INFINITE FINITELY GENERATED FIELDS ARE BIÏNTERPRETABLE WITH $\mathbb{N}$

THOMAS SCANLON

Abstract. Using the work of several other mathematicians, principally the results of Poonen refining the work of Pop that algebraic independence is definable within the class of finitely generated fields and of Rumely that the ring of rational integers is uniformly interpreted in global fields, and a theorem on the definability of valuations on function fields of curves, we show each infinite finitely generated field considered in the ring language is parametrically biïnterpretable with $\mathbb{N}$. As a consequence, for any finitely generated field there is a first-order sentence in the language of rings which is true in that field but false in every other finitely generated field, and, hence, Pop's conjecture that elementarily equivalent finitely generated fields are isomorphic is true.

1. Introduction

Pop conjectured that if K and L are two finitely generated fields having the same first-order theories in the language of rings, then they must be isomorphic [15]. The best known result towards this conjecture is that if $K \equiv L$, then there is an embedding $K \hookrightarrow L$ making L into a finite extension of K and *vice versa* [15]. The key to the proof of this theorem is that the transcendence degree is encoded in the elementary theory of a finitely generated field. We make essential use of a refinement of this result due to Poonen that algebraic dependence is first-order definable within the class of finitely generated fields [14].

While Pop's conjecture refers directly to logic, it has been approached primarily from the standpoint of arithmetic algebraic geometry. We propose to reconnect the problem to logic though some further algebraic work is required to complete the solution.

The work on Pop's conjecture predates its formulation. Indeed, Duret studied the elementary theory of function fields of curves a full decade before Pop publicized his conjecture [3] and formulated a version of the conjecture for function fields of curves over algebraically closed fields [4]. Moreover, G. Sabbagh explicitly asked whether the class of function fields of curves over number fields could be distinguished from function fields of surfaces over number fields by a first-order sentence (see the discussion in [15]). For us, the work of Rumely [18] on definability in global fields generalizing the seminal work of J. Robinson on the rational numbers [16] is the most important precursor.

The reader might ask what relevance work on global fields could possibly have to problems in higher transcendence degree. Indeed, it is very easy to see that elementarily equivalent number fields must be isomorphic for if K is a number field, it may be expressed as $\mathbb{Q}[X]/(P)$ for some irreducible polynomial P with integer

2000 *Mathematics Subject Classification.* Primary 12L12; Secondary 03C60.
Partially supported by an NSF CAREER grant DMS-0450010.

coëfficients and any field elementarily equivalent to K must satisfy the sentence $(\exists x)P(x) = 0$. In particular, any number field elementarily equivalent to K must be expressible as an extension of K and *vice versa*.

The point is that rather than dealing only with the theory of a global field Rumely described the class of sets definable in the field showing that this class is as rich as it could possibly be for a recursively presented model. That is, using Gödel coding of sequences one may enumerate the elements of a global field in such a way that the field operations correspond to computable functions. As such, every definable set in the field must be arithmetically definable, *ie* definable in $(\mathbb{N}, +, \times)$. Rumely shows that every arithmetic set is already parametrically definable in the field. It is hard to overstate the strength of this theorem. In essence, it says that any conceivable set in a global field is definable.

We resolve Pop's conjecture by extending Rumely's theorem to infinite finitely generated fields in general. That is, we show that if K is an infinite finitely generated field regarded as a recursively presented structure, then the parametrically definable sets in K are precisely the arithmetic sets. Unlike Rumely's proof in the case of global fields, rather than first defining the family of finite sets in K and then concluding that K admits Gödel coding, we show that K can definably recognize its recursive presentation in an interpreted copy of $\mathbb{N}$. That is, we show that K is parametrically *biïnterpretable* with $\mathbb{N}$.

Our proof of the biïnterpretation theorem proceeds by induction on the transcendence degree of K with the base case coming from Rumely's work. For the inductive step, we realize K as a function field of a curve and then show via a theorem on the definability of valuations on function fields of curves that the evaluation function is definable. It follows that K can recognize its interpreted version by comparing its evaluation function with that of the interpreted field.

This paper is organized as follows. In section 2 we recall some of the formalism of interpretations. In section 3 we prove a theorem about the definability of valuations on function fields of curves. In section 4 we prove our main theorem that infinite finitely generated fields are biïnterpretable with $\mathbb{N}$. In section 5 we show how Pop's conjecture follows from the other results of this paper.

The problem of determining the isomorphism type of a finitely generated field from its first-order theory and especially our eventual solution through a biïnterpretation with the natural numbers are closely related to problem of quasifinite axiomatizability for finitely generated groups considered by A. Nies [13]. Indeed, in work independent from our own, A. Khelif employs biïnterpretations with the natural numbers in order to relatively axiomatize certain finitely generated groups and rings. After we became aware of each other's work, Khelif showed that quasifinite axiomatizability for finitely generated commutative rings follows from the main theorem of the present paper (see Théorème 8 of [10]).

Thanks are due to a number of people and institutes for their help with this project. Specifically, I thank K. Eisenträger, M. Knebusch, J. Koenigsmann, B. Poonen, F. Pop, and the other members of the working group on Pop's conjecture at the 2005 AIM meeting on Hilbert's Tenth Problem for listening to these ideas, noting errors (in this regard, F. Pop especially for noting a very serious error in an earlier verdion of this paper), and suggesting some useful references. I thank A. Khelif, F. Oger and G. Sabbagh for discussing their approaches to quasifinite axiomatizability and sharing preliminary versions of their work with me. I thank the

American Institute of Mathematics, the Isaac Newton Institute, and the organizers of the Meeting on Valuation Theory at UNICAMP for providing good working conditions. I especially thank the anonymous referees of this paper for their many useful suggestions for improvements.

2. Interpretations

In this section we recall the formalism around interpretations of one first-order structure within another. The reader may wish to consult Chapter 5 of [8] for further details.

The notions of interpretation and biïnterpretation make sense for general classes of first-order structures, but we shall restrict attention to semirings.

Definition 2.1. Let $\mathcal{L}$ be a first-order language and $\mathfrak{M}$ an $\mathcal{L}$-structure.

The semiring $(R, +, \times)$ is *(parametrically) interpreted* in $\mathfrak{M}$ if there is a definable (with parameters) set X in some Cartesian power of $\mathfrak{M}$ and a bijection $f : X \to R$ for which the inverse images of the graphs of addition and multiplication are definable (with parameters).

Remark 2.2. In the usual definition of *interpretation* one allows the map f to be merely surjective provided that the set $\{(x, y) \in X^2 \mid f(x) = f(y)\}$ is definable.

Remark 2.3. An important special case of interpretation is the case where R is a subsemiring of the ring S and R is a definable subset of S. In this case the map f is simply the identity map.

If R is interpretable in $\mathfrak{M}$, then questions about truth and definability in R may be answered in $\mathfrak{M}$. That is, if Z is a subset of some Cartesian power of R which is definable in the language of rings, then its preimage in the corresponding Cartesian power of $\mathfrak{M}$ is $\mathcal{L}_{\mathfrak{M}}$-definable. Moreover, given a sentence φ in the language of rings there is a natural way to produce an $\mathcal{L}_{\mathfrak{M}}$-sentence $\widetilde{\varphi}$ for which $R \models \varphi$ just in case $\mathfrak{M} \models \widetilde{\varphi}$. We refer to this process as *relativization*.

While it can be useful to know that one structure is interpretable in another (for instance, it follows from the fact that $\mathbb{N}$ is interpretable in $\mathbb{Q}$ that the theory of the field of rational numbers is undecidable), we need to understand families of interpretations. These come in two different flavors. It might happen that the same structure is interpreted in several other structures. We shall encounter this with the natural numbers being interpreted in infinite finitely generated fields. In the other direction, by varying the parameters used for an interpretation, we might produce families of interpreted structures. We shall use this construction to encode finite extensions of fields within a given ground field.

Notation 2.4. We use boldface variables to indicate that the variables in question might range over tuples of some fixed length.

Definition 2.5. Fix a first-order language $\mathcal{L}$ and a class $\mathcal{K}$ of $\mathcal{L}$-structures and a set $\mathcal{R}$ of semirings. We say that $\mathcal{R}$ is *uniformly interpretable* in $\mathcal{K}$ if there are formulas $\pi(\boldsymbol{u})$, $U(\boldsymbol{x}; \boldsymbol{u})$, $A(\boldsymbol{x}, \boldsymbol{y}, \boldsymbol{z}; \boldsymbol{u})$, and $P(\boldsymbol{x}, \boldsymbol{y}, \boldsymbol{z}; \boldsymbol{u})$ such that for any $K \in \mathcal{K}$ there are parameters $\boldsymbol{a}$ from K and a bijection between some $R \in \mathcal{R}$ and the set $U(K; \boldsymbol{a}) := \{\boldsymbol{x} \mid K \models U(\boldsymbol{x}; \boldsymbol{a})\}$ for which the preimage of the graphs of addition and multiplication are $A(K; \boldsymbol{a})$ and $P(K; \boldsymbol{a})$. We require moreover that for any tuple $\boldsymbol{a}$ from K for which $K \models \pi(\boldsymbol{a})$, then the above data give an interpretation of

some $R \in \mathcal{R}$ and that each $R \in \mathcal{R}$ arises from some choice of $K \in \mathcal{K}$ and parameter $\boldsymbol{a}$ from K.

We use the notion of uniform interpretability primarily in the case of the interpretation of $(\mathbb{N}, +, \times)$ in the class of infinite finitely generated fields and *vice versa*. The fact that $\mathbb{N}$ is uniformly interpretable in infinite finitely generated fields is not explicitly described in the literature. So, we explain here how to derive it from theorems of Poonen and Rumely.

Fact 2.6.
- *For each positive integer n there is a formula $\psi_n(x_1, \dots, x_n)$ in the language of rings such that for any finitely generated field K and tuple $\boldsymbol{a} = (a_1, \dots, a_n)$ from K one has $K \models \psi_n(\boldsymbol{a})$ if and only if $a_1, \dots, a_n$ is algebraically dependent over the prime field. (Theorem 1.4 of* [14]*)*
- *There is a sentence ζ in the language of rings for which if K is a finitely generated field then $K \models \zeta$ if and only if the characteristic of K is zero. (Theorem 1.1 of* [14]*)*

It follows from Fact 2.6 that every infinite finitely generated field interprets a global field. Indeed, if $\operatorname{char}(K) = 0$, then $\psi_1(K) := \{b \in K \mid K \models \psi_1(b)\}$ is a number field and if $\operatorname{char}(K) > 0$ and $t \in K$ is transcendental over the prime field, then $\psi_2(K, t) := \{b \in K \mid K \models \psi_2(b, t)\}$ is the function field of a curve over a finite field. Moreover, if we take $\theta(x; u) := [(\zeta \ \& \ \psi_1(x)) \ \vee \ (\neg\zeta \ \& \ \neg\psi_1(u) \ \& \ \psi_2(x, u))]$, then θ gives a uniform interpretation of the class of global fields in the class of infinite finitely generated fields.

To get from the global fields to $\mathbb{N}$ we use one of the main results of [18] and a construction due to R. Robinson [17].

Fact 2.7 (Theorems 2 and 3 of [18])**.** *The semiring of natural numbers is uniformly interpretable in the class of global fields. In fact, if K is a number field, then the interpreted version of $\mathbb{N}$ is actually $\mathbb{N}$ given as a substructure of K and if K is a function field of a curve over a finite field and t is any nonconstant element of K, then the interpreted version of $\mathbb{N}$ is $\{t^n \mid n \in \mathbb{N}\}$.*

Combining Fact 2.7 with the observation that global fields are uniformly interpretable in the class of infinite finitely generated fields we see that $(\mathbb{N}, +, \times)$ is uniformly interpretable in the class of infinite finitely generated fields. Indeed, by relativizing Rumely's uniform interpretation of $\mathbb{N}$ to an interpreted global field one obtains a uniform interpretation of $\mathbb{N}$ in infinite finitely generated fields.

Proposition 2.8. *The semiring of natural numbers is uniformly interpretable in the class of infinite finitely generated fields.*

It follows from this observation that the theory of an infinite finitely generated field is undecidable, but we need to say more in order to pin down the theory.

Not only do infinite finitely generated fields interpret $(\mathbb{N}, +, \times)$, but the natural numbers interpret these fields. In fact, it follows on general grounds from the theory of Gödel coding that $\mathbb{N}$ uniformly interprets all computable structures.

Proposition 2.9. *There are formulas $A(x, y, z; u)$ and $P(x, y, z; u)$ in the language of rings for which for any natural number n the set of realizations of $A(-.-, -; n)$ and of $P(-, -, -; n)$ in $\mathbb{N}$ are the graphs of binary operations $\oplus_n$ and $\otimes_n$ for which $(\mathbb{N}, \oplus_n, \otimes_n)$ is a finitely generated field. Moreover, for any infinite finitely generated field K there is a natural number $n =: [K]$ for which $(K, +, \times) \cong \widetilde{K} := (\mathbb{N}, \oplus_{[K]}, \otimes_{[K]})$.*

Proof. This proposition is a special case of the general result that recursively presented structures are definable in arithmetic. Since we shall have recourse to the form of our presentation later in the argument, we sketch the construction of A and P.

In general, if $X \subseteq \mathbb{N}^m$ is a computable (or even just recursively enumerable) set, then X is definable in the language of rings by an existential formula (see Corollary 3.7 in [9] and Chapter 6 of [12] to go from Σ_1^0 to existential). The standard bijections between $\mathbb{N}$ and $\mathbb{Z}[X_0, \ldots, X_{n-1}] =: \mathbb{Z}[\boldsymbol{X}]$ are clearly computable uniformly in n. That is, there are computable functions $\boxplus : \mathbb{N}^3 \to \mathbb{N}$ and $\boxtimes : \mathbb{N}^3 \to \mathbb{N}$ for which $(\mathbb{Z}[\boldsymbol{X}], +, \times) \cong (\mathbb{N}, \boxplus_n, \boxtimes_n)$. Given a sequence $\boldsymbol{f} = f_0, \ldots, f_{m-1} \in \mathbb{Z}[\boldsymbol{X}]$, which using the above identification of the polynomial ring with $\mathbb{N}$ and Gödel coding of sequences may be presented as a natural number, provided that the ring $\mathbb{Z}[\boldsymbol{X}]/(\boldsymbol{f})$ is infinite, there is a natural computable bijection between $\mathbb{N}$ and the ring of quotients of $\mathbb{Z}[\boldsymbol{X}]/(\boldsymbol{f})$. To see that the natural enumeration of the ring of quotients of $\mathbb{Z}[\boldsymbol{X}]/(\boldsymbol{f})$ is computable, one needs to know that one can computably test ideal membership in $\mathbb{Z}[\boldsymbol{X}]$, but this is consequence of the main theorem of [1]. Using the standard bijection between $\mathbb{N}^2$ and $\mathbb{N}$, we may encode the pair (n, code for the sequence $\boldsymbol{f}$) as a single natural number, M. If $(f_0, \ldots, f_{m-1}) \subseteq \mathbb{Z}[X_0, \ldots, X_{n-1}]$ generates a non-maximal prime ideal (which one can test computably), then we take $\oplus_M$ and $\otimes_M$ to be the operations transferred to $\mathbb{N}$ from the above mentioned bijection. Otherwise, we let $\oplus_M$ and $\otimes_M$ be the operations induced from a fixed computable bijection with $\mathbb{Q}$. □

From Propositions 2.8 and 2.9 we see that $(\mathbb{N}, +, \times)$ and infinite finitely generated fields are mutually (parametrically) interpretable. It remains to see whether they recognize this fact. That is, if K is a finitely generated field and $\widetilde{K}$ is the copy of K interpreted in the copy of $(\mathbb{N}, +, \times)$ interpreted in K, is there a *definable* (in $(K, +, \times)$) isomorphism between K and $\widetilde{K}$ and if $\widetilde{\mathbb{N}}$ is the copy of $\mathbb{N}$ interpreted in $\widetilde{K}$ is there a *definable* (in $(\mathbb{N}, +, \times)$) isomorphism between $\mathbb{N}$ and $\widetilde{\mathbb{N}}$? If these definable isomorphisms exist, then we say that K and $\mathbb{N}$ are *(parametrically) biïnterpretable*. We should note that in general parameters are necessary as $\mathbb{N}$ is rigid but finitely generated fields can have automorphisms.

In answering whether the infinite finitely generated field K and $\mathbb{N}$ are biïnterpretable, we need only worry about showing that the isomorphism between K and $\widetilde{K}$ is definable. Indeed, when K has characteristic zero, and M is a code for $\widetilde{K}$, the copy $\widetilde{\mathbb{N}}$ of $\mathbb{N}$ in $\widetilde{K}$ is identified with the set $\{\overbrace{1_K \oplus_M \cdots \oplus_M 1_K}^{n \text{ times}} : n \in \mathbb{N}\}$ which from the presentation of $\widetilde{K}$ is clearly recursive (and, hence, definable) as is the map $n \mapsto \overbrace{1_K \oplus_M \cdots \oplus_M 1_K}^{n \text{ times}}$. When K has positive characteristic, the universe of $\widetilde{\mathbb{N}}$ is the set $\{t^n \mid n \in \mathbb{N}\}$ for some (any) nonconstant element $t \in \widetilde{K}$ and the map $n \mapsto t^n$ is clearly computable, and, hence, definable in $\mathbb{N}$.

The bulk of the remainder of this paper is devoted to showing that an isomorphism between K and $\widetilde{K}$ is definable. We would have preferred to have shown that $\mathbb{N}$ is *uniformly* biïnterpretable with the class of infinite finitely generated fields, but our proof is not totally uniform. Let us note that it is possible to uniformly test whether a given formula defines an isomorphism between K and a field interpreted in $\mathbb{N}$.

Proposition 2.10. *Fix $\pi(t)$, $U(\boldsymbol{x};t)$, $A(\boldsymbol{x},\boldsymbol{y},\boldsymbol{z};t)$, and $P(\boldsymbol{x},\boldsymbol{y},\boldsymbol{z};t)$ formulas giving the uniform interpretation of $(\mathbb{N},+,\times)$ in the class of infinite finitely generated fields described above. Fix also a formula $\eta(\boldsymbol{w},\boldsymbol{x};t,\boldsymbol{u})$. Then there is another formula $\xi_\eta(t,\boldsymbol{u},M)$ for which an infinite finitely generated field K satisfies $\xi(t,\boldsymbol{u},M)$ if and only if $K\models\pi(t)$, $K\models U(M,t)$ and $\eta(K;t,\boldsymbol{u})$ is the graph of an isomorphism between $(K,+,\times)$ and the field $(U(K;t),\oplus_M,\otimes_M)$ where $\oplus_M$ and $\otimes_M$ are defined by the formulas defining them in $\mathbb{N}$ relativized to the interpreted model of $(\mathbb{N},+,\times)$.*

Proof. The construction of ξ_η is simply a matter of translating the stated requirements into the formal language. □

We note that Corollary 5 of [18] may be interpreted as saying that the natural numbers are uniformly biïnterpretable with the class of global fields.

We end our discussion of interpretation by returning to the case of encoding field extensions in a given field.

Suppose that L/K is a finite extension of K. If we fix a basis $e_1,\dots,e_d$ (with $e_1=1$) of L over K, then we may identify K^n with L via $(x_1,\dots,x_n)\mapsto\sum x_ie_i$. Of course, addition on L pulls back to coördinatewise addition on K^n whilst the multiplication operation on L pulls back to a bilinear function on K^n. If $e_ie_j=\sum\mu_{i,j,\ell}e_\ell$ for $\mu_{i,j,\ell}\in K$, then on K^N we have the definable binary function $\otimes_L:K^n\times K^n\to K^n$ given by

$$((x_1,\dots,x_n),(y_1,\dots,y_n))\mapsto(\sum_{i,j}\mu_{i,j,1}x_iy_j,\dots,\sum_{i,j}\mu_{i,j,n}x_iy_j)$$

The set of d^3-tuples for which this operation gives a field is clearly definable. Using this construction, first-order properties of degree n (or, more generally, degree $\leq n$) extensions of K may be uniformly interpreted in K.

In what follows we might quantify over the class of field extensions of some fixed degree. In so doing, we are really quantifying over the above codes for interpretations of these field extensions.

3. Defining valuations on function fields of curves

In this section we show for that fields of the form $k(C)$ where k is an infinite finitely generated field and C is an absolutely irreducible smooth curve over k the valuations $\mathrm{ord}_P:k(C)^\times\to\mathbb{Z}$ corresponding to closed points $P\in C$ are uniformly definable in a natural expansion of the language of rings as P ranges over closed points of a fixed degree. We exploit a refinement of Faddeev's theorem (generalized beyond characteristic zero by Auslander and Brumer [2]) on a local-global principle for the Brauer group of fields of rational functions [5]. Our method applies more generally than to the case of finitely generated fields of constants, though it fails in the geometric case of an algebraically closed constant field. As such, we present the definability theorem in the somewhat more abstract setting of Hilbertian constant fields and then in a later section we specialize to infinite finitely generated fields as constant fields. (See Chapters 12 and 13 of [6] for the properties of Hilbertian fields that we shall be using.) We present the proof in two parts beginning at the end by showing that (most) rational places are definable if the condition of a central simple algebra being everywhere unramified is definable and then checking that this latter fact is indeed true by performing an exercise in Galois cohomology.

Let us start by specifying our language $\mathcal{L}$, the intended interpretation of $\mathcal{L}$, and our hypotheses. $\mathcal{L}$ is an expansion of the language of rings by a unary predicate

k. We shall allow for some constant symbols. Precisely which constant symbols are required will become clear in due course. Our intended model is a field K of the form $k(C)$ where C is an absolutely irreducible curve over k for which the ring operations have their natural interpretations and k is interpreted eponymously. For the time being, our only hypothesis on k is that it is Hilbertian. We shall fix a sufficiently large prime ℓ. Here "sufficiently large" means that ℓ is not equal to the characteristic of k and the we can find generators s and t for K for which the extension $K/k(s)$ is separable, $\ell > e := [K : k(s)]$ and $\ell > [K : k(t)]$. In what follows, we shall insist that s and t are named by constants of $\mathcal{L}$ and that the coëfficients of an irreducible polynomial $F(X, Y) \in k[X, Y]$ which vanishes at (s, t) are also named by constants.

We shall define the valuations on K by considering properties of cyclic algebras over finite extensions of K. Recall that for a field L containing an ℓ^{th} root of unity ω and nonzero elements a and b, the algebra $(a, b)_\omega(L)$ is the associative unital L-algebra generated by indeterminates α and β subject to the relations $\alpha^\ell = a$, $\beta^\ell = b$, and $\beta\alpha = \omega\alpha\beta$. The algebra $(a, b)_\omega(L)$ is a central simple algebra over L and gives rise to an element of the Brauer group of L of order ℓ (or 1 if it splits).

If (L, v) is a discretely valued field with residue field $L(v)$ containing an ℓ^{th} root of unity ω, then there is homomorphism (which we shall describe cohomologically below) $r = r_v : \mathrm{Br}(L)_\ell \to \mathrm{Hom}_{\mathrm{cont}}(\mathrm{Gal}(L(v)^{\mathrm{sep}}/L(v)), \mathbb{Z}/\ell\mathbb{Z})$ from the ℓ-torsion of the Brauer group of L to the group of continuous homomorphisms from the absolute Galois group of the residue field to $\mathbb{Z}/\ell\mathbb{Z}$. We say that a central simple algebra D over L is *unramified* if $r([D]) = 0$ where $[D]$ is the class of D in $\mathrm{Br}(L)_\ell$.

In case $D = (a, b)_\omega(L)$, we have an explicit computation of $r([D])$. From the Kummer exact sequence and the map $\mathbb{Z}/\ell\mathbb{Z} \to \mu_\ell$ given by $1 \mapsto \omega$, we have an isomorphism

$$\mathrm{Hom}_{\mathrm{cont}}(\mathrm{Gal}(L(v)^{\mathrm{sep}}/L(v)), \mathbb{Z}/\ell\mathbb{Z}) \cong \mathrm{Hom}_{\mathrm{cont}}(\mathrm{Gal}(L(v)^{\mathrm{sep}}/L(v)), \mu_\ell) \cong L(v)^\times/(L(v)^\times)^\ell$$

Via this identification, $r([D]) = \overline{a^{v(b)}/b^{v(a)}}(L(v)^\times)^\ell \in L(v)^\times/(L(v)^\times)^\ell$ where by $\overline{x}$ we mean the reduction of x in the residue field.

When $L = k'(C')$ is the function field of an absolutely irreducible curve over the field k' and $D \in \mathrm{Br}(L)_\ell$, then we say that D is *everywhere unramified* if for every closed point $P \in C'$ we have $r_P(D) := r_{\mathrm{ord}_P}(D) = 0$. In the special case that $C' = \mathbb{P}^1_{k'}$ is the projective line and $L = k'(\mathbb{P}^1)$, then the theorem of Faddeev asserts that $D \in \mathrm{Br}(L)_\ell$ is everywhere unramified just in case D is in the image of $\mathrm{Br}(k) \to \mathrm{Br}(L)$. Evidently, the condition of being Brauer equivalent to an algebra defined over the constants is an $\mathcal{L}$-definable condition. Examining the calculations behind Faddeev's theorem, we will observe at the end of this section that the condition of being everywhere unramified is always $\mathcal{L}$-definable.

It is important for our applications that one can uniformly define the condition of some algebra being everywhere unramified even as the base field varies. Before we can state this theorem in its uniform version we need to say a little something about how one recovers from a presentation of a finite extension L of K as a field a presentation of L as $k'(C')$ where k'/k is a finite extension and $C' \to C_{k'}$ is a curve lying over $C_{k'}$. If $[L : K] = d$ and L is presented with a basis over K, then k', the relative algebraic closure of k in L, is $\mathcal{L}$-definable as $\{a \in L : (\exists \alpha_0, \ldots, \alpha_{d-1} \in k)\ a^d + \sum \alpha_i a^i = 0\}$. Of course, the map of smooth projective curves $C' \to C_{k'}$ is uniquely determined by the field extension $K \hookrightarrow L$, but it might not be possible to

definably produce a system of equations of C' and for this map. However, we can find a definable set of presentations of C'. For instance, the presentations could be given by the set of tuples $(u_1, \beta_{0,1}, \ldots, \beta_{e_1,1}, u_2, \boldsymbol{\beta}_2, \ldots, u_m, \beta_{0,m}, \ldots, \beta_{e_m,m})$ for some $m < d$ and $e_i \leq d$ where $u_{i+1} \in L$ has maximal degree (> 1) over $K(u_1, \ldots, u_i)$ and its minimal monic polynomial is $x^{e_{i+1}+1} + \sum \beta_{i+1,j} x^j$. The point is that from a presentation of L as a field over K of some bounded degree, we can recover in a first-order way its presentation as $k'(C')$. As a consequence, $\mathcal{L}$ may access basic properties of the pair (C', k'). For example, the property of $C'(k')$ being nonempty is a first-order property of L (or, really, of the presentation of L as a finite extension of K of some bounded degree). We shall say that L *has a rational point* if $C'(k') \neq \varnothing$.

We may now state our theorem on the uniform definability of being everywhere unramified.

Theorem 3.1. *Relative to the usual encodings of field extensions and finite dimensional algebras, for each natural number d the following set is $\mathcal{L}$-definable.*

$$\begin{aligned}\Upsilon(d; K) := \quad \{(L, D) : \quad & L/K \text{ is an extension of degree dividing } d,\\ & L \text{ has a rational point, and}\\ & D \text{ is an everywhere unramified central simple algebra}\\ & \quad \text{of dimension } \ell^2 \text{ over } L\}\end{aligned}$$

We delay the proof of Theorem 3.1 until the end of this section and show now how the main result of this section follows from this theorem.

Theorem 3.2. *Evaluation at affine points of C is $\mathcal{L}$-definable. That is, for any natural number d the set*

$$\begin{aligned}E(d; K) := \quad \{(k', f, a, b, Q) : \quad & [k' : k] \mid d,\\ & a, b \in k'\\ & f \in K,\\ & F(a, b) = 0,\\ & f(a, b) = Q \in \mathbb{P}^1(k')\}\end{aligned}$$

is $\mathcal{L}$-definable.

Remark 3.3. Our hypothesis in Theorem 3.2 that k is Hilbertian is certainly too strong. We conjecture that it may be replaced by the hypothesis simply that k is not separably closed. Moreover, the method of proof presented here should adapt to the case that k is merely neither separably nor real closed.

Before launching into the proofs of Theorems 3.1 and 3.2, we note a simple reductions.

Lemma 3.4. *Theorems 3.1 and 3.2 follow from the case in which k contains a primitive ℓ^{th} root of unity, ω.*

Proof. If L is an extension of K and $D \in \mathrm{Br}(L)_\ell$, then as $[L(\omega) : L] < \ell$, $D \otimes_L L(\omega)$ is everywhere unramified if and only if D is everywhere unramified.

In the case of Theorem 3.2, if M is any finite extension of K presented as a finite dimensional vector space over K with a bilinear form and an embedding $K \hookrightarrow M$, then $E(d; K)$ may be identified with $\{(k', f, a, b, Q) \in E(d; M) : k' \subseteq K \text{ and } f \in K\}$. □

Thus, henceforth we assume that k contains a primitive ℓ^{th} root of unity ω and that ω is named by a constant of $\mathcal{L}$.

Of course, on general grounds, defining evaluation at the point $P = (a, b)$ is equivalent to defining the valuation ord_P and this in turn is equivalent to defining the condition $\ell \mid \text{ord}_P(f)$. It is this last condition we shall concentrate on defining.

To ease notation, in the following formula we write Υ for $\Upsilon(e!d\ell^{2(e+1)}; K)$.

Consider the following formula.

$$\begin{aligned}
\varphi(k', a, b, f) \quad := \quad & [k' : k] \mid d, \\
& a, b \in k' \\
& F(a, b) = 0, \\
& f \in K^\times, \\
& \text{so that writing } k'' \text{ for the splitting field of } F(a, Y) \\
& \quad \text{and } K'' \text{ for the Galois extension of } Kk'' \text{ obtained by adjoining} \\
& \quad \sqrt[\ell]{s - (a+1)} \text{ and } \sqrt[\ell]{t - \beta} \text{ for each solution } \beta \text{ of } F(a, Y) = 0 \text{ other than } b, \\
& \exists L' \text{ an extension of } K'' \text{ of degree dividing } \ell, \\
& \exists \widetilde{k} \text{ an extension of } k'' \text{ of degree dividing } e\ell^{e+1} \\
& \exists \pi \in k^\times \text{ so that if } L = \widetilde{k}L', \\
& \quad (L, (f, \pi)_\omega(L)) \in \Upsilon \text{ and} \\
& \quad (L, (s - a, \pi)_\omega(L)) \notin \Upsilon
\end{aligned}$$

Given Theorem 3.1 and the standard encodings of field extensions, it is an easy matter to check that φ may be expressed in $\mathcal{L}$.

We start by checking that when $\varphi(k', a, b, f)$ holds, $\text{ord}_{(a,b)}(f) \equiv 0 \pmod{\ell}$.

Lemma 3.5. *If $\varphi(k', a, b, f)$ holds, then $\text{ord}_{(a,b)}(f) \equiv 0 \pmod{\ell}$.*

Proof. Let L and π be chosen so as to witness $\varphi(k', a, b, f)$.

The algebra $((s - a), \pi))_\omega(k(s))$ ramifies only at a and at ∞. As $\ell > e = [K : k(s)] = [Kk'' : k''(s)]$, $(s - a, \pi)_\omega(Kk'')$ ramifies exactly at the places lying above a and ∞. As the extension K''/Kk'' ramifies to degree ℓ over each of the places $\text{ord}_{(a,\beta)}$ (for β a root of $F(a, Y)$ different from b) and each place at infinity, $(s - a, \pi)_\omega(K'')$ ramifies at the places lying over $\text{ord}_{(a,b)}$ and nowhere else.

As $(s - a, \pi)_\omega(L)$ is not everywhere unramified, there is some valuation w lying over $\text{ord}_{(a,b)}$ for which $r_w([((s - a), \pi)_\omega(L)]) \neq 0$. Thus, $w(s - a)$ is not divisble by ℓ and π is not an ℓ^{th} power in the residue field $L(w)$. In particular, the ramification degree of w over $\text{ord}_{(a,b)}$ is prime to ℓ.

By hypothesis, $r_w([(f, \pi)_\omega(L)]) = 0$ so that the residue of $\pi^{-w(f)}$ is an ℓ^{th} power in $L(w)$. By the above considerations, this is only possible if $w(f)$ is divisible by ℓ. As the ramification degree of w over $\text{ord}_{(a,b)}$ is prime to ℓ, we must have $\text{ord}_{(a,b)}(f) \equiv 0 \pmod{\ell}$. □

With the next lemma we establish a basic property of Hilbertian fields needed for the proof of a converse to Lemma 3.5. The main point is that for Hilbertian constant fields we may adjoin points to curves without solving specified radical equations.

Lemma 3.6. *Let E be a Hilbertian field, X an absolutely irreducible curve over E, $f : X \to \mathbb{P}^1_E$ a separable map of degree d, $\Sigma \subseteq X$ a finite set of closed points, and*

$\pi \in E^\times$ which is not *an ℓ^{th} power in $E(P)$, the residue field at P, for any $P \in \Sigma$. Then there is an extension field E' of E with $X(E') \neq \varnothing$, $[E' : E] = d$, and P is still not an ℓ^{th} power in any of the residue fields $E'(P)$ for P a closed point of $X_{E'}$ lying over some $P \in \Sigma$.*

Proof. Regarding each of the residue fields $E(P)$ as P runs through Σ as subfields of an algebraic closure of E, we may form M, a compositum of these $E(P)$. Let $N := M(\sqrt[\ell]{\pi})$. By the primitive element theorem, we may express the field extension corresponding to $f : X \to \mathbb{P}^1_E$ as $E(t) = E(\mathbb{P}^1) \hookrightarrow E(X) = E(t)[y]/(g(t,y))$ where $g(t,y) \in E[t,y]$ is a polynomial which remains irreducible even in $E^{\mathrm{alg}}[t,y]$. As E is Hilbertian, there is some $a \in E$ for which $g(a,y)$ is an irreducible polynomial of degree d in $N[y]$. Let $E' := E[y]/(g(a,Y))$. For each $P \in \Sigma$, $g(a,y)$ is irreducible over $E(P)(\sqrt[\ell]{\pi})$. Thus, calculating the degree of the field extension $[E'(P)(\sqrt[\ell]{\pi}) : E(P)]$ in two ways, we see that $[E'(P)(\sqrt[\ell]{\pi}) : E'(P)] = \ell$. □

We prove now a converse to Lemma 3.5.

Lemma 3.7. *Let k'/k be an extension of degree dividing d, $f \in K^\times$, $P = (a,b) \in C(k')$ a k'-rational affine point of C and suppose that $\mathrm{ord}_P(f) \equiv 0 \pmod{\ell}$, then $\varphi(k', a, b, f)$ holds in K.*

Proof. There are exactly ℓ places rational over k' lying over ord_a in $k'(\sqrt[\ell]{s-(a+1)})$. As $\ell > [K : k(s)] = [Kk' : k'(s)] = [Kk'(\sqrt[\ell]{s-(a+1)}) : k'(\sqrt[\ell]{s-(a+1)})]$, it follows that for any place Q of $Kk'(\sqrt[\ell]{s-(a+1)})$ lying over ord_a any element of k' which is an ℓ^{th} power at Q was already an ℓ^{th} power in k'.

Let k'' be the splitting field of $F(a,Y)$ over k'. Choose $\pi \in k^\times$ so that π is not in the multiplicative group generated by the ℓ^{th} powers and $(b-\beta)$ for β ranging over the roots of $F(a,Y)$ different from b. As k is Hilbertian, $k^\times/(k^\times)^\ell$ is infinite so that such a π is guaranteed to exist.

Let $\Sigma \subseteq \mathrm{Spec}(k''[s,t]/(F))$ be the set of primes at which $(f,\pi)_\omega(k''K)$ ramifies. For each $\mathfrak{p} \in \Sigma$ let $h_\mathfrak{p} \in k''[s,t]$ be a representative of $r_\mathfrak{p}([(f,\pi)_\omega(k''K)]) \in k''(\mathfrak{p})^\times/(k'(\mathfrak{p})^\times)^\ell$. By the Chinese remainder theorem as $P \notin \Sigma$, we can find some $h \in k'[s,t]/(F)$ with $h(P) = 1$ and $h - h_\mathfrak{p} \in \mathfrak{p}$ for $\mathfrak{p} \in \Sigma$.

Let L' be the extension of $k''K$ obtained by adjoining $\sqrt[\ell]{h}$, $\sqrt[\ell]{s-(a+1)}$, and $\sqrt[\ell]{t-\beta}$ for each root β of $F(a,Y)$ different from b.

By Kummer theory, π not an ℓ^{th} power in $L'(Q)$ for any place Q of L' lying over P. By Lemma 3.6 we may find a constant field extension L/L' of degree $e\ell^{e+1}$ for which the associated curve has a rational point and π is still not an ℓ^{th} power at the places lying over P. By construction, every place of L over P is unramified. Hence, $(s-a,\pi)_\omega(L)$ is *not* everywhere unramified.

On the other hand, $(f,\pi)_\omega(L)$ is everywhere unramified. Indeed, $(f,\pi)_\omega(k'K)$ is ramified only at elements of Σ and possibly at places lying over ∞. Since, every place of L lying above ∞ ramifies to a degree divisible by ℓ while the residue of $h_\mathfrak{p}$ is an ℓ^{th} power at each place lying above $\mathfrak{p} \in \Sigma$, we see that $(f,\pi)_\omega(L)$ is everywhere unramified. □

With these two lemmata in place we may finish the proof of Theorem 3.2.

Proof. From Lemma 3.5 and Lemma 3.7 and using the fact that $1 \leq \mathrm{ord}_{(a,b)}(s-a) < \ell$ as $[K : k(s)] < \ell$, it is easy to see that $(k', f, a, b, Q) \in E(d; K)$ if and only if each

of the components of the quintuple is of the right type and either $Q = \infty$ and $\varphi(k', a, b, f^\ell + (s-a)^{-1})$ or $Q \in k'$ and $\varphi(k', a, b, (f-Q)^{-\ell} + (s-a))$. □

We must now pay our debt to Galois cohomology with a proof of Theorem 3.1. Most of the essential features of our proof appear already in the proof of Faddeev's theorem and the reader may wish to consult Section 6.4 of [7] for more details.

In analyzing $\Upsilon(d; K)$ we must consider field extensions L/K of degree dividing d. As discussed above, such extensions may be expressed as $k'(C')$ where k' is relatively algebraically closed in L and k'/k is itself an extension of fields of degree dividing d and C' is a curve over k' admitting a map $C' \to C_{k'}$ of degree dividing d and presentations of such may be recovered $\mathcal{L}$-definably. From the Riemann-Hurwitz formula we see that there is a bound g just depending on K and d so that for any field extension L/K of degree dividing d if we express L as $k'(C')$ with C' smooth and projective, then the genus of C' is at most g.

For the time being, fix one such extension $L = k'(C')$. In order for (L, D) to belong to $\Upsilon(d; K)$, we must have $C'(k') \neq \varnothing$. Let $G := \mathrm{Gal}(k'^{\mathrm{sep}}/k')$ be the absolute Galois group of k'. To compress the notation, when A is a G-module we write $H^i(A)$ for $H^i(G, A)$, the i^{th} Galois cohomology group of A unless we need to indicate G. As usual, Galois cohomology is defined in terms of continuous cocycles and when we speak of homomorphisms between profinite groups we mean continuous homomorphisms.

A standard calculation (see section 6.4 of [7]) shows that

$$H^i(\mathrm{Div}(C'_{k'^{\mathrm{sep}}})) = \bigoplus_{P \in C'} H^i(\mathrm{Gal}(k'(P)^{\mathrm{sep}}/k'(P)), \mathbb{Z})$$

for $i \geq 0$ and

$$H^i(\mathrm{Div}(C'_{k'^{\mathrm{sep}}})) = \bigoplus_{P \in C'} H^{i-1}(\mathrm{Gal}(k'(P)^{\mathrm{sep}}/k'(P)), \mathbb{Q}/\mathbb{Z})$$

for $i \geq 2$. In particular, $H^1(\mathrm{Div}(C'_{k'^{\mathrm{sep}}})) = 0$ and $H^2(\mathrm{Div}(C'_{k'^{\mathrm{sep}}})) = \bigoplus_{P \in C'} X(P)$ where to ease notation, for $\mathrm{Hom}_{\mathrm{cont}}(\mathrm{Gal}(k'(P)^{\mathrm{sep}}/k'(P)), \mathbb{Q}/\mathbb{Z})$, the local character group, we have written $X(P)$.

As $C'(k') \neq \varnothing$, the degree sequence

$$0 \longrightarrow \mathrm{Div}^0(C'_{k'^{\mathrm{sep}}}) \longrightarrow \mathrm{Div}(C'_{k'^{\mathrm{sep}}}) \xrightarrow{\deg} \mathbb{Z} \longrightarrow 0 \tag{1}$$

splits so that $H^i(\mathrm{Div}(C'_{k'^{\mathrm{sep}}})) = H^i(\mathrm{Div}^0(C'_{k'^{\mathrm{sep}}})) \oplus H^i(\mathbb{Z})$ for every $i \geq 0$. Thus, $H^1(\mathrm{Div}^0(C'_{k'^{\mathrm{sep}}})) = 0$ and $H^2(\mathrm{Div}^0(C'_{k'^{\mathrm{sep}}}))$ may be identified with a direct summand of $\bigoplus_{P \in C'} X(P')$.

Using these calculations, from the long exact sequence expressing the Jacobian of a curve as a quotient of the group of degree zero Weil divisors by the divisors of rational functions

$$1 \longrightarrow k'^{\mathrm{sep}}(C')^\times / k'^{\mathrm{sep}\times} \longrightarrow \mathrm{Div}^0(C'_{k'^{\mathrm{sep}}}) \longrightarrow J_{C'}(k^{\mathrm{sep}}) \longrightarrow 0 \tag{2}$$

we obtain our most important exact sequence

$$0 \longrightarrow H^1(J_{C'}(k'^{\mathrm{sep}})) \xrightarrow{\delta} H^2(k'^{\mathrm{sep}}(C)^\times / k'^{\mathrm{sep}\times}) \longrightarrow \bigoplus_{P \in C'} X(P) \tag{3}$$

Since $C'(k') \neq \varnothing$, the quotient sequence

$$1 \longrightarrow k'^{\mathrm{sep}\times} \longrightarrow k'^{\mathrm{sep}}(C')^\times \longrightarrow k'^{\mathrm{sep}}(C')^\times/k'^{\mathrm{sep}\times} \longrightarrow 1 \tag{4}$$

splits. Indeed, if $Q \in C'(k')$ and $u_Q \in k'(C')^\times$ is a uniformizer at Q, then the map $k'^{\mathrm{sep}}(C')^\times \to k'^{\mathrm{sep}\times}$ given by $f \mapsto (f/u_Q^{\mathrm{ord}_Q(a)})(Q)$ is a splitting. Thus, in particular, we have $H^2(k'^{\mathrm{sep}}(C')^\times/k'^{\mathrm{sep}\times}) = H^2(k'^{\mathrm{sep}\times}) \oplus H^2(k'^{\mathrm{sep}}(C')^\times)$.

By Tsen's theorem, we may identify the ℓ-torsion of the Brauer group of $k'(C')$ with the ℓ-torsion of $H^2(k'^{\mathrm{sep}}(C')^\times))$. Thus, we have $\mathrm{Br}(k'(C'))_\ell = \mathrm{Br}(k)_\ell \oplus H^2(k'^{\mathrm{sep}}(C')^\times/k'^{\mathrm{sep}\times})_\ell$. Composing the second projection map with the last map in Sequence 3, we obtain a morphism $\mathrm{Br}(k'(C'))_\ell \to \bigoplus_{P\in C'} X(P)$. Up to sign, the individual components of this map may be identified with the maps r_P already discussed. In other words, the kernel of this map is the set of classes in the Brauer group of everywhere unramified algebras. From Sequence 3, we see that $[D] \in \mathrm{Br}(k'(C'))_\ell$ is everywhere unramified just in case its image in $H^2(k^{\mathrm{sep}\prime}(C')^\times/k'^{\mathrm{sep}\times})$ is also in the image of δ. Our task is to show that the image of δ may be recognized definably.

The objects we have been considering up to this point (*eg* $H^2(k'^{\mathrm{sep}}(C')^\times/k'^{\mathrm{sep}\times})$, $\mathrm{Div}^0(C'_{k'^{\mathrm{sep}}})$, *et cetera*) are not directly accessible to $\mathcal{L}$. However, some of them may be approximated well enough by definable sets so that the relevant conditions may be expressed. In some sense, $\mathrm{Div}(C')$ and $k'(C')$ and the map $\mathrm{div} : k'(C')^\times \to \mathrm{Div}(C')$ are *ind*-definable in $(k, +, \times)$. For instance, for each pair of natural numbers n and m, we may identify $\Delta_{m,n}(k') := (\mathrm{Sym}^m(C') \times \mathrm{Sym}^n(C'))(k')$ with degree $(m-n)$ divisors on C' via $([(P_1, \ldots, P_m)], [(Q_1, \ldots, Q_n)]) \mapsto \sum(P_i) - \sum(Q_j)$. In so doing, $\mathrm{Div}(C') = \bigcup \Delta_{m,n}(k')$ and the group operations on the group of divisors when restricted to finite subunions of these definable sets may be expressed as a finite union of definable functions. Likewise, by stratifying $k'(C')$ by the total degrees of the representing polynomials, we may express $k'(C')$ as a countable union of definable sets, $\Xi_n(k')$. What may be a little less obvious, is that for each natural number n there is another number $m = m(n)$ so that $\mathrm{div}(\Xi_n(k')) \subseteq \bigcup_{i\leq m} \Delta_{i,i}(k')$ and for each M there is an $N = N(M)$ so that $\mathrm{div}(k'(C')) \cap \Delta_{M,M}(k') = \mathrm{div}(\bigcup_{i\leq N} \Xi_i(k')) \cap \Delta_{M,M}(k')$. To find these bounds, recall that we have access to a presentation of (most of) C' as an affine curve. For any $f \in \Xi_n(k')$, we may express the effective part of $\mathrm{div}(f)$ as the intersection $C' \cap V(f)$, whose degree we may bound in terms of the presentation of C' and f. Likewise, the polar part of the divisor may be similarly bounded. It is important to note here that these bounds depend only on the shape of the affine embedding of C' and so for us are uniform across the field extensions L/K we are now considering.

As long as we can access the G-module A definably we may understand $H^i(A)$ provided that we may bound the degree of a Galois field extension k''/k' from which the relevant elements of the cohomology group arise via restriction. More precisely, if k''/k' is a finite Galois extension and A is a definable $\mathrm{Gal}(k''/k')$-module, then one sees that the cohomology group $H^i(\mathrm{Gal}(k''/k'), A)$ is definable simply by expressing it as the quotient of the group of i-cocyles, itself a definable subgroup of a certain Cartesian power of A, by the group of coboundaries. Likewise, the various maps in the long exact cohomology sequence associated to a short exact sequence of definable $\mathrm{Gal}(k''/k')$-modules are definable. Now, if we are given an exact sequence merely of ind-definable $\mathrm{Gal}(k''/k)$-modules, the connecting homomorphisms

might not be definable, but we can definably describe the image of the connecting homomorphism when restriced to some definable chunk of the cohomology group provided that we can demonstrate that the various liftings required in the proof of the snake lemma may be chosen from a fixed definable set. This is exactly what we shall do.

We need to recognize those elements of $H^2(k'^{\mathrm{sep}}(C')^\times/k'^{\mathrm{sep}\,\times})_\ell$ which are also in the image of δ. As δ is injective, it suffices to consider the image of δ on $H^1(J_C(k'^{\mathrm{sep}}))_\ell$. From the long exact sequence associated to the multiplication by ℓ on $J_C(k'^{\mathrm{sep}})$ sequence, we see that $H^1(J_C(k'^{\mathrm{sep}}))_\ell$ is the image of $H^1(J_C[\ell](k'^{\mathrm{sep}}))$, the cohomology of the ℓ-torsion of the Jacobian. Hence, it suffices to compute the image of δ restricted to $H^1(J_C[\ell](k^{\mathrm{sep}}))$.

Let $k'' := k'(J_{C'}[\ell](k'^{\mathrm{sep}}))$ be the field generated by the ℓ-torsion points of the Jacobian of C' and let $H := \mathrm{Gal}(k''^{\mathrm{sep}}/k'')$ be the absolute Galois group of k''. Writing A for $J_{C'}[\ell](k'^{\mathrm{sep}})$, we have an exact sequence describing $H^1(G, J_{C'}[\ell](k'^{\mathrm{sep}}))$ (see Proposition 4 of Section 6 of Chapter VII of [19])

$$0 \longrightarrow H^1(G/H, A) \longrightarrow H^1(G, A) \longrightarrow H^1(H, A)^{G/H} \tag{5}$$

From Sequence 5 we see that for each $\eta \in H^1(J_{C'}[\ell](k'^{\mathrm{sep}}))$ there is some Galois extension $\widetilde{k}$ of k'' of degree dividing ℓ^{2g} so that η lies in the image of the map $H^1(\mathrm{Gal}(\widetilde{k}/k'), A) \hookrightarrow H^1(G, A)$.

Fix now an isomorphism $(\mathbb{Z}/\ell\mathbb{Z})^{2g} \cong J_C[\ell](k'^{\mathrm{sep}})$ and representatives in $\Delta_{g,g}(k'') \subseteq \mathrm{Div}^0(C'_{k''})$ of the ℓ-torsion of the Jacobian of C', $\{a_\gamma\}_{\gamma\in(\mathbb{Z}/\ell\mathbb{Z})^{2g}}$. For each pair γ_1 and γ_2 in $(\mathbb{Z}/\ell\mathbb{Z})^{2g}$, the divisor $a_{\gamma_1} + a_{\gamma_2} - a_{\gamma_1+\gamma_2}$ is rationally equivalent to zero so we may find some $f_{\gamma_1,\gamma_2} \in \Xi_{\leq M(3g)}(k'')$ with $\mathrm{div}(f_{\gamma_1,\gamma_2}) = a_{\gamma_1} + a_{\gamma_2} - a_{\gamma_1+\gamma_2}$. Of course, these particular choices of a_γ and f_{γ_1,γ_2} are not uniformly definable, but the set of such tuples is definable, uniformly as we vary L. Using these choices of a_γ and f_{γ_1,γ_2} and the snake lemma, we may uniformly compute $\delta(\psi)$ for $\psi \in H^1(\mathrm{Gal}(\widetilde{k}/k'), J_C[\ell](k'^{\mathrm{sep}}))$ as $\widetilde{k}$ ranges through the set of Galois extensions of k'' of degree dividing ℓ^{2g}.

With all this in place, we may define the condition of the central simple algebra D of dimension ℓ^2 over L being everywhere unramified. Namely, D is everywhere unramified if and only if there is an algebra $D' \in \mathrm{Br}(k')_\ell$ and a Galois field extension $\widetilde{k}$ of k'' of degree dividing ℓ^{2g} and some $\psi \in H^1(\mathrm{Gal}(\widetilde{k}/k'), J_C[\ell](\widetilde{k}))$ for which $\delta(\psi)$ is equal to the image of $(D\otimes_k D')$ in $H^2(\mathrm{Gal}(\widetilde{k}/k'), \widetilde{k}(C')^\times/\widetilde{k}^\times)$ under the composition of the natural maps $H^1(\mathrm{Gal}(\widetilde{k}/k'), \mathrm{PGL}_{\ell^2}(\widetilde{k}(C'))) \to H^2(\mathrm{Gal}(\widetilde{k}/k'), \widetilde{k}(C')^\times) \to H^2(\mathrm{Gal}(\widetilde{k}/k), \widetilde{k}(C)^\times/\widetilde{k}^\times)$.

With this we conclude the proof of Theorem 3.1 and hence also of Theorem 3.2.

4. Main theorem

In this section we prove our main theorem that if K is a finitely generated field, then K is parametrically biïnterpretable with the semiring of natural numbers. Our proof proceeds by induction on the transcendence degree of K and as such is not uniform. As we demonstrate in the following section, Pop's conjecture and Poonen's refined conjecture on the relative finite axiomatization of a finitely generated field follow from the main theorem of this section, but Poonen's stronger conjecture that

any arithmetic class of finitely generated infinite fields is axiomatized by a single sentence remains open.

Theorem 4.1. *If K is an infinite finitely generated field, then K is biinterpretable in the language of rings with constants for the elements of K with $(\mathbb{N}, +, \times)$.*

Proof. We work by induction on the transcendence degree of K beginning with transcendence degree zero in characteristic zero and transcendence degree one in positive characteristic. This base case is (properly interpreted) already Corollary 5 of [18].

Our work begins with transcendence degree $n+1$ where n is at least 1 if the characteristic is positive.

Let $a_1, \dots, a_n \in K$ be n algebraically independent elements of K. Let

$$k := \{u \in K \mid K \models \psi_{n+1}(u, a_1, \dots, a_n)\}$$

be the relative algebraic closure of the field generated by $a_1, \dots, a_n$ in K which is defined using Poonen's formula ψ_{n+1} which describes algebraic dependence amongst $n+1$-tuples. Let C be a smooth projective curve over k for which $K = k(C)$.

By induction, k is biinterpretable with a standard copy of $\mathbb{N}$. Thus, every arithmetically definable set in any power of k is parametrically definable in k. Choose s and t in K for which $K/k(s)$ is a separable extension of fields of degree e and $t \notin k$. Let $F(X, Y) \in k[X, Y]$ be an irreducible polynomial satisfied by (s, t). Then, using the parameters s, t, the coëfficients of F, and the parameters already specified to name k and give its biinterpretation with $\mathbb{N}$, we may regard K as a a structure for the language considered in Section 3.

Let $\widetilde{K} = (\mathbb{N}, \oplus_{[K]}, \otimes_{[K]})$ be the interpreted copy of K corresponding to the presentation $a_1, \dots, a_n, s, t; F$.

The set

$$\widetilde{E}(e!; \widetilde{K}) := \{(k', \widetilde{f}, a, b, Q) \mid [k' : k] \mid e!, (a, b) \in C(k'), Q \in \mathbb{P}^1(k'), \widetilde{f} \in \widetilde{K}, \widetilde{f}(a, b) = Q\}$$

is computable, and, hence, definable in k. By Theorem 3.2 the set

$$E(e!; K) := \{(k', a, b, f, Q) \mid [k' : k] \mid e!, (a, b) \in C(k'), f \in K, f(a, b) = Q \in \mathbb{P}^1(k')\}$$

is definable. As there are infinitely many k'-rational points on C as k' varies through the extensions of degree dividing $e!$ and rational functions on curves which agree at infinitely many points are identical, the association

$$\begin{aligned} f \mapsto \widetilde{f} \quad \Leftrightarrow \quad & (\forall k'/k \text{ of degree dividing } e!)(\forall (a, b) \in C(k'))(\forall Q \in \mathbb{P}^1(k')) \\ & [(k', f, a, b, Q) \in E(e!; K) \to (k', \widetilde{f}, a, b, Q) \in \widetilde{E}(e!; \widetilde{K})] \end{aligned}$$

defines an isomorphism between K and $\widetilde{K}$.

□

5. Pop's conjecture

In this section we note how Pop's conjecture follows as a corollary of Theorem 4.1.

Theorem 5.1. *If K is a finitely generated field, then there is a sentence Φ_K in the language of rings for which K is the only finitely generated field, up to isomorphism, satisfying Φ_K. In particular, Pop's conjecture holds: two finitely generated fields are elementarily equivalent if and only if they are isomorphic.*

Proof. If K is finite of cardinality q, then the sentence

$$\Phi_K := (\exists x_1 \dots x_q)(\bigwedge_{1\le i<j\le q} x_i \neq x_j \ \&\ (\forall z)\bigvee_{i=1}^{q} z = x_i)$$

which expresses that the cardinality of the universe is indeed q determines K up to isomorphism.

If K is infinite, then by Theorem 4.1 there is an integer M and a parametrically definable isomorphism between K and $(\mathbb{N}, \oplus_M, \otimes_M)$. The isomorphism between K and the interpreted copy of K in an interpreted copy of $\mathbb{N}$ is defined by specializing the parameters of some formula η.

If $\mathrm{char}(K) = 0$, then let

$$\Phi_K := \zeta \ \&\ (\exists \boldsymbol{u})\xi_\eta(0, \boldsymbol{u}, M)$$

If $\mathrm{char}(K) > 0$, then let

$$\Phi_K := \neg\zeta \ \&\ (\exists \boldsymbol{u})(\exists t)\xi_\eta(t, \boldsymbol{u}, t^M)$$

Here ξ_η is the formula of Proposition 2.10 and ζ is the sentence expressing that the characteristic is zero. □

Remark 5.2. The use of the formula η in our proof of Theorem 5.1 obscures an important failure of uniformity in our proof. *Prima facie*, the formula η depends on K. Tracing through our proof, one could eliminate some of this dependence, but certainly not all. For instance, Rumely's biïnterpretation for global fields is completely uniform. Our formulas seem to depend in an essential way on the transcendence degree of the finitely generated field in question.

Conjecture 5.3 (Poonen's Conjecture γ, Question 1.8 of [14])**.** *Given a definable set $X \subseteq \mathbb{N}$ of codes for infinite finitely generated fields which is closed under isomorphism in the sense that if $M \in X$ and $(\mathbb{N}, \oplus_M, \otimes_M) \cong (\mathbb{N}, \oplus_N, \otimes_N)$, then $N \in X$, there is a sentence Ξ_X in the language of rings for which $(\mathbb{N}, \oplus_M, \otimes_M) \models \Xi_X$ if and only if $M \in X$.*

While our methods do not yield Conjecture 5.3, they do show that every definable class of finitely generated fields is axiomatizable by a first-order theory.

Theorem 5.4. *Given a formula $\vartheta(x)$ in the language of arithmetic which is closed under isomorphism in the sense that if $\mathbb{N} \models \vartheta(M)$ and $(\mathbb{N}, \oplus_M, \otimes_M) \cong (\mathbb{N}, \oplus_N, \otimes_N)$, then $\mathbb{N} \models \vartheta(N)$, there is a set of sentences Θ in the language of rings for which $(\mathbb{N}, \oplus_M, \otimes_M) \models \Theta$ if and only if $\mathbb{N} \models \vartheta(M)$.*

Proof. We let $\widetilde{\vartheta}(x, t)$ be the formula obtained by relativizing ϑ to the copy of $\mathbb{N}$ interpreted with parameter t.

Let

$$\begin{aligned}\Theta \ := \ & \{(\exists N)(\exists \boldsymbol{u})(\exists t)\xi_\eta(t, \boldsymbol{u}, N) \leftrightarrow \\ & (\forall M)(\exists t)(\exists \boldsymbol{u})[\xi_\eta(t, \boldsymbol{u}, M) \leftrightarrow \widetilde{\vartheta}(M, t)] \mid \\ & \eta \text{ a formula in the language of rings } \}\end{aligned}$$

If K is an infinite finitely generated field, then by Theorem 4.1 there are η, N, $\boldsymbol{u}$ and t for which $K \models \xi_\eta(t, \boldsymbol{u}, N)$. If $K \models \Theta$, then we must have $K \models \widetilde{\vartheta}(N)$. That is, the code for a presentation of K satisfies ϑ. Conversely, if the code for a presentation

of K satisfies ϑ, then by our hypothesis that ϑ is closed under isomorphism, every code for K satisfies ϑ so that $K \models \Theta$. □

References

[1] M. Aschenbrenner, Ideal membership in polynomial rings over the integers, *J. Amer. Math. Soc.* **17** (2004), no. 2, 407–441.

[2] M. Auslander and A. Brumer, Brauer groups of discrete valuation rings, *Nederl. Akad. Wetensch. Proc. Ser. A* **71** (*Indag. Math.* **30**) (1968), 286–296.

[3] J.-L. Duret, Sur la théorie élémentaire des corps de fonctions, *J. Symbolic Logic* **51** (1986), no. 4, 948–956.

[4] J.-L. Duret, Équivalence élémentaire et isomorphisme des corps de courbe sur un corps algébriquement clos, *J. Symbolic Logic* **57** (1992), no. 3, 808–823.

[5] D. K. Faddeev Simple algebras over a field of algebraic functions of one variable. (Russian) Trudy Mat. Inst. Steklov., v. 38, pp. 321–344. Izdat. Akad. Nauk SSSR, Moscow, 1951.

[6] M. Fried and M. Jarden **Field arithmetic** Second edition. Ergebniße der Mathematik und ihrer Grenzgebiete. 3. Folge. A Series of Modern Surveys in Mathematics, 11. Springer-Verlag, Berlin, 2005. xxiv+780 pp.

[7] P. Gille and T. Szamuely **Central simple algebras and Galois cohomology**, Cambridge Studies in Advanced Mathematics, 101. Cambridge University Press, Cambridge, 2006. xii+343 pp.

[8] W. Hodges, **Model theory**, Encyclopedia of Mathematics and its Applications, **42**, Cambridge University Press, Cambridge, 1993.

[9] R. Kaye, **Models of Peano Arithmetic**, Oxford Logic Guides **15**, Oxford Science Publications, The Clarendon Press, Oxford University Press, New York, 1991.

[10] A. Khelif Bi-interprétabilité et structures QFA: étude de groupes résolubles et des anneaux commutatifs, *C. R. Acad. Sci. Paris Sér. I Math.*, to appear.

[11] T.-Y. Lam, **A first course in noncommutative rings**, Graduate Texts in Mathematics **131** Springer-Verlag, New York, 1991.

[12] Y. Matiyasevich, **Hilbert's Tenth Problem**, Translated from the 1993 Russian original by the author with a foreword by Martin Davis, Foundations of Computing Series, MIT Press, Cambridge, MA, 1993.

[13] A. Nies, Describing groups, *Bulletin of Symbolic Logic*, to appear.

[14] B. Poonen, Uniform first-order definitions in finitely generated fields, *Duke Math. J.* **138** (2007), no. 1, 1–22.

[15] F. Pop, Elementary equivalence versus isomorphism, *Invent. Math.* **150** (2002), no. 2, 385–408.

[16] J. Robinson, The undecidability of algebraic rings and fields, *Proc. Amer. Math. Soc.* **10** (1959) 950–957.

[17] R. Robinson, Undecidable rings, *Trans. Amer. Math. Soc.* **70** (1951) 137–159.

[18] R. Rumely, Undecidability and definability for the theory of global fields, *Trans. Amer. Math. Soc.* **262** (1980), no. 1, 195–217.

[19] J.-P. Serre **Local fields** Translated from the French by Marvin Jay Greenberg. Graduate Texts in Mathematics, 67. Springer-Verlag, New York-Berlin, 1979. viii+241 pp.

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

E-mail address: scanlon@math.berkeley.edu