Undecidability of expansions of Laurent series fields by cyclic discrete subgroups

Leo Gitin

University of Oxford, Oxford, U.K.
leo.gitin@maths.ox.ac.uk

Abstract

In 1987, Pheidas showed that the field of Laurent series $\mathbb{F}_q(\!(t)\!)$ with a constant for the indeterminate t and a predicate for the natural powers $\{t^n \mid n > 0\}$ of t is existentially undecidable. We show that the same result holds true if t is replaced by any element α of positive t-adic valuation.

Introduction. Hilbert's Tenth Problem asks for an *algorithm* that, given a polynomial $f(X_1, \dots, X_n)$ with integer coefficients, will determine whether or not it has a root in integers $\mathbb{Z}$, see [10, 11]. Building on previous work by Robinson, Davis, and Putnam, Matiyasevich famously showed that no such algorithm exists [16]. Hilbert's Tenth Problem can be equivalently phrased as asking whether or not the positive existential theory $\mathrm{Th}_{\exists^+}(\mathbb{Z})$ in the first-order language of rings $\mathcal{L}_{\mathrm{ring}} = \{0, 1, +, \cdot\}$ is decidable [13, 1.1] (in what follows, we will omit the symbols of $\mathcal{L}_{\mathrm{ring}}$ when speaking of ring structures). In the context of model theory, it is both natural to consider other structures $\mathcal{M}$ that may differ from $\mathbb{Z}$ and to extend the family of sentences that we look at (e.g. the existential theory $\mathrm{Th}_\exists(\mathcal{M})$ or the entire theory $\mathrm{Th}(\mathcal{M})$). Many classical results in logic and model theory subsume answers to decidability questions.

Before Matiyasevich's negative solution to Hilbert's Tenth Problem, it was already known by Gödel's work on his Incompleteness Theorems [8] that the full first-order $\mathcal{L}_{\mathrm{ring}}$-theory $\mathrm{Th}(\mathbb{Z})$ is undecidable. In the 1930s and 1950s, Tarski [18, 19] determined the $\mathcal{L}_{\mathrm{ring}}$-theories of the real and complex fields $\mathbb{R}$, $\mathbb{C}$ (the archimedean local fields) and consequently showed that both are decidable. Ax and Kochen [4] studied the model theory of non-archimedean local fields, i.e., p-adic fields K (finite field extensions of the p-adic numbers $\mathbb{Q}_p$) and Laurent series fields

$$\mathbb{F}_q(\!(t)\!) = \left\{ \sum_{i=-k}^{\infty} a_i t^i \,\middle|\, a_i \in \mathbb{F}_q,\ k \in \mathbb{Z} \right\}$$

over finite fields $\mathbb{F}_q$ with $q = p^n$ elements, p a prime number. It follows from their work that the theory $\mathrm{Th}(K)$ of any p-adic field K is decidable. Whether or not the Laurent series fields are decidable, is a major open question in the model theory of valued fields. In 2016, Anscombe and Fehm [2] made substantial progress towards this question by proving the decidability of the existential theory $\mathrm{Th}_\exists(\mathbb{F}_q(\!(t)\!))$ of Laurent series fields. For other recent results in this direction, we refer to Anscombe, Dittmann, and Fehm [1, 7].

It is natural to consider the structures mentioned above in expansions of the language of rings. Van den Dries [20] considered the real ordered field with a new predicate for $2^{\mathbb{Z}}$, the cyclic multiplicative subgroup generated by 2. He proves the surprising result that $(\mathbb{R}, 2^{\mathbb{Z}})$ is decidable by showing quantifier elimination in a natural expansion of $(\mathbb{R}, 2^{\mathbb{Z}})$. This still holds if 2 is replaced by a recursive real number $\alpha > 1$. In the same paper, van den Dries asks if his results can be generalised to the structure $(\mathbb{R}, 2^{\mathbb{Z}}, 3^{\mathbb{Z}})$. In 2010, Hieronymi [9] gave a negative answer: for two real numbers $\alpha, \beta > 1$ satisfying $\alpha^{\mathbb{Z}} \cap \beta^{\mathbb{Z}} = \{1\}$, the theory $\mathrm{Th}(\mathbb{R}, \alpha^{\mathbb{Z}}, \beta^{\mathbb{Z}})$ is undecidable. Expansions of $\mathbb{Q}_p$ by discrete cyclic (multiplicative) subgroups have been studied by Mariaule

[14, 15]. He proves that for $\alpha \in \mathbb{Q}_p$ of positive p-adic valuation $v_p(\alpha) > 0$, the theory $\mathrm{Th}(\mathbb{Q}_p, \alpha^{\mathbb{Z}})$ is decidable, whereas $\mathrm{Th}(\mathbb{Q}_p, \alpha^{\mathbb{Z}}, \beta^{\mathbb{Z}})$ is undecidable whenever $v_p(\beta) > 0$ and $\alpha^{\mathbb{Z}} \cap \beta^{\mathbb{Z}} = \{1\}$. Ax already knew (unpublished) that $\mathrm{Th}(\mathbb{F}_q(\!(t)\!), t^{\mathbb{Z}})$ is undecidable. An elementary proof was given by Becker, Denef, and Lipshitz [5]. Later, a considerable strengthening was obtained by Pheidas [17]. This is particularly interesting, as not much is known about these fields from the point of view of (un)decidability. He shows:

Theorem (Pheidas)**.** *Let $P = \{t^n \mid n > 0\}$ be the set of powers of the indeterminate t. Then $\mathrm{Th}_\exists(\mathbb{F}_q(\!(t)\!), t, P)$ is undecidable.*

Note that by virtue of Anscombe and Koenigsmann [3], who show that the valuation ring $\mathbb{F}_q[\![t]\!]$ in $\mathbb{F}_q(\!(t)\!)$ is existentially $\mathcal{L}_{\mathrm{ring}}$-definable without parameters, it follows moreover that $\mathrm{Th}_\exists(\mathbb{F}_q(\!(t)\!), t, t^{\mathbb{Z}})$ is undecidable (observe that $t^{\mathbb{Z}} \cap \mathbb{F}_q[\![t]\!] = P \cup \{1\}$). We generalise this theorem to arbitrary cyclic discrete subgroups of $\mathbb{F}_q(\!(t)\!)$, i.e., subgroups generated by an element α of positive t-adic valuation $v_t(\alpha)$.

Theorem. *Let $\alpha \in \mathbb{F}_q(\!(t)\!)$ be an element with $v_t(\alpha) > 0$. Then the existential theory of the structure $(\mathbb{F}_q(\!(t)\!), \alpha, \alpha^{\mathbb{Z}})$ is undecidable.*

See Remark 10 for a more general formulation. Another way of viewing $\alpha^{\mathbb{Z}}$ is to think of it as the image of a homomorphism from the value group $\mathbb{Z}$ into the multiplicative group $\mathbb{F}_q(\!(t)\!)^\times$. When $v_t(\alpha) = 1$, such a homomorphism is called a cross-section.

Pheidas' work. Pheidas proves his theorem in two steps. His key tool is the following (somewhat unusual) relation on natural numbers that goes back to Denef [6] and is sometimes called *p-divisibility*. We write

$$n \mid_p m \text{ if and only if } \exists k \in \mathbb{N}\ m = n \cdot p^k.$$

His proof now proceeds as follows.

(I) Prove that $\mathrm{Th}_\exists(\mathbb{N}, 0, 1, +, \mid_p)$ is undecidable by giving an existential definition of multiplication in this structure and invoking the Matiyasevich/MRDP theorem.

(II) Show that the relation $n \mid_p m$ can be effectively coded in $\mathbb{F}_q(\!(t)\!)$ by an existential formula via $P = \{t^n \mid n > 0\}$.

To generalise from t to arbitrary α, we precisely follow Pheidas' strategy. The main content of this note is to explain how Pheidas' coding needs to be modified in this more general context.

Essential to the coding is the unique arithmetic of $\mathbb{F}_q(\!(t)\!)$.

Remark 1. *In characteristic p, both the Frobenius map $x \longmapsto x^p$ and the Artin-Schreier map $x \longmapsto x^p - x$ are additive. Moreover, the Frobenius map is an automorphism on the finite field $\mathbb{F}_q$ and a non-surjective monomorphism on $\mathbb{F}_q(\!(t)\!)$ with image*

$$\mathbb{F}_q(\!(t^p)\!) = \left\{ \sum_{i=-k}^{\infty} a_{pi} t^{pi} \,\middle|\, a_{pi} \in \mathbb{F}_q,\ k \in \mathbb{Z} \right\}.$$

This is the field of p^{th} powers in $\mathbb{F}_q(\!(t)\!)$.

Lemma 2. *Fix an element $\alpha \in \mathbb{F}_q(\!(t)\!)$ with $v_t(\alpha) > 0$ not divisible by p. We can characterise the relation $n \mid_p m$ for natural $m, n > 0$ as follows:*

$$n \mid_p m \quad \textit{iff} \quad m \geq n \wedge \exists a \in \mathbb{F}_q(\!(t)\!)\ \alpha^{-m} - \alpha^{-n} = a^p - a. \tag{1}$$

Proof. Pheidas' proof [17, Lem. 1] for $\alpha = t$ goes through in this case. We will use this opportunity to show his beautiful argument.

Assume $n \mid_p m$ holds such that $m = n \cdot p^k$ for some $k \in \mathbb{N}$. In that case, the element

$$a = \alpha^{-np^{k-1}} + \alpha^{-np^{k-2}} + \ldots + \alpha^{-n}$$

witnesses the right-hand side of (1). Conversely, assume that for positive integers $m \geq n$, there exists $a \in \mathbb{F}_q((t))$ satisfying $\alpha^{-m} - \alpha^{-n} = a^p - a$. Write $m = m_0 p^{v_p(m)}$ and $n = n_0 p^{v_p(n)}$, where both $m_0, n_0 > 0$ are not divisible by p. By the first part of the proof, we can find $b, c \in \mathbb{F}_q((t))$ with

$$\alpha^{-m} - \alpha^{-m_0} = b^p - b$$
$$\alpha^{-n} - \alpha^{-n_0} = c^p - c.$$

Setting $d = a - b + c$, we can combine these three equations to $\alpha^{-m_0} - \alpha^{-n_0} = d^p - d$. If $m_0 = n_0$, we are done since $m \geq n$. Otherwise, we may assume $m_0 \neq n_0$, in which case

$$v_t(d^p - d) = v_t(\alpha^{-m_0} - \alpha^{-n_0}) = -v_t(\alpha) \max\{m_0, n_0\}.$$

We know $v_t(d) < 0$ implies that $v_t(d^p - d)$ is divisible by p, which is in contradiction to our assumptions that $v_t(\alpha)$, m_0, n_0 are not divisible by p. □

Remark 3. *Note that (1) still holds in the case when we can write $\alpha = \beta^{p^k}$, $k \in \mathbb{N}$, where $v_t(\beta)$ is not divisible by p. Indeed, for $m \geq n$, we have*

$$\exists a \in \mathbb{F}_q((t))\ \alpha^{-m} - \alpha^{-n} = \beta^{-mp^k} - \beta^{-np^k} = a^p - a$$

iff $np^k \mid_p mp^k$ iff $n \mid_p m$.

The general case. This characterisation of $\mid_p$ given by (1) will not work for all possible values of α, as we can see by the following counterexample.

Example 4. *Consider $p = q = 3$, i.e., the local field $\mathbb{F}_3((t))$ and the element*

$$\alpha = (t^{-3} + 1 + t + t^2)^{-1}$$

with $v_t(\alpha) = 3$ divisible by $p = 3$. Then $\alpha^{-2} - \alpha^{-1} = a^3 - a$ has a solution in $\mathbb{F}_3((t))$,

$$a = t^{-2} + t^{-1} - t + t^2 + \sum_{i \geq 0} (-1)^i (-t^{4 \cdot 3^i} + t^{6 \cdot 3^i}),$$

but the relation $1 \mid_3 2$ does not hold.

Hence a new observation is needed. For this purpose, we define the following unusual function, which we call the "p^{th}-powers-omitting t-adic valuation" for lack of a better name.*

Definition 5. *Given $x \in \mathbb{F}_q((t))$, written as a Laurent series*

$$x = \sum_{i=-k}^{\infty} a_i t^i,$$

*Note that, strictly speaking, $\hat{v}_t$ is not a valuation on $\mathbb{F}_q((t))$: it does not satisfy $x = 0 \iff \hat{v}_t(x) = \infty$ and it is also not a group homomorphism.

define $\hat{v}_t(x)$ to be the integer

$$\hat{v}_t(x) = \min\{i \mid a_i \neq 0 \wedge p \nmid i\},$$

and $\hat{v}_t(x) = \infty$ if this minimum does not exist, i.e., if $x \in \mathbb{F}_q((t^p))$.

Curiously, it captures exactly the kind of algebraic-combinatorial behaviour of $\mathbb{F}_q((t))$ that becomes invisible to v_t.

Lemma 6. *Assume that $\alpha \in \mathbb{F}_q((t))$ is not a p^{th} power, but $p \mid v_t(\alpha) > 0$. Let $N \in \mathbb{N}$ be not divisible by p. Then*

$$\hat{v}_t(\alpha^N) = (N-1)v_t(\alpha) + \hat{v}_t(\alpha).$$

Proof. Decompose α as $\alpha = \beta + \gamma$, where $\beta \neq 0$ contains all monomials with exponent divisible by p and $\gamma \neq 0$ contains all monomials with exponent not divisible by p. By our assumptions,

$$v_t(\beta) = v_t(\alpha) < \hat{v}_t(\alpha) = \hat{v}_t(\gamma).$$

Considering the binomial theorem for $(\beta+\gamma)^N$, we observe that

$$\binom{N}{N-1}\beta^{N-1}\gamma$$

must contain the monomial with smallest exponent not divisible by p. Thus

$$\hat{v}_t(\alpha^N) = \hat{v}_t(N\beta^{N-1}\gamma) = (N-1)v_t(\beta) + \hat{v}_t(\gamma) = (N-1)v_t(\alpha) + \hat{v}_t(\alpha). \qquad \square$$

Lemma 7. *Fix an element $\alpha \in \mathbb{F}_q((t))$ with valuation $v_t(\alpha) = C > 0$ divisible by p. Assume additionally that α is not a p^{th} power, so that $\hat{v}_t(\alpha^{-1}) = D \in \mathbb{Z}$. Then for any choice of $N > 0$ satisfying*

$$N > \frac{D}{C} + 1 \quad \textit{and} \quad p \nmid N,$$

we have

$$n \mid_p m \quad \textit{iff} \quad m \geq n \wedge \exists a \in \mathbb{F}_q((t))\ \alpha^{-mN} - \alpha^{-nN} = a^p - a$$

for all $m, n > 0$.

Proof. If $n \mid_p m$ holds, we essentially take the same witness $a \in \mathbb{F}_q((t))$ as in Lemma 2. As for the converse, let us consider positive integers $m \geq n$ such that there exists $a \in \mathbb{F}_q((t))$ with

$$\alpha^{-mN} - \alpha^{-nN} = a^p - a.$$

By repeating the same steps as in the proof of Lemma 2, we can write $m = m_0 p^{v_p(m)}$, $n = n_0 p^{v_p(n)}$ and find $d \in \mathbb{F}_q((t))$ such that

$$\alpha^{-m_0 N} - \alpha^{-n_0 N} = d^p - d. \tag{2}$$

We are done if $m_0 = n_0$. So assume without loss of generality that $m_0 > n_0 \geq 1$. Instead of considering the t-adic valuation on both sides of (2), we look at the p^{th}-powers-omitting t-adic valuation instead. By Lemma 6 and $p \nmid m_0 N$, we observe

$$\hat{v}_t(\alpha^{-m_0 N} - \alpha^{-n_0 N}) = -(m_0 N - 1)C + D. \tag{3}$$

If we evaluate the right-hand side of (2), we get

$$\hat{v}_t(d^p - d) = \hat{v}_t(d) \geq v_t(d). \tag{4}$$

Since $v_t(d) < 0$, we can use

$$pv_t(d) = v_t(d^p - d) = v_t(\alpha^{-m_0 N} - \alpha^{-n_0 N}) = -m_0 NC,$$

together with (2), (3), and (4), to deduce the inequality

$$-(m_0 N - 1)C + D \geq \frac{-m_0 NC}{p}.$$

After rearranging, we have

$$N \leq \frac{Cp + Dp}{m_0 C(p-1)} = \frac{C + D}{C} \frac{p}{m_0(p-1)} \leq \frac{D}{C} + 1,$$

contradicting our choice of N. Hence $m_0 = n_0$. □

In Example 4, it would suffice to take $N = 2$.

By combining Lemma 2 and Lemma 7, we can complete our coding of $|_p$ inside $\mathbb{F}_q((t))$.

Proposition 8. *Fix an element $\alpha \in \mathbb{F}_q((t))$ with valuation $v_t(\alpha) > 0$. Then there exists a parameter $N > 0$, depending on α, such that*

$$n \mid_p m \quad \textit{iff} \quad m \geq n \wedge \exists a \in \mathbb{F}_q((t)) \ \alpha^{-mN} - \alpha^{-nN} = a^p - a$$

holds for all $m, n > 0$.

Proof. Write $\alpha = \beta^{p^k}$, $k \in \mathbb{N}$, such that β is not a p^{th} power in $\mathbb{F}_q((t))$. We consider two cases:

Case 1. p does not divide $v_t(\beta)$. By Lemma 2 and Remark 3, we can choose $N = 1$.

Case 2. p divides $v_t(\beta)$. By Lemma 7 and Remark 3, we can choose N to be the smallest natural number not divisible by p bigger than $\hat{v}_t(\beta^{-1})/v_t(\beta) + 1$. □

From this, we conclude our main theorem.

Theorem 9. *Let $\alpha \in \mathbb{F}_q((t))$ be an element with $v_t(\alpha) > 0$. Then the existential theory of the structure $(\mathbb{F}_q((t)), \alpha, \alpha^{\mathbb{Z}})$ is undecidable.*

Proof. First, we identify $\{\alpha^n \mid n > 0\}$ in this structure. This set is given by $\alpha^{\mathbb{Z}} \cap \mathbb{F}_q[[t]] \setminus \{1\}$. In [3], Anscombe and Koenigsmann show that $\mathbb{F}_q[[t]]$ is existentially $\mathcal{L}_{\text{ring}}$-definable in $\mathbb{F}_q((t))$ without parameters, so the same is true of $\{\alpha^n \mid n > 0\}$ inside $(\mathbb{F}_q((t)), \alpha, \alpha^{\mathbb{Z}})$. By Proposition 8, we can interpret $(\mathbb{N}, 0, 1, +, |_p)$ in $(\mathbb{F}_q((t)), 0, 1, +, \cdot, \alpha, \alpha^{\mathbb{Z}})$ using existential formulas. By (I), $\text{Th}_\exists(\mathbb{N}, 0, 1, +, |_p)$ is undecidable, so $\text{Th}_\exists(\mathbb{F}_q((t)), \alpha, \alpha^{\mathbb{Z}})$ must also be undecidable. □

Remark 10. *Pheidas formulates his theorem in slightly more general terms: for any integral domain F of characteristic p, quotient field K of F, and intermediate ring $F[t] \subseteq R \subseteq K((t))$, the existential theory $\text{Th}_\exists(R, t, P)$ is undecidable. The same is true of our result: as long as $\alpha \in R$, we have that $\text{Th}_\exists(R, \alpha, \{\alpha^n \mid n > 0\})$ is undecidable (essentially by the same proof).*

More recently, an adaption of Pheidas' theorem via the so-called Krasner-Kazhdan-Deligne philosophy was obtained by Kartas [12], who shows that the asymptotic theory of all p-adic fields is undecidable in the language of rings with a cross-section. We hope to further adapt these types of results to infinitely ramified valued fields.

Acknowledgements. First and foremost, I would like to express my gratitude to Philipp Hieronymi who advised this work in 2022. Moreover, I would like to thank Philip Dittmann, Konstantinos Kartas, and Jochen Koenigsmann for valuable comments that helped improve the exposition of this note.

References

[1] Sylvy Anscombe, Philip Dittmann, and Arno Fehm. Axiomatizing the existential theory of $\mathbb{F}_q((t))$. *Algebra & Number Theory*, 17(11):2013–2032, 2023.

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

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

[4] James Ax and Simon B. Kochen. Diophantine problems over local fields I. *American Journal of Mathematics*, 87(3):605–630, 1965.

[5] Joseph Becker, Jan Denef, and Leonard Lipshitz. Further remarks on the elementary theory of formal power series rings. In *Model Theory of Algebra and Arithmetic*, pages 1–9. Springer, 1980.

[6] Jan Denef. The diophantine problem for polynomial rings of positive characteristic. In *Logic Colloquium '78, Proceedings of the colloquium held in Mons*, pages 131–145. Elsevier, 1979.

[7] Philip Dittmann and Arno Fehm. On the existential theory of the completions of a global field, 2024. Preprint, arXiv:2401.11930.

[8] Kurt Gödel. Über formal unentscheidbare Sätze der Principia Mathematica und verwandter Systeme I. *Monatshefte für Mathematik und Physik*, 38(1):173–198, 1931.

[9] Philipp Hieronymi. Defining the set of integers in expansions of the real field by a closed discrete set. *Proceedings of the American Mathematical Society*, 138(06):2163–2168, 2010.

[10] David Hilbert. Mathematische Probleme. In *Nachrichten von der Königl. Gesellschaft der Wissenschaften zu Göttingen, mathematisch-physikalische Klasse*, Heft 3, pages 253–297. Dieterichsche Universitätsbuchhandlung, Göttingen, 1900.

[11] David Hilbert. Mathematical problems. *Bulletin of the American Mathematical Society*, 8(10):437–479, 1902.

[12] Konstantinos Kartas. An undecidability result for the asymptotic theory of p-adic fields. *Annals of Pure and Applied Logic*, 174(2):103203, 2023.

[13] Jochen Koenigsmann. Decidability in local and global fields. In *Proceedings of the International Congress of Mathematicians (ICM 2018)*. World Scientific, 2019.

[14] Nathanaël Mariaule. Model theory of the field of p-adic numbers expanded by a multiplicative subgroup, 2018. Preprint, arXiv:1803.10564.

[15] Nathanaël Mariaule. Expansions of the p-adic numbers that interpret the ring of integers. *Mathematical Logic Quarterly*, 66(1):82–90, 2020.

[16] Yuri V. Matiyasevich. *Hilbert's Tenth Problem.* Foundations of Computing Series. MIT Press, Cambridge, MA, 1993.

[17] Thanases Pheidas. An undecidability result for power series rings of positive characteristic. II. *Proceedings of the American Mathematical Society*, 100(3):526–530, 1987.

[18] Alfred Tarski. Sur les ensembles définissables de nombres réels. *Fundamenta Mathematicae*, 17(1):210–239, 1931.

[19] Alfred Tarski and J. C. C. McKinsey. *A Decision Method for Elementary Algebra and Geometry.* University of California Press, 1951.

[20] Lou van den Dries. The field of reals with a predicate for the powers of two. *manuscripta mathematica*, 54(1-2):187–195, 1985.