E$ is an ordinary elliptic curve over $k$. Choose $u \in L - k$ as in Lemma 4.7. Let $U_1 = x(E_u(K)) - \{0\}$. Let $U_2$ be the set of $u_2 \in K$ expressible*

as $z(Q_1) + z(Q_2)$ *for some* $Q_1, Q_2 \in E(K_u) - \{poles\ of\ z\}$ *with* $x(Q_1), x(Q_2) \in U_1$. *Suppose* $c \in k^\times - k^{\times d}$. *For* $t \in K$, *we have* $t \in L$ *if and only if for all* $u_1 \in U_1$ *and* $u_2 \in U_2$

$$\langle\langle t - u_2, u_1^{-1} \rangle\rangle_d \otimes \langle 1, -c \rangle_d$$

*has a nontrivial zero over* $K$.

*Proof.* Suppose $t \in L$. By choice of $u$, we have $E_u(K) = E_u(L)$, so $U_1 \subseteq L$. The conditions $x(Q_1), x(Q_2) \in U_1$ imply $Q_1, Q_2 \in E(L_u)$, so each $u_2 \in U_2$ is algebraic over $L$, and hence in $L$. Then Proposition A.3 implies that $\langle\langle t - u_2, u_1^{-1} \rangle\rangle_d \otimes \langle 1, -c \rangle_d$ has a nontrivial zero over $L$, and hence also over $K$.

Now suppose $t \in K - L$. Thus $t$ is transcendental over $L$. All fields below will be viewed as subfields of $K_u$. We have $k(E) \subseteq L_u \subseteq K_u$. Then $k(E)(t) \subseteq K_u$ is the function field of $\mathbb{A}^1 \times E$ over $k$. Let $M_0 \subseteq K_u$ be a purely transcendental extension of $k(E)(t)$ such that $[K_u : M_0] < \infty$. Let $M$ be the relative separable closure of $M_0$ in $K_u$. Since $L_u/L$ is ramified somewhere, each of $k$, $L_u$, $K_u$ is relatively algebraically closed in the next, so $k$ is relatively algebraically closed in $M$. So there is a geometrically integral $k$-variety $W$ with function field $M$. Shrinking $W$, we may assume that the rational map $W \dashrightarrow \mathbb{A}^1 \times E$ corresponding to the extension $M$ over $k(E)(t)$ is a smooth morphism $\pi = (\pi_1, \pi_2)$ whose image is disjoint from $\mathbb{A}^1 \times E[2]$. Let $\ell$, $w$, $Q_1$, $Q_2$ be as provided by Lemma 4.6 (with $\mathbb{F}_q = k$). Let $(\tau, P) = \pi(w) \in (\mathbb{A}^1 \times E)(\mathbb{F}_{q^\ell})$. Thus $\tau = z(Q_1) + z(Q_2)$, and for $i = 1, 2$ we have $Q_i = \rho_i(P)$ for some $\rho_i \in R := \mathrm{End}_k(E)$. Let $\eta$ be a separable endomorphism of $E$ killing $P$: for instance, we could take $\eta = F^\ell - 1$. As explained before Lemma 4.7, $\bar{\eta} \in E(K_u)^{\sigma=-1}$, so $u_1 := x(\bar{\eta}) \in k(E) \subseteq K_u$. Also, the element $u_2 := z(\bar{\rho}_1) + z(\bar{\rho}_2)$ is in $U_2$. Since $P \notin E[2]$, the rational function $u_1$ on $E$ has a simple pole at $P$. The value of the rational function $t - u_2$ on $\mathbb{A}^1 \times E$ at $(\tau, P)$ is $\tau - (z(\rho_1(P)) + z(\rho_2(P))) = 0$. Thus $t - u_2, u_1^{-1}$ are a system of local parameters at $(\tau, P)$ on $\mathbb{A}^1 \times E$. We pull them back to $W$. Since $W \to \mathbb{A}^1 \times E$ is smooth, we can extend this pair to a system of local parameters at $w$ on $W$. Since the residue field of $w$ is $\mathbb{F}_{q^\ell}$ with $\ell$ prime to $d$, the form $\langle 1, -c \rangle_d$ has no nontrivial zero over $\mathbb{F}_{q^\ell}$. By Lemma A.5, the form

$$Q := \langle\langle t - u_2, u_1^{-1} \rangle\rangle_d \otimes \langle 1, -c \rangle_d$$

has no nontrivial zero over $M$. By Corollary A.2, $Q$ has no nontrivial zero over $K_u$, so it has no nontrivial zero over $K$. $\qquad\square$

**Lemma 4.9.** *There exists a definable family of subsets of $K$, defined by a formula independent of $K$, such that if $K$ is a finitely generated field of characteristic $p > 0$ and $K$ contains a primitive cube root of $1$ if $p = 2$, then all $L \in \mathcal{L}$ belong to the family.*

*Proof.* For each elliptic curve $E$ over $K$ and $u, c \in K$, let $U_1$ and $U_2$ be as in Lemma 4.8 (there we assumed we assumed $u \notin k$, but the same formulas define something for any $u$), and define $S_{E,u,c}$ to be the set of $t \in K$ such that for all $u_1 \in U_1$ and $u_2 \in U_2$,

$$\langle\langle t - u_2, u_1^{-1} \rangle\rangle_d \otimes \langle 1, -c \rangle_d$$

has a nontrivial zero over $K$. We can quantify over $E$ by quantifying over the vector of coefficients $\vec{a} = (a_1, a_2, a_3, a_4, a_6)$ of a Weierstrass equation subject to the nonsingularity constraint $\Delta(a_1, \ldots, a_6) \neq 0$. Thus $\{S_{E,u,c}\}$ is a definable family.

Given $L \in \mathcal{L}$, choose an ordinary $E$ over $k$ as in Lemma 4.4, and choose $u \in L - k$ as in Lemma 4.7. Also we can choose $c \in k^{\times} - k^{\times d}$ since either $\#k$ is odd and $d = 2$, or $\#k$ is even and $d = 3$ and $k$ contains a primitive cube root of 1. Then $S_{E,u,c} = L$ by Lemma 4.8. $\qquad \square$

**Proposition 4.10.** *There exists a definable family of subsets of $K$, defined by a formula independent of $K$, such that if $K$ is a finitely generated field of characteristic $p > 0$, the subsets in the family are exactly those in $\mathcal{L}$.*

*Proof.* Let $K' = K(\zeta)$ where $\zeta^2 + \zeta + 1 = 0$. Take the family of Lemma 4.9 for $K'$, and intersect each set with $K$. Using Theorem 2.3, retain only the sets in the family that are fields of Kronecker dimension 1. $\qquad \square$

## 5. Proofs of theorems

*Proof of Theorem 1.1.* Using Lemma 3.7 and Theorem 2.2(3), we can find a formula defining a set $S$ such that whenever $K$ is finitely generated and of characteristic 0, we get $S = \mathbb{Z}$. Use the sentence that says that $S$ is closed under addition and $S \neq 2S$ and $2 \neq 0$. This sentence is true for $S = \mathbb{Z}$, but false for any subset of a field of positive characteristic. $\qquad \square$

Now that Theorem 1.1 is proved, we may handle the characteristic 0 and $> 0$ cases separately in proving Theorems 1.2, 1.3, and 1.4.

*Proof of Theorem 1.2.* If char $K = 0$, combine Lemma 3.7 with Theorem 2.2(2). If char $K > 0$, use Theorem 2.2(2) to take the prime subfield of each member of the family given by Proposition 4.10, and take their intersection: this works as long as the family is nonempty, which holds since $K$ is infinite. $\qquad \square$

*Proof of Theorem 1.3.* If char $K = 0$, use Lemma 3.7. If char $K > 0$, the field $k$ is the set of elements belonging to the field of constants of each relatively algebraically closed subfield of transcendence degree 1: this is uniformly definable by Theorem 2.2(5) and Proposition 4.10. $\qquad \square$

*Remark* 5.1. Using Proposition 4.10 and the theorems just proved, we can also extend other results in [Rum80] to the finitely generated case. For instance, there is a formula $\phi(x, y)$ such that when $K$ is an infinite finitely generated field of characteristic $> 0$ and $x \in K$, we have $\{y \in K : \phi(x, y)\} = \mathbb{F}[x]$. The same can be done for $k[x]$ in place of $\mathbb{F}[x]$.

*Remark* 5.2. Combining our extensions of the results in [Rum80] with the undecidability of the first-order theory of $(\mathbb{N}, +, \cdot)$ (see [EFT94, Theorem X.6.9], for instance), we get also the undecidability of the first-order theory of any infinite finitely generated field.

Most of the remaining work in proving Theorem 1.4 is contained in the following lemma, whose proof is very close to that of Fact 1.3(3) in [Pop02].

**Lemma 5.3.** *For each $n \in \mathbb{N}$, there exists a formula $\phi_n(t_1, \ldots, t_n)$ in the language of fields augmented by a predicate for a subfield such that the following holds. Let $K$ be a finitely generated extension of a global field $L$, and assume $L$ is relatively algebraically closed in $K$. Then elements $t_1, \ldots, t_n \in K$ are algebraically dependent over $L$ if and only if $\phi_n(t_1, \ldots, t_n)$ holds over $K$ with the predicate corresponding to $L$.*

*Proof.* The elements $t_1, \ldots, t_n$ are algebraically dependent over $L$ if and only if they are algebraically dependent over $L(\sqrt{-1})$, so by replacing $K, L$ by $K(\sqrt{-1}), L(\sqrt{-1})$, we may reduce to the case that $\sqrt{-1} \in L$. Similarly we may assume that $L$ contains $\zeta$ satisfying $\zeta^2 + \zeta + 1 = 0$.

It will suffice to show that $t_1, \ldots, t_n$ are algebraically dependent over $L$ if and only if for all $a, b, c_1, \ldots, c_n \in L$, the form

$$q := \langle\langle t_1 - c_1, \ldots, t_n - c_n, a \rangle\rangle_d \otimes \langle 1, -b \rangle_d$$

has a nontrivial zero.

If $t_1, \ldots, t_n$ are algebraically dependent over $L$ and $a, b, c_1, \ldots, c_n \in L$, then $q$ has a nontrivial zero by Proposition A.3.

Now suppose $t_1, \ldots, t_n$ are algebraically independent over $L$. Extend to a transcendence basis $t_1, \ldots, t_N$ of $K$ over $L$. Let $M$ be the maximal separable extension of $L(t_1, \ldots, t_N)$ in $K$. Choose a smooth integral $L$-variety $W$ with function field $M$. Shrinking $W$, we may assume that $\tau := (t_1, \ldots, t_N) \colon W \to \mathbb{A}_L^N$ is an étale morphism. Choose $c := (c_1, \ldots, c_N) \in \mathbb{A}^N(L)$ in the image of $\tau$, and let $w \in W$ be a closed point in the fiber $\tau^{-1}(c)$. Then $t_1 - c_1, \ldots, t_N - c_N$ are a system of local parameters at $w$ on $W$. Let $L'$ be the residue field of $w$, so $L'$ is a finite extension of $L$. Choose a nonarchimedean place $\mathfrak{p}$ of $L$ that splits completely in $L'$, so $L'$ injects into the completion $L_\mathfrak{p}$. Choose a $\mathfrak{p}$-adic unit $b \in L$ whose residue is not a $d$-th power, and choose $a \in L$ of $\mathfrak{p}$-adic valuation 1. By Lemma A.4, $\langle\langle a \rangle\rangle_d \otimes \langle 1, -b \rangle_d$ has no nontrivial zero over $L_\mathfrak{p} \supset L'$. By Lemma A.5, $q$ has no nontrivial zero over $M$. By Corollary A.2, it also has no nontrivial zero over $K$. $\qquad\square$

*Proof of Theorem 1.4.* We may assume $n \geq 1$. If $\operatorname{char} K = 0$, Lemma 5.3 does the job. If $\operatorname{char} K > 0$, we have that $t_1, \ldots, t_n$ are algebraically dependent if either $t_1 \in k$ or there exists $L \in \mathcal{L}$ such that $t_1 \in L$ and $t_2, \ldots, t_n$ are algebraically dependent over $L$: this is uniformly definable by a formula, by Theorem 1.3, Proposition 4.10, and Lemma 5.3. $\qquad\square$

## 6. Negative results for existential definitions

In this section, we show that existential formulas cannot satisfy the requirements of Theorems 1.1, 1.2, 1.3, 1.4.

Given an existential formula, we can convert each polynomial inequality $f(x_1, \ldots, x_n) \neq 0$ to $(\exists y) f(x_1, \ldots, x_n) y = 1$ and convert each disjunction of polynomial equalities $f = 0 \vee g = 0$ to $fg = 0$. Thus we need only consider formulas given as a conjunction of polynomial equalities, preceded by existential quantifiers.

The following gives a negative result for Theorem 1.1.

**Proposition 6.1.** *There is no existential sentence that is true for $\mathbb{Q}$ and false for $\mathbb{F}_p$ for all primes $p$.*

*Proof.* If a closed subscheme $V$ of $\mathbb{A}_\mathbb{Z}^n$ has a $\mathbb{Q}$-point $P$, then it has an $\mathbb{F}_p$-point for any $p$ not dividing the denominators of the coordinates of $P$. $\qquad\square$

*Remark* 6.2. The sentence $\exists x \exists y (x^2 + y^2 + 1 = 0)$ is true for every field of positive characteristic, but false for $\mathbb{Q}$. On the other hand, any sentence true for a family of fields with infinitely many distinct characteristics must also hold for some number field: take an ultraproduct, pass to a finitely generated subfield, and specialize.

The following gives a negative result for Theorem 1.2.

**Proposition 6.3.** *There is no existential formula that defines the prime field $\mathbb{F}$ in every infinite finitely generated field $K$.*

*Proof.* Suppose such a formula exists. Then there is a closed subscheme $V$ of $\mathbb{A}^n_{\mathbb{Z}}$ such that if $\pi\colon V \to \mathbb{A}^1_{\mathbb{Z}}$ is the projection onto the first coordinate, $\pi(V(K)) = \mathbb{F}$ for every infinite finitely generated field $K$. The morphism $\pi$ must be dominant, since otherwise $\#\pi(V(K))$ would be bounded for all finitely generated $K$ of sufficiently large characteristic, while $\#\mathbb{F}$ is unbounded.

Choose an irreducible component $V_0$ of $V$ that dominates $\mathbb{A}^1_{\mathbb{Z}}$. Take $K$ to be the function field of $V_0$. The value of $\pi$ at the tautological point of $V_0(K)$ is not in $\mathbb{F}$, contradicting the assumption on $V$. $\qquad\square$

The following gives a negative result for Theorem 1.3, and hence also for the more general Theorem 1.4.

**Proposition 6.4.** *For each fixed $p \geq 0$, there is no existential formula that defines the field of constants for all finitely generated fields of characteristic $p$.*

*Proof.* Repeat the proof of Proposition 6.3, observing that the size of the field of constants is unbounded, even when we fix the characteristic. $\qquad\square$

## Appendix A. Diagonal forms

Let $d$ be a positive integer. and let $a_1, \ldots, a_n$ be elements of a field $K$. Then $\langle a_1, \ldots, a_n \rangle_d$ denotes the diagonal form

$$a_1 x_1^d + \cdots + a_n x_n^d \in K[x_1, \ldots, x_n].$$

Define the tensor product of two such forms $\langle a_1, \ldots, a_m \rangle_d$ and $\langle b_1, \ldots, b_n \rangle_d$ to be the diagonal form in $mn$ variables whose coefficients are the products $a_i b_j$. Finally, define

$$\langle\langle a \rangle\rangle_d := \langle 1, a, \ldots, a^{d-1} \rangle_d$$
$$\langle\langle a_1, \ldots, a_n \rangle\rangle_d := \langle\langle a_1 \rangle\rangle_d \otimes \cdots \otimes \langle\langle a_n \rangle\rangle_d,$$

so $\langle\langle a_1, \ldots, a_n \rangle\rangle_d$ is a diagonal degree-$d$ form in $d^n$ variables. If $d = 2$, then $\langle\langle a_1, \ldots, a_n \rangle\rangle_d$ is called a Pfister form.

**Proposition A.1.** *Let $q(x_1, \ldots, x_n)$ be a homogeneous form over a field $K$, and let $L$ be a finite extension of $K$. Suppose that either $\deg q = 2$ and $[L : K]$ is odd, or $\deg q = 3$ and $[L : K] = 2$. If $q$ has a nontrivial zero over $L$, then $q$ has a nontrivial zero over $K$.*

*Proof.* This is well known: see [Lan02, Chapter V, Exercise 28]. $\qquad\square$

**Corollary A.2.** *Let $K$ be a field. Let $d = 3$ if $\operatorname{char} K = 2$, and $d = 2$ otherwise. Let $q(x_1, \ldots, x_n)$ be a homogeneous form of degree $d$ over $K$. Let $L$ be a purely inseparable extension of $K$. If $q$ has a nontrivial zero over $L$, then $q$ has a nontrivial zero over $K$.*

*Proof.* If $q$ has a nontrivial zero over $L$, the coordinates of this zero generate a finite purely inseparable extension of $K$. By induction, we reduce to the case $[L : K] = p$, where $p := \operatorname{char} K$. Now the result follows from Proposition A.1. $\qquad\square$

**Proposition A.3.** *Let $k$ be a separably closed field, a finite field, or a number field; define $\epsilon$ to be 0, 1, or 2, respectively. Let $d = 3$ if char $k = 2$, and $d = 2$ otherwise. If $k$ is a number field, assume that $\sqrt{-1} \in k$. Let $K$ be a finitely generated extension of $k$ of transcendence degree $r$. If $n \geq r + \epsilon$ and $m \geq 2$ then for all $a_1, \ldots, a_n, b_1, \ldots, b_m \in K$, the form*

$$\langle\langle a_1, \ldots, a_n \rangle\rangle_d \otimes \langle b_1, \ldots, b_m \rangle_d$$

*has a nontrivial zero over $K$.*

*Proof.* The separably closed case reduces to the algebraically closed case by Corollary A.2. If $k$ is algebraically closed or finite, then $k$ is a $C_\epsilon$ field in the sense of [Lan52], and $K$ is a $C_{r+\epsilon}$ field, so the result follows. If $k$ is a number field, use [Pop02, Fact 1.3(1)]. $\square$

**Lemma A.4.** *Let $K$ be a field with discrete valuation $v \colon K^\times \twoheadrightarrow \mathbb{Z}$. Let $\mathcal{O}$ be the valuation ring, let $\pi \in K$ be such that $v(\pi) = 1$, and let $k = \mathcal{O}/(\pi)$. Let $d \in \mathbb{Z}_{\geq 2}$. Let $q$ be a diagonal degree-$d$ form over $\mathcal{O}$ whose reduction modulo $\pi$ has no nontrivial zero over $k$. Then the form $q' := q \otimes \langle\langle \pi \rangle\rangle_d$ has no nontrivial zero over $K$.*

*Proof.* Write

$$q' = q(\vec{x}_0) + \pi q(\vec{x}_1) + \cdots + \pi^{d-1} q(\vec{x}_{d-1}).$$

If the coordinates of $\vec{x}_0$ are in $\mathcal{O}$ and not all in $\pi\mathcal{O}$, then $v(q(\vec{x}_0)) = 0$, since $q$ has no nontrivial zero in $k$. More generally, if $\vec{x}_0$ is nonzero, it is a power of $\pi$ times such a primitive vector, so $v(q(\vec{x}_0)) \equiv 0 \pmod{d}$. Similarly, if $\vec{x}_i$ is nonzero, then $v(\pi^i q(\vec{x}_i)) \equiv i \pmod{d}$. Since these valuations are distinct (when not $+\infty$), the form $q'$ has no nontrivial zero over $K$. $\square$

The following is close to results used in [Pop02].

**Lemma A.5.** *Let $k$ be a field, and let $V$ be an integral $k$-variety with function field $K$. Suppose that $v$ is a regular point on $V$, and that $t_1, \ldots, t_m$ are part of a system of local parameters at $v$. Let $d \in \mathbb{Z}_{\geq 2}$. Let $q$ be a diagonal degree-$d$ form over $k$ having no nontrivial zero in the residue field of $v$. Then $q \otimes \langle\langle t_1, \ldots, t_m \rangle\rangle_d$ has no nontrivial zero over $K$.*

*Proof.* We may assume that $t_1, \ldots, t_m$ is a complete system of local parameters (i.e., $m = \operatorname{codim} v$). For $0 \leq j \leq m$, put $Y_j := \operatorname{Spec} \mathcal{O}_{V,v}/(t_1, \ldots, t_j)$, let $v_j$ be the generic point of $Y_j$, and let $k_j$ be the residue field of $v_j$. Thus $v_m = v$ and $k_0 = K$. For $0 < j \leq m$, the local ring of $Y_{j-1}$ at $v_j$ is a discrete valuation ring in which the image of $t_j$ is a uniformizer.

We prove by (descending) induction that for $j = m, m-1, \ldots, 0$, the form $q_j := q \otimes \langle\langle t_{j+1}, \ldots, t_m \rangle\rangle_d$ has no nontrivial zero over $k_j$. The case $j = m$ is given, and Lemma A.4 applied to the local ring of $Y_{j-1}$ at $v_j$, the form $q_j$ and the uniformizer $t_j$ provides the inductive step.

Taking $j = 0$ gives the result. $\square$

## References

[Asc04] Matthias Aschenbrenner, *Ideal membership in polynomial rings over the integers*, J. Amer. Math. Soc. **17** (2004), no. 2, 407–441 (electronic). MR2051617 (2005c:13032) ↑1.2

[CvdDM92] Zoé Chatzidakis, Lou van den Dries, and Angus Macintyre, *Definable sets over finite fields*, J. reine angew. Math. **427** (1992), 107–135. MR1162433 (94c:03049) ↑1.1

[Den78] J. Denef, *The Diophantine problem for polynomial rings and fields of rational functions*, Trans. Amer. Math. Soc. **242** (1978), 391–399. MR0491583 (58 #10809) ↑3

[EFT94] H.-D. Ebbinghaus, J. Flum, and W. Thomas, *Mathematical logic*, 2nd ed., Undergraduate Texts in Mathematics, Springer-Verlag, New York, 1994. Translated from the German by Margit Meßmer. MR1278260 (95e:03002) ↑5.2

[KR95] K. H. Kim and F. W. Roush, *Diophantine unsolvability over p-adic function fields*, J. Algebra **176** (1995), no. 1, 83–110. MR1345295 (96f:11165) ↑3

[Lan52] Serge Lang, *On quasi algebraic closure*, Ann. of Math. (2) **55** (1952), 373–390. MR0046388 (13,726d) ↑A

[Lan02] _____, *Algebra*, 3rd ed., Graduate Texts in Mathematics, vol. 211, Springer-Verlag, New York, 2002. MR1878556 (2003e:00003) ↑A

[Len96] H. W. Lenstra Jr., *Complex multiplication structure of elliptic curves*, J. Number Theory **56** (1996), no. 2, 227–241. MR1373549 (97a:11096) ↑4.1

[MB05] Laurent Moret-Bailly, *Elliptic curves and Hilbert's tenth problem for algebraic function fields over real and p-adic fields*, J. reine angew. Math. **587** (2005), 77–143. MR2186976 ↑3

[Pop02] Florian Pop, *Elementary equivalence versus isomorphism*, Invent. Math. **150** (2002), no. 2, 385–408. MR1933588 (2003i:12016) ↑1.2, 2.3, 2, 5, A, A

[Rum80] R. S. Rumely, *Undecidability and definability for the theory of global fields*, Trans. Amer. Math. Soc. **262** (1980), no. 1, 195–217. MR583852 (81m:03053) ↑2, 6, 5.1, 5.2

[Sil92] Joseph H. Silverman, *The arithmetic of elliptic curves*, Graduate Texts in Mathematics, vol. 106, Springer-Verlag, New York, 1992. Corrected reprint of the 1986 original. MR95m:11054 ↑4.2

Department of Mathematics, University of California, Berkeley, CA 94720-3840, USA

*E-mail address*: poonen@math.berkeley.edu

*URL*: http://math.berkeley.edu/~poonen