Decidability in local and global fields

Jochen Koenigsmann
Oxford

Abstract

This lecture highlights some recent advances on classical decidability issues in local and global fields.

2010 Mathematics Subject Classification: Primary 11U05; Secondary: 03B25, 11F85, 12J10, 12L05.

Contents

1 Introduction

In 1900, at the International Congress of Mathematicians in Paris, Hilbert presented his celebrated and influential list of 23 mathematical problems ([Hil00]). One of them is

Hilbert's 10th Problem ('H10') Find an algorithm which gives on INPUT any $f(X_1, \ldots, X_n) \in \mathbb{Z}[X_1, \ldots, X_n]$

$$\text{OUTPUT} \begin{cases} \textbf{YES} & \text{if } \exists \overline{x} \in \mathbb{Z}^n \text{ such that } f(\overline{x}) = 0 \\ \textbf{NO} & \text{else} \end{cases}$$

Hilbert did not ask to prove that there is such an algorithm. He was convinced that there should be one, and that it was all a question of producing it — one of those instances of Hilbert's optimism reflected in his famous slogan '*wir müssen wissen, wir werden wissen*' ('*we must know, we will know*'). As it happens, Hilbert was too optimistic: after previous work since the 50's by Martin Davis, Hilary Putnam and Julia Robinson (cf., e.g., [DPR61]), Yuri Matiyasevich showed in 1970 that there is no such algorithm ([Mat70]). The key result here is the most remarkable so-called DPRM-Theorem that every (algorithmically) listable set of integers is *diophantine*, i.e., first-order definable in the language of rings $L_{ring} := \{+, \times, 0, 1\}$ by an *existential* formula.

The original formulation of Hilbert's 10th Problem was weaker than the standard version above in that he rather asked *'Given a polynomial f, find an algorithm ...'*. So maybe you could have different algorithms depending on the number of variables and the degree. Yet it is even possible to find a single polynomial for which no such algorithm exists — this is essentially because there are universal Turing Machines.

One should, however, mention that, in the special case of $n = 1$, that is, for polynomials in one variable, there is an easy algorithm: if, for some $x \in \mathbb{Z}$, $f(x) = 0$ then $x \mid f(0)$; hence one only has to check the finitely many divisors of $f(0)$. Similarly, by the effective version of the Hasse-Minkowski-Local-Global-Principle for quadratic forms and some extra integrality considerations, one also has an algorithm for polynomials in an arbitrary number of variables, but of total degree ≤ 2. And, even if there is no general algorithm, it is one of the major projects of computational arithmetic geometry to exhibit other families of polynomials for which such algorithms exist.

Let us point in a different direction of generalizing Hilbert's 10th Problem, namely, generalizing it to rings other than $\mathbb{Z}$: If R is an integral domain, there are two natural ways of generalizing **H10**:

$$\textbf{H10}/R = \textbf{H10} \text{ with the 2nd occurrence of } \mathbb{Z} \text{ replaced by } R$$
$$\textbf{H10}^+/R = \textbf{H10} \text{ with both occurrences of } \mathbb{Z} \text{ replaced by } R$$

Observation 1.1. *Let R be an integral domain whose field of fractions does not contain the algebraic closure of the prime field ($\mathbb{F}_p$ resp. $\mathbb{Q}$). Then*

$$\begin{array}{rcl} \mathbf{H10}/R \text{ is solvable} & \Leftrightarrow & \mathtt{Th}_{\exists^+}(R) \text{ is decidable} \\ \mathbf{H10}^+/R \text{ is solvable} & \Leftrightarrow & \mathtt{Th}_{\exists^+}(\langle R; r \mid r \in R\rangle) \text{ is decidable,} \end{array}$$

where $\mathtt{Th}_{\exists^+}$ denotes the positive existential theory consisting of existential sentences where the quantifier-free part is a conjunction of disjunctions of polynomial equations (no inequalities).

Note that the language on the right hand side of the 2nd line contains a constant symbol for each $r \in R$.

Proof: '$\Leftarrow$' is obvious in both cases. For '$\Rightarrow$' one has to see that a disjunction of two polynomial equations is equivalent to (another) single equation, and, likewise, for conjunctions: By our assumption we can find some monic $g \in \mathbb{Z}[X]$ of degree > 1 which is irreducible over R. Then, for any polynomials f_1, f_2 over $\mathbb{Z}$ resp. R and for any tuple $\overline{x}$ over R,

$$\begin{array}{rcl} f_1(\overline{x}) = 0 \vee f_2(\overline{x}) = 0 & \Longleftrightarrow & f_1(\overline{x}) \cdot f_2(\overline{x}) = 0 \\ f_1(\overline{x}) = 0 \wedge f_2(\overline{x}) = 0 & \Longleftrightarrow & g(\frac{f_1(\overline{x})}{f_2(\overline{x})}) \cdot f_2(\overline{x})^{\deg g} = 0 \end{array}$$

□

Since in fields, inequalities can be expressed by a positive existential formula ($f(\overline{x}) \neq 0 \leftrightarrow \exists y\ f(\overline{x}) \cdot y = 1$), we immediately obtain the following:

Corollary 1.2. *Let K be a field not containing the algebraic closure of the prime field. Then*

$$\mathbf{H10}/K \text{ is solvable} \Leftrightarrow \mathtt{Th}_{\exists}(K) \text{ is decidable.}$$

In fact, the same is true for $\mathcal{O}_K$, the ring of integers of a number field K:

Observation 1.3. *If K is a number field,*

$$\mathcal{O}_K \models \forall x[x \neq 0 \leftrightarrow \exists y\ x \mid (2y-1)(3y-1)].$$

Hence $\mathtt{Th}_{\exists}(\mathcal{O}_K) = \mathtt{Th}_{\exists^+}(\mathcal{O}_K)$.

One of the biggest open questions in the area is

Question 1.4. *Is $\mathbf{H10}/\mathbb{Q}$ solvable?*

Let us recall that, by the ground breaking work of Kurt Gödel, the full first order theory of $\mathbb{Z}$ is undecidable, so there is no algorithm which decides, on INPUT any first-order L_{ring}-sentence ϕ, whether or not ϕ holds in $\mathbb{Z}$ (cf. [Göd31]). In [Rob49], Julia Robinson managed to find an L_{ring}-first-order definition of $\mathbb{Z}$ in $\mathbb{Q}$, thus showing, via Gödel's Theorem, that the full first-order theory of $\mathbb{Q}$ is also undecidable. If one had an *existential* first-order L_{ring}-formula defining $\mathbb{Z}$ in $\mathbb{Q}$ then one could, via Matiyasevich's Theorem, conclude that Hilbert's 10th Problem over $\mathbb{Q}$ is also unsolvable. However, the best we have at the moment (in terms of logical complexity) is a *universal* formula for $\mathbb{Z}$ in $\mathbb{Q}$ (cf. Theorem 3.1 below).

Hilbert's 10th Problem for the ring of integers of a number field (that is, a finite extension of $\mathbb{Q}$ — they are the *global* fields of characteristic 0) has been shown to be unsolvable in several cases, the general case could sofar only be proven modulo a (widely believed) conjecture regarding elliptic curves (see section 3.2).

For global fields of positive characterisitc, that is, for finite extensions of the rational function field $\mathbb{F}_p(t)$ over the finite field $\mathbb{F}_p$ in one variable t, Hilbert's 10th Problem, again, has no solution (cf. section 3.3).

Many of the results obtained for global fields rely heavily on results and techniques developed for *local fields*. Local fields are defined to be fields F which are locally compact with respect to the topology induced by some non-trivial absolute value on F. It turns out that local fields are precisely the completions of global fields (w.r.t such absolute values) and they are classified as follows: the *archimedean* local fields are just the field $\mathbb{R}$ of real numbers and the field $\mathbb{C}$ of complex numbers; the non-archimedean local fields of characteristic 0 are precisely all finite extensions of $\mathbb{Q}_p$, the field of *p-adic numbers*, where p is any rational prime; and the non-archimedean local fields of positive characteristic p are precisely the finite extensions of $\mathbb{F}_p((t))$, the field of formal Laurent series over the field $\mathbb{F}_p$ with p elements. For the non-archimedean local fields, the absolute value is induced by a canonical valuation, which is the p-adic valuation on $\mathbb{Q}_p$ and the t-adic valuation on $\mathbb{F}_p((t))$, and these valuations extend uniquely to all finite extensions, a property of valuations called *henselian*.

All decidability issues for the two archimedean local fields have been settled by Tarski in the 1930s: The full first order theory of $\mathbb{R}$ and of $\mathbb{C}$ is decidable (and hence, in particular, Hilbert's 10th Problem is solvable for those two fields).

The decidability of $\mathbb{Q}_p$ was proved independently by Ax-Kochen in [AK65]

and by Ershov in [Ers65]. They effectively axiomatized $\mathbb{Q}_p$ as a henselian valued field of characteristic 0 whose residue field is $\mathbb{F}_p$, whose value group is a $\mathbb{Z}$-group (so elementarily equivalent to the ordered abelian group of integers) such that the value of p is minimal positive. And there are similar axiomatizations for all finite extensions of $\mathbb{Q}_p$ (see [PR84] for a general treatment of p-adic fields).

Since those results of Ax-Kochen and Ershov in 1965 it has been a big open problem whether the theory of $\mathbb{F}_p((t))$ is decidable as well. Recently major progress has been made on this problem which we will discuss in section 2 below.

There are several important infinite extension of local and global fields for which decidability issues are of great interest, too. For example, the field $\mathbb{Q}^{ab}$, the maximal Galois extension of $\mathbb{Q}$ with an abelian Galois group which, by the famous Kronecker-Weber Theorem, is just the field obtained from $\mathbb{Q}$ by adjoining all roots of unity, is not known to be decidable or undecidable. Similarly, one does not know this about Q^{solv}, the maximal Galois extension of $\mathbb{Q}$ with prosolvable Galois group which is obtained from $\mathbb{Q}$ by iteratedly adjoining radicals (n-th roots of elements for arbitrary n). It is an open problem in Field Arithmetic whether or not $\mathbb{Q}^{solv}$ is pseudo-algebraically closed in the sense that every absolutely irreducible curve defined over $\mathbb{Q}^{solv}$ has a $\mathbb{Q}^{solv}$-rational point (Problem 11.5.9(a) in [FJ08]). If this Problem has a positive answer and if the famous Shafarevich Conjecture that the absolute Galois group of $\mathbb{Q}^{ab}$ is a free profinite group is true then one can show that $\mathbb{Q}^{solv}$ is decidable.

In section 4 we will briefly consider two infinite extensions of $\mathbb{Q}_p$ for which there has been recent progress, namely $\mathbb{Q}_p^{ur}$, the maximal unramified extension of $\mathbb{Q}_p$ which turns out to be decidable and model theoretically well behaved, and $\mathbb{Q}_p^{ab}$, the maximal abelian extension of $\mathbb{Q}_p$, for which a promising new suggestion for a first-order axiomatization will be presented.

Some notation from valuation theory: The reader is expected to be acquainted with the basics of valuation theory (cf., e.g., [EP05]). For a valued field (K, v), the valuation ring will be denoted by $\mathcal{O}_v$, the residue field by Kv and the value group by vK.

2 Local fields of positive characteristic

Regarding the question of decidability of the field $\mathbb{F}_q((t))$ of formal Laurent series over a finite field $\mathbb{F}_q$ there have been two recent breakthroughs: one is the result of Anscombe-Fehm that the *existential* L_{ring}-theory of $\mathbb{F}_q((t))$ is decidable (Theorem 2.1). The other is a new promising suggestion for an effective first order axiomatization for $\mathbb{F}_q((t))$ using the notion of *extremal valued fields*.

Throughout this section we will fix q, a power of the rational prime $p > 0$.

2.1 The existential theory of $\mathbb{F}_q((t))$

In [DS03], Jan Denef and Hans Shoutens managed to prove that the *existential* theory of $\mathbb{F}_q((t))$ in $L_{ring} \cup \{t\}$, the language of rings augmented by a constant symbol for t, is decidable if one assumes resolution of singularities in positive characteristic. Sylvy Anscombe and Arno Fehm then found a surprisingly elementary unconditional proof for the decidability of the existential L_{ring}-theory of $\mathbb{F}_q((t))$ (see [AF16]). More generally they prove the following

Theorem 2.1. *Let (K, v) be an equicharacteristic henselian valued field (so char K = char Kv). Then the existential L_{val}-theory of K is decidable if and only if the existential L_{ring}-theory of the residue field Kv is decidable.*

Here $L_{val} = L_{ring} \cup \{\mathcal{O}\}$ is the language of valued fields, that is, the language of rings augmented by a unary predicate symbol $\mathcal{O}$ for the valuation ring. There are many alternative possibilities for a first order language for valued fields (you could, for example, have a three-sorted language distinguishing the field sort, the residue field sort and the value group sort with additional function symbols for the valuation map and the canonical restriction map to the residue field). But it turns out that all these languages are mutually translatable into each other, so they all have the same expressive power.

Let us point out that, for the question of the decidability of the existential theory of $\mathbb{F}_q((t))$, it makes no difference whether you ask this question about the existential theory in L_{ring} or in L_{val}, because, by the main theorem of [AKo14], the valuation ring $\mathbb{F}_q[[t]]$ of $\mathbb{F}_q((t))$ is existentially first-order definable in the language of rings. This leads immediately to the following

Corollary 2.2. *The existential L_{ring}-theory of $\mathbb{F}_q[[t]]$ is dedicable.*

So, in other words, Hilbert's 10th Problem has a positive solution both for $\mathbb{F}_q((t))$ and for $\mathbb{F}_q[[t]]$.

A more general result on almost existential definability of henselian valuation rings in valued fields with finite or pseudo-finite residue fields can be found in [CDLM13].

Whether or not the existential $L_{ring} \cup \{t\}$-theory of $\mathbb{F}_q((t))$ is decidable (without assuming resolution of singularities) is still open.

2.2 Axiomatizing $\mathbb{F}_q((t))$

The biggest open question in the model theory of valued fields, however, is the question whether the full first-order theory of $\mathbb{F}_q((t))$ is decidable. There have been a number of suggestions of how to axiomatize this field. The most promising suggestion builds on the notion of *extremal* valued fields, originally introduced (though with a 'wrong' definition) by Yuri Ershov in [Ers04], then, following a suggestion of Sergei Starchenko, the definition was amended and the 'correct' definition was put forward in [Ers09] and in [AKP12]. The suggested axiomatization for $\mathbb{F}_q((t))$ given below first appeared in [AKu16].

Definition 2.3. *A valued field (K, v) is* extremal *if, for every polynomial $f(X_1, \ldots, X_n) \in K[X_1, \ldots, X_n]$, the set*

$$\{v(f(a_1, \ldots, a_n)) \mid a_1, \ldots, a_n \in \mathcal{O}_v\} \subseteq vK \cup \{\infty\}$$

has a maximal element.

It turns out that extremal valued fields are *algebraically maximal*, that is, for each finite extension $(L, w)/(K, v)$, the fundamental equality '$n = e \cdot f$' holds, where $n = [L : K]$, $e = [wL : vK]$ and $f = [Lw : Kv]$, and so, in particular, extremal fields are henselian. Moreover, their value group is either divisible or a $\mathbb{Z}$-group (elementarily equivalent to the ordered abelian group $\mathbb{Z}$ of integers) and that in the first case the residue field has to be large in the sense of having infinitely many rational points for each algebraic curve with at least one rational point (cf. [Pop96]).

The axiomatization for $\mathbb{F}_q((t))$ using this notion of extremal valued fields is now very simple:

(1) (K, v) is an extremal valued field of charactersitic p,

(2) the value group vK is a $\mathbb{Z}$-group,

(3) the residue field Kv is the field $\mathbb{F}_q$.

It has long been known that the 'naive' axiomatization for $\mathbb{F}_q((t))$, where axiom (1) is replaced by just asking (K, v) to be henselian, is not complete.

3 Global fields

3.1 A universal definition for $\mathbb{Z}$ in $\mathbb{Q}$

Hilbert's 10th problem over $\mathbb{Q}$, i.e., the question whether the existential L_{ring}-theory of $\mathbb{Q}$ is decidable, is still open.

If one had an *existential* (= *diophantine*) definition of $\mathbb{Z}$ in $\mathbb{Q}$ (i.e., a definition by an existential 1st-order $\mathcal{L}_{ring}$-formula) then the existential theory of $\mathbb{Z}$ would be interpretable in that of $\mathbb{Q}$, and the answer would, by (for short) Matiyasevich's Theorem, again be no. But it is still open whether $\mathbb{Z}$ is existentially definable in $\mathbb{Q}$.

The earliest 1st-order definition for $\mathbb{Z}$ in $\mathbb{Q}$, due to Julia Robinson ([R49]), can be expressed by an $\forall\exists\forall$-formula of the shape

$$\phi(t): \ \forall x_1 \forall x_2 \exists y_1 \dots \exists y_7 \forall z_1 \dots \forall z_6 \ f(t; x_1, x_2; y_1, \dots, y_7; z_1, \dots, z_6) = 0$$

for some $f \in \mathbb{Z}[T; X_1, X_2; Y_1, \dots, Y_7; Z_1, \dots, Z_6]$, i.e., for any $t \in \mathbb{Q}$,

$$t \in \mathbb{Z} \text{ iff } \phi(t) \text{ holds in } \mathbb{Q}.$$

In 2009, Bjorn Poonen ([P09a]) managed to find an $\forall\exists$-definition with 2 universal and 7 existential quantifiers (earlier, in [CZ07], an $\forall\exists$-definition with just one universal quantifier was proved modulo an open conjecture on elliptic curves).

In [Koe16], the author then provided a $\forall$-definition of $\mathbb{Z}$ in $\mathbb{Q}$:

Theorem 3.1. *There is a polynomial $g \in \mathbb{Z}[T; X_1, \dots, X_{418}]$ such that, for all $t \in \mathbb{Q}$,*

$$t \in \mathbb{Z} \text{ iff } \forall \overline{x} \in \mathbb{Q}^{418} \ g(t; \overline{x}) \neq 0.$$

If one measures logical complexity in terms of the number of changes of quantifiers then this is the simplest definition of $\mathbb{Z}$ in $\mathbb{Q}$, and, in fact, it is the simplest possible: there is no quantifier-free definition of $\mathbb{Z}$ in $\mathbb{Q}$.

Corollary 3.2. *$\mathbb{Q} \setminus \mathbb{Z}$ is diophantine in $\mathbb{Q}$.*

Corollary 3.3. *$Th_{\forall\exists}(\mathbb{Q})$ is undecidable.*

Theorem 3.1 came somewhat unexpected because it does not give what you would like to have, namely an existential definition of $\mathbb{Z}$ in $\mathbb{Q}$. However, if you had the latter the former would follow:

Observation 3.4. *If there is an existential definition of $\mathbb{Z}$ in $\mathbb{Q}$ then there is also a universal one.*

Proof: If $\mathbb{Z}$ is diophantine in $\mathbb{Q}$ then so is

$$\mathbb{Q} \setminus \mathbb{Z} = \{x \in \mathbb{Q} \mid \exists m, n, a, b \in \mathbb{Z} \text{ with } n \neq 0, \pm 1,\ am + bn = 1 \text{ and } m = xn\}$$

□

The machinery for proving these three first-order definitions of $\mathbb{Z}$ in $\mathbb{Q}$ is not very heavy: Julia Robinson made essentially use of the Hasse-Minkowski Local-Global Principle for quadratic forms, Bjorn Poonen augmented that using the Hasse bound for the number of rational points on genus-1 curves over finite fields (and he ingeniously rearranged the use of quadratic form theory), while in [Koe16] the Quadratic Reciprocity Law came in as additional tool, and then some elementary tricks (inspired by the model theory of valued fields) for transforming existential formulas into universal ones were needed to complete the proof.

Using more serious number theory, Jennifer Park ([Par13])has generalised Theorem 3.1 to number fields:

Theorem 3.5. *For any number field K, the ring of integers $\mathcal{O}_K$ is universally definable in K.*

In the course of the proof of [Koe16] many new diophantine subsets of $\mathbb{Q}$ emerged, for example the set of non-squares turned out to be diophantine (this was obtained earlier in [Poo09b] using much deeper techniques). If, however, $\mathbb{Z}$ was also diophantine in $\mathbb{Q}$ then there would be many more important diophantine subsets of $\mathbb{Q}$, for example the set of tuples of coefficients of irreducible polynomials (of fixed degree) over $\mathbb{Q}$. Later, Philip Dittmann managed to prove this unconditionally and in much greater generality ([Dit16]):

Theorem 3.6. *Irreducibility of polynomials over global fields is diophantine.*

3.2 Hilbert's 10th Problem for number rings using elliptic curves

In this section only one major achievement is being reported on. There is a multitude of surveys on the subject, each with its own emphasis. For the interested reader, let us mention at least some of them: [RRo51], [Maz94], [Phe94], [Mat00], [PZ00], [Shl00], [Poo03], [Shl07], [Poo08] and [Koe14].

For number rings and number fields, the question of decidability has been answered in the negative by Julia Robinson in [Rob59]. The question whether Hilbert's 10th Problem is solvable is much harder. Given that we don't know the answer over $\mathbb{Q}$ (though almost everyone working in the field believes it to be no) there is even less hope that we find the answer for arbitrary number fields in the near future. For number *rings* the situation is much better.

Let K be a number field with ring of integers $\mathcal{O}_K$. Then Hilbert's 10th Problem could be shown to be unsolvable over $\mathcal{O}_K$ in the following cases:

- if K is totally real or a quadratic extension of a totally real number field ([Den75], [DL78] and [Den80]),
- if $[K:\mathbb{Q}] \geq 3$ and $c_K = 2$ ([Phe88])[1],
- if $K/\mathbb{Q}$ is abelian ([SS89]).

In each of the proofs the authors managed to find an existential definition of $\mathbb{Z}$ in $\mathcal{O}_K$ using Pell-equations, the Hasse-Minkowski Local-Global Principle (which holds in all number fields) and ad hoc methods that are very specific to each of these special cases.

The hope for a uniform proof of the existential undecidability of all number rings only emerged when elliptic curves were brought into the game:

Theorem 3.7 ([Poo02])**.** *Let K be a number field. Assume[2] there is an elliptic curve E over $\mathbb{Q}$ with $\mathtt{rk}(E(\mathbb{Q})) = \mathtt{rk}(E(K)) = 1$. Then $\mathbb{Z}$ is existentially definable in $\mathcal{O}_K$ and so Hilbert's 10th Problem over $\mathcal{O}_K$ is unsolvable.*

[1] c_K denotes the *class number* of K, that is, the size of the ideal class group of K. It measures how far $\mathcal{O}_K$ is from being a PID: $c_K = 1$ iff $\mathcal{O}_K$ is a PID, so $c_K = 2$ is 'the next best'. It is not known whether there are infinitely many number fields with $c_K = 1$.

[2] The set $E(K)$ of K-rational points of E is a finitely generated abelian group isomorphic to the direct product of its torsion subgroup $E_{tor}(K)$ and a free abelian group of rank '$\mathtt{rk}(E(K))$'.

In his proof, Poonen uses divisibility relations for denominators of x-coordinates of $n \cdot P$, where $P \in E(K) \setminus E_{tor}(K)$ and $n \cdot P \in E(\mathbb{Q})$ (for a similar approach cf. [CPZ05]).

The assumption made in the theorem turns out to hold modulo a generally believed conjecture, the so called *Tate-Shafarevich Conjecture*. For an elliptic curve E over a number field K, it refers to the *Tate-Shafarevich group* (or *Shafarevich-Tate group*) $Ш_{E/K}$, an abelian group defined via cohomology groups. It measures the deviation from a local-global principle for rational points on E.

Tate-Shafarevich Conjecture $Ш_{E/K}$ *is finite.*

Weak Tate-Shafarevich Conjecture $\dim_{\mathbb{F}_2} Ш_{E/K}/2$ *is even.*

The latter follows from the former due to the Cassels pairing (Theorem 4.14 in [Sil86] which is an excellent reference on elliptic curves).

Theorem 3.8 ([MR10])**.** *Let K be a number field. Assume the weak Tate-Shafarevich Conjecture for all elliptic curves E/K. Then there is an elliptic curve $E/\mathbb{Q}$ with* $\mathtt{rk}(E(\mathbb{Q})) = \mathtt{rk}(E(K)) = 1$.

Taking those two theorems together you obtain immediately the following

Corollary 3.9. *Let K be a number field. Assume the weak Tate-Shafarevich Conjecture for all elliptic curves E/K. Then Hilbert's 10th Problem is unsolvable over $\mathcal{O}_K$.*

3.3 Global fields of positive characteristic

It is natural to ask decidability questions not only over number fields, but also over global fields of positive characteristic, i.e., algebraic function fields in one variable over finite fields, and also, more generally, for function fields.

Hilbert's 10th Problem (with t resp. t_1, t_2 in the language) has been shown to be unsolvable for the following function fields:

- $\mathbb{R}(t)$ ([Den78]),
- $\mathbb{C}(t_1, t_2)$ ([KR92]),
- $\mathbb{F}_q(t)$ ([Phe91] and [Vid94]),
- finite extensions of $\mathbb{F}_q(t)$ ([Shl92] and [Eis03]).

The first two cases were achieved by existentially defining $\mathbb{Z}$ in the field, and then applying Matiyasevich's Theorem. This is, clearly, not possible in the last two cases. Instead of existentially *defining* $\mathbb{Z}$ the authors existentially *interpret* $\mathbb{Z}$ via elliptic curves: the multiplication by n-map on an elliptic curve E/K where $E(K)$ contains non-torsion points easily gives a diophantine interpretation of the additive group $\langle \mathbb{Z}; + \rangle$. The difficulty is to find an elliptic curve E/K such that there is also an existential definition for multiplication on that additive group.

For the ring of *polynomials* $\mathbb{F}_q[t]$, Demeyer has even shown the analogue of the DPRM-Theorem: listible subsets are diophantine ([Dem07]).

Generalizing earlier results ([Che84], [Dur86] and [Phe04]), it is shown in [ES09], that the *full* first-order theory of any function field of characteristic > 2 is undecidable.

For analogues of Hilbert's 10th Problem for fields of meromorphic or analytic functions cf., e.g., [Rub95], [Vdau03] and [Pas13].

4 Two infinite extensions of $\mathbb{Q}_p$

Let us recall that the field $\mathbb{Q}_p$ is axiomatized as a valued field (K, v) satisfying the following four axioms:

(1) (K, v) is henselian of mixed characteristic $(0, p)$,

(2)' $Kv = \mathbb{F}_p$,

(3)' $vK \equiv \mathbb{Z}$, so vK is a $\mathbb{Z}$-group,

(4)' $v(p)$ is minimal positive.

It is an immediate consequence of the main result of [DM16] that the field $\mathbb{Q}_p^{ur}$, the maximal unramified extension of $\mathbb{Q}_p$ (obtained from $\mathbb{Q}_p$ by adjoining all prime to p roots of unity), is model complete, that is, every first order definable subset is already existentially definable. Using this, you can easily give an axiomatization of $\mathbb{Q}_p^{ur}$, namely as valued field (K, v) satisfying these axioms:

(1) (K, v) is henselian of mixed characteristic $(0, p)$,

(2) $Kv = \overline{Kv}$, so the residue field is algebraically closed,

(3)' $vK \equiv \mathbb{Z}$, so vK is a $\mathbb{Z}$-group,

(4)' $v(p)$ is minimal positive.

The next natural challenge is to find an axiomatization for $\mathbb{Q}_p^{ab}$, the maximal abelian extension of $\mathbb{Q}_p$, which, by the local Kronecker-Weber Theorem, is obtained from $\mathbb{Q}_p$ by adjoining all roots of unity. The axiomatization suggested (but not yet proved to be complete) in [Koe18] is the axiomatization as valued field (K, v) satisfying these axioms:

(1) (K, v) is henselian of mixed characteristic $(0, p)$,

(2) $Kv = \overline{Kv}$,

(3) $vK \equiv \frac{1}{p^\infty}\mathbb{Z}$,

(4) $q \nmid v(1 - \zeta_p)$ for any prime $q \neq p$,

(5) $K \cap \overline{\mathbb{Q}} = \mathbb{Q}_p^{ab} \cap \overline{\mathbb{Q}}$,

(6) $v = v_K^p$,

(7) the Frobenius map $x \mapsto x^p$ is surjective on $\mathcal{O}_v/p\mathcal{O}_v$.

Here $\frac{1}{p^\infty}\mathbb{Z}$ is the ordered subgroup of the group of rational numbers having only p-th powers as denominators, ζ_p is a primitive p-th root of unity, and v_K^p is the *canonical p-henselian valuation* on K, that is here the coarsest p-henselian valuation with p-closed residue field, where p-henselian means that the valulation extends uniquely to every Galois extension of degree p. That these axioms can be expressed by (recursive sets of) first-order formulas is not too hard to show, except for axiom (6), for which this is proved in [JK15]. It is also not too difficult to check that all these axioms are true in $\mathbb{Q}_p^{ab}$. However, it requires substantial work to prove that these axioms are independent, that is, for each of the seven axioms one finds a valued field not satisfying this particular axiom, but satisfying all the other axioms (this is done in [Koe18]. The planned strategy for establishing that these axioms are complete is via showing quantifier elimination in a variant of the Macintyre language for valued fields including n-th power predicates.

References

[AF16] Sylvy Anscombe, Arno Fehm, *The existential theory of equicharacteristic henselian valued fields*, Algebra and Number Theory **10(3)** (2016), 665-683 .

[AKo14] Will Anscombe, Jochen Koenigsmann, *An existential $\emptyset$-definition of $\mathbb{F}_q[[t]]$ in $\mathbb{F}_q((t))$*, Journal of Symbolic Logic **79(4)** (2014), 1336-1343.

[AKu16] Sylvy Anscombe, Franz-Viktor Kuhlmann, *Notes on extremal and tame valued fields*, Journal of Symbolic Logic **81(2)** (2016), 400-416.

[AK65] James Ax, Simon Kochen, *Diophantine problems over local fields I + II*, Am. J. Math. **87** (1965), 605-630 and 631-648.

[AKP12] Salih Azgin, Franz-Viktor Kuhlmann, Florian Pop, *Characterization of extremal valued fields*, Proc. AMS **140(5)** (2012), 1535-1547.

[Che84] Gregory L. Cherlin, *Undecidability of rational function fields in nonzero characteristic*, Stud. Logic Found. Math. **112** (1984), 85-95.

[CDLM13] Raf Cluckers, Jamshid Derakhshan, Eva Leenknegt, Angus Macintyre, *Uniformly defining valuation rings in Henselian valued fields with finite or pseudo-finite residue field*, Annals of Pure and Appl. Logic **164(12)** (2013), 1236-1246.

[CPZ05] Gunther Cornelissen, Thanases Pheidas, Karim Zahidi, *Division-ample sets and the Diophantine problem for rings of integers*, J. Th. Nombres de Bordeaux **17** (2005), 727-735.

[CZ07] Gunther Cornelissen, Karim Zahidi, *Elliptic divisibility sequences and undecidable problems about rational points*, J. Reine Angew. Math. **613** (2007), 1-33.

[DPR61] Martin Davis, Hilary Putnam, Julia Robinson, *The decision problem for exponential Diophantine equations*, Ann. Math. (2) **74** (1961), 425-436.

[Dem07] Jeroen Demeyer, *Recursively enumerable sets of polynomials over a finite field are Diophantine*, Invent. Math. **170(3)** (2007), 655-670.

[Den75] Jan Denef, *Hilbert's 10th Problem for quadratic rings*, Proc. AMS **48** (1975), 214-220.

[Den78] —, *The diophantine problem for polynomial rings and fields of rational functions*, Trans. AMS **242** (1978), 391-399.

[Den80] —, *Diophantine sets over algebraic integer rings II*, Trans. AMS **257** (1980), 227-236.

[DL78] Jan Denef, Leonard Lipshitz, *Diophantine sets over some rings of algebraic integers*, J. LMS **18** (1978), 385-391.

[DLPG00] Jan Denef, Leonard Lipshitz, Thanases Pheidas, Jan Van Geel, *Hilbert's Tenth Problem: relations with arithmetic and algebraic geometry*, Contemporary Math. (AMS) **270**, 2000.

[DM16] Jamshid Derakhshan, Angus Macintyre, *Model Completeness for Henselian fields with finite ramification valued in a $\mathbb{Z}$-group*, arXiv:1603.08598v1 [math.LO] (2016).

[Dit16] Philip Dittmann, *Irreducibility of polynomials over global fields is diophantine*, arXiv:1601.07829v3 [math.NT] (2016), to appear in Compositio Math.

[DS03] Jan Denef, Hans Schoutens, *On the decidability of the existential theory of $\mathbb{F}_p[[T]]$*, in: Franz-Viktor Kuhlmann et al. (eds), *Valuation theory and its applications 2*, Fields Inst. Comm. **33** (2003), 43-60.

[Dur86] Jean-Louis Duret, *Sur la théorie élémentaire des corps de fonctions*, J. Symb. Logic **51(4)** (1986), 948-956.

[Eis03] Kirsten Eisenträger, *Hilbert's 10th Problem for algebraic function fields of characteristic 2*, Pac. J. Math. **210(2)** (2003), 261-281.

[ES09] Kirsten Eisenträger, Alexandra Shlapentokh, *Undecidability in function fields of positive characteristic*, Int. Math. Res. Not. **2009** (2009), 4051-4086.

[EP05] Antonio J. Engler, Alexander Prestel, *Valued fields*, Springer 2005.

[Ers65] Yuri L. Ershov, *On elementary theories of local fields* Algebra i Logika **4** (1965), 5-30.

[Ers04] —, *Extremal valued fields*, Algebra i Logika **43** (2004), 582-588. Tranlation in Algebra Logic **43** (2004), 327-330.

[Ers09] —, $\star$*-extremal valued fields*, Sibirsk. Mat. Zh. **50** (2009), 1280-1284.

[FJ08] Michael Fried, Moshe Jarden, *Field arithmetic*, Springer, 3rd edition 2008.

[Göd31] Kurt Gödel, *Über formal unentscheidbare Sätze der Principia Mathematica und verwandter Systeme*, Monatshefte Math. Phys. **38** (1931), 173-198.

[Hil00] David Hilbert, *Mathematische Probleme. Vortrag, gehalten auf dem internationalen Mathematiker Kongress zu Paris 1900*, Nachr. K. Ges. Wiss., Göttingen, Math.-Phys. Kl. (1900), 253-297.

[JK15] Franziska Jahnke, Jochen Koenigsmann, *Uniformly defining p-henselian valuations*, Annals of Pure and Applied Logic **166(7-8)** (2015), 741-754.

[Koe14] Jochen Koenigsmann, *Undecidability in Number Theory*, in Dugald Macpherson, Carlo Toffalori (eds.): *Model Theory in Algebra, Analysis and Arithmetic*, Springer Lecture Notes in Mathematics **2111** (2014), 159-195.

[Koe16] —, *Defining* $\mathbb{Z}$ *in* $\mathbb{Q}$, Ann. of Math. **183(1)** (2016), 73-93.

[Koe18] —, *On the decidability of* $\mathbb{Q}_p^{ab}$, manuscript.

[KR92] Ki Hang Kim, Fred W. Roush, *Diophantine undecidability of* $\mathbb{C}(t_1, t_2)$, J. Algebra **150(1)**, 35-44.

[Mat70] Yuri V. Matiyasevich, *Diofantovost' perechislimykh mnozhestv*, Dokl. AN SSSR **191(2)** (1970), 278-282. Translated in: Soviet Math. Doklady **11(2)** (1970), 354-358.

[Mat00] —, *Hilbert's 10th Problem: what was done and what is to be done*, in: [DLPG00] (2000), 1-47.

[Maz94] Barry Mazur, *Questions of Decidability and Undecidability in Number Theory*, J. Symb. Logic **59(2)** (1994), 353-371.

[MR10] Barry Mazur, Karl Rubin, *Ranks of twists of elliptic curves and Hilbert's tenth problem*, Invent. Math. **181(3)** (2010), 541-575.

[Par13] Jennifer Park, *A universal first order formula defining the ring of integers in a number field*, Mathematical Research Letters **20(5)** (2013), 961-980.

[Pas13] Hector Pasten, *Powerful values of polynomials and a conjecture of Vojta*, J. Number Theory **133(9)** (2013), 2843-3206.

[Phe88] Thanases Pheidas, *Hilbert's tenth problem for a class of rings of algebraic integers*, Proc. AMS **104** (1988), 611-620.

[Phe91] —, *Hilbert's 10th Problem for fields of rational functions over finite fields*, Invent. Math. **103** (1991), 1-8.

[Phe04] —, *Endomorphisms of elliptic curves and undecidability in function fields of positive characteristic*, J. Algebra **273(1)** (2004), 395-411.

[PZ00] Thanases Pheidas, Karim Zahidi, *Undecidability of existential theories of rings and fields: a survey*, in: [DLPG00] (2000), 49-105.

[Poo02] Bjorn Poonen, *Using elliptic curves of rank one towards the undecidability of Hilbert's 10th Problem over rings of algebraic integers*, in: Claus Fieker, David R. Kohel (eds.) *Algorithmic number theory*, Springer 2002, 33-42.

[Poo03] —, *Hilbert's 10th problem over rings of number-theoretic interest*, www-math.mit.edu/ poonen/papers/aws2003.pdf, 2003.

[Poo08] —, *Undecidability in Number Theory*, Notices AMS **55(3)** (2008), 344-350.

[Poo09a] —, *Characterizing integers among rational numbers with a universal-existential formula*, Amer. J. Math. **131(3)** (2009), 675-682.

[Poo09b] —, *The set of nonsquares in a number field is diophantine*, Math. Res. Lett. **16(1)** (2009), 165-170.

[Pop96] Florian Pop, *Embedding problems over large fields*, Ann. Math. (2) **144(1)** (1996), 1-34.

[PR84] Alexander Prestel, Peter Roquette, *Formally p-adic fields*, Springer Lecture Notes **1050**, 1984.

[Rob49] Julia Robinson, *Definability and decision problems in arithmetic*, J. Symb. Logic **14(2)** (1949), 98-114.

[Rob59] —, *The undecidability of algebraic rings and fields*, Proc. AMS **10** (1959), 950-957.

[RRo51] Raphael M.Robinson, *Undecidable Rings*, Trans. AMS **70(1)** (1951), 137-159.

[Rub95] Lee A. Rubel, *An essay on diophantine equations for analytic functions*, Exp. Math **13** (1995), 81-92.

[Shl92] Alexandra Shlapentokh, *Hilbert's 10th Problem for rings of algebraic functions in one variable over fields of constants of positive characteristic*, Trans. AMS **333** (1992), 275-298.

[Shl00] —, *Hilbert's 10th Problem over number fields: a survey*, in [DPLG] (2000), 107-137.

[Shl07] —, *Hilbert's 10th Problem, Diophantine classes and extensions to global fields*, CUP 2007.

[SS89] Alexandra Shlapentokh, Harold N. Shapiro, *Diophantine relationships between algebraic number fields*, Comm. Pure Appl. Math. **42** (1989), 1113-1122.

[Sil86] Joseph H. Silverman, *The arithmetic of elliptic curves*, Springer 1986.

[Vdau03] Xavier Videaux, *An analogue of Hilbert's 10th problem for fields of meropmorphic functions over non-Archimedean valued fields*, J. Number Theory **101** (2003), 48-73.

[Vid94] Carlos Videla, *Hilbert's 10th Problem for rational function fields in characteristic 2*, Proc. AMS **120(1)** (1994), 249-253.

Mathematical Institute, Radcliff Observatory Quarter, Oxford OX2 6GG, UK
koenigsmann@maths.ox.ac.uk