# Decidability in expansions of local fields

Leo Gitin

Born 23rd October 1999 in Leipzig, Germany

June 13, 2022

Master's Thesis Mathematics

Advisor: Prof. Dr. Philipp Hieronymi

Second Advisor: Prof. Dr. Peter Koepke

Mathematisches Institut

Mathematisch-Naturwissenschaftliche Fakultät der

Rheinischen Friedrich-Wilhelms-Universität Bonn

Contents

## 1. Introduction

Among the list of 23 problems David Hilbert presented to the International Congress of Mathematicians in Paris in the year 1900, the following—particularly short one—stands out.

**Hilbert's Tenth Problem**

> Eine Diophantische Gleichung mit irgend welchen Unbekannten und mit ganzen rationalen Zahlencoefficienten sei vorgelegt: *man soll ein Verfahren angeben, nach welchem sich mittelst einer endlichen Anzahl von Operationen entscheiden läßt, ob die Gleichung in ganzen rationalen Zahlen lösbar ist.* [10]
>
> Given a diophantine equation with any number of unknown quantities and with rational integral numerical coefficients: *To devise a process according to which it can be determined by a finite number of operations whether the equation is solvable in rational integers.* [11]

Today, we would say that Hilbert's Tenth Problem asks for an *algorithm* that, given a polynomial $f(X_1, \dots, X_n)$ with coefficients in $\mathbb{Z}$ as input, will output Yes if $f(X_1, \dots, X_n)$ has a solution in $\mathbb{Z}$, and No if $f(X_1, \dots, X_n)$ has no solution in $\mathbb{Z}$.

Seventy years after Hilbert had presented his problems, Matiyasevich famously showed that no such algorithm exists, building on previous work of Robinson, Davis and Putnam. In other words, Hilbert's Tenth Problem has a negative answer (see [17] for a self-contained treatment on this result). It is evident that a rigorous notion of algorithm is needed to prove such a negative result. *Turing machines* provide such a rigorous notion, as well as other models of computation introduced in the 1930s by Church, Kleene and Post (see [5, Chap. 8]).

If we look at Hilbert's Tenth Problem from the point of view of logic, then this problem is asking for an algorithm that decides which sentences of the form

$$\exists x_1 \dots \exists x_n \ f(x_1, \dots, x_n) = 0,$$

in the language of rings $\mathcal{L}_{\text{ring}} = \{0, 1, +, -, \cdot\}$, hold in $\mathbb{Z}$ or not. From this point of view, it is reasonable to ask for a more general algorithm that would decide for *any* $\mathcal{L}_{\text{ring}}$-sentence $\varphi$ whether it is satisfied in $\mathbb{Z}$ or not. However, the existence of such an algorithm can be seen to be ruled out by Gödel's 1931 landmark work [8] on his Incompleteness Theorems.

So far, we have mentioned two decision problems with a negative solution. There are nonetheless important decision problems with a positive solution. Given a first-order language $\mathcal{L}$, we say that an $\mathcal{L}$-theory $T$ is *decidable* if there is an algorithm that, given an $\mathcal{L}$-sentence $\varphi$ as input, will output Yes if $\varphi \in T$, and No if $\varphi \notin T$. An $\mathcal{L}$-structure $\mathcal{M}$ is said to be decidable if $\mathrm{Th}(\mathcal{M})$ is decidable (see Section 2.1 for more precise definitions). Tarski showed that the structure of the real ordered field

$$(\mathbb{R}, 0, 1, +, -, \cdot, \leq)$$

is decidable. He found this result already in 1930; one year later, he mentioned it implicitly and without proof in [22]. A full proof was published only twenty years later in [23], after the Second World War. We will briefly discuss the decidability of the theory of the real ordered field in Section 2.3. Another example of a decidable theory, namely *Presburger arithmetic*, will be given in Section 2.1.

One can describe the negative solution to Hilbert's Tenth Problem as a metamathematical theorem of number theory—the objects of study are algorithms that determine, for all Diophantine equations, whether they have an integer solution or not. Motivated, in contrast, by concrete conjectures about Diophantine equations, Ax and Kochen studied the model theory of valued fields in 1965 (see [3]). They obtained, among other things, a decidability result linking back to the subject of decidable theories: they showed that the $\mathcal{L}_{\text{ring}}$-theory of the field $\mathbb{Q}_p$ of *p-adic numbers* is decidable [4]. The field $\mathbb{Q}_p$, a central object in number theory, is the completion of $\mathbb{Q}$ with respect to the $p$-adic absolute value $|\cdot|_p$. In Section 2.2, we will define absolute values and cover other number theoretic prerequisites. We will see that $\mathbb{R}$ and $\mathbb{Q}_p$ are instances of *local fields*. In general, there are three types of local fields:

- the real field $\mathbb{R}$ and complex field $\mathbb{C}$ (archimedean local fields);
- finite extensions $K$ of $\mathbb{Q}_p$ ($p$-adic fields);
- fields of formal Laurent series $\mathbb{F}_q(\!(t)\!)$ over finite fields with $q = p^r$ elements (local fields of characteristic $p$).

It is remarkable that although the decidability of $\mathbb{R}$, $\mathbb{C}$, and all $p$-adic fields $K$ (see [21, Cor. 5.3]) in the language of rings has been established, it is not known whether or not $\mathbb{F}_q(\!(t)\!)$ is decidable. As of today, this is still a major open problem. There has been some recent progress, e.g. Anscombe and Fehm [1] showed that the existential theory of $\mathbb{F}_q(\!(t)\!)$ is decidable (see [12] for a discussion of other partial results).

Until this point, we have only considered questions regarding decidability in the language of rings or ordered rings. Generalisations of Hilbert's Tenth Problem can be obtained by expanding the language we work in. For example, Tarski asked in [23] whether the structure of the ordered real field together with the exponential function,

$$\mathbb{R}_{\exp} = (\mathbb{R}, 0, 1, +, -, \cdot, \leq, \exp),$$

is decidable (Tarski's exponential function problem). This question leads to the study of o-minimal structures (see [25] for an introduction to this subject). Macintyre and Wilkie proved the conditional result that a weak version of Schanuel's conjecture implies that $\mathbb{R}_{\exp}$ is decidable, see [13].

Another natural expansion of the real ordered field is obtained by adding a relation symbol for small subgroups of $\mathbb{R}$. Any non-trivial discrete additive subgroup of $\mathbb{R}$ is of the form $c\mathbb{Z}$ for some constant $c \in \mathbb{R}_{>0}$. Adding a relation symbol for this subgroup leads to the same obstruction for decidability as we encountered in the structure $(\mathbb{Z}, +, \cdot)$ by virtue of Gödel's Incompleteness Theorem. A more interesting question is obtained by adding a relation symbol for non-trivial discrete *multiplicative* subgroups. In [24], van den Dries proves that the real ordered field together with a predicate for $2^{\mathbb{Z}}$, the cyclic multiplicative subgroup generated by $2 \in \mathbb{R}$, is decidable. This generalises to cyclic subgroups generated by any $\alpha \in \mathbb{R}_{>1}$ as follows.

**Theorem 1.1** (van den Dries [24])**.** *Let $\alpha \in \mathbb{R}_{>1}$ be a fixed constant that is recursive. Then*

$$(\mathbb{R}, 0, 1, +, -, \cdot, \leq, \alpha^{\mathbb{Z}})$$

*is decidable.*

A real number $\alpha$ is called *recursive* if there is an algorithm that can compute its decimal representation to any given degree of accuracy. This includes all real algebraic numbers,

but also transcendental constants such as $e$ or $\pi$. In Section 3.1, we will present van den Dries proof [24] with minor modifications made necessary by considering a general constant $\alpha \in \mathbb{R}_{>1}$. Let us also mention a similar result for the field of complex numbers:

**Theorem 1.2** (van den Dries, Günaydin [26, Cor. 8.8]). *Let $\alpha \in \mathbb{C}^\times$ be any non-zero complex number. Then $(\mathbb{C}, 0, 1, +, -, \cdot, \alpha^{\mathbb{Z}})$ is decidable.*

In [24], van den Dries asks whether his result also applies to the structure $(\mathbb{R}, +, \cdot, 2^{\mathbb{Z}}, 3^{\mathbb{Z}})$. This was answered negatively by Hieronymi in [9], where he shows that the real field with predicates for two cyclic subgroups is undecidable.

**Theorem 1.3** (Hieronymi [9]). *Let $\alpha, \beta \in \mathbb{R}_{>1}$ be two real numbers satisfying $\alpha^{\mathbb{Z}} \cap \beta^{\mathbb{Z}} = \{1\}$, or equivalently, $\log_\alpha(\beta) \notin \mathbb{Q}$. Then the theory of the structure $(\mathbb{R}, +, \cdot, \alpha^{\mathbb{Z}}, \beta^{\mathbb{Z}})$ is undecidable.*

In this thesis, we will investigate questions of decidability for local fields with predicates for discrete infinite cyclic subgroups. For the field of reals $\mathbb{R}$, we have stated the main results. The question for the $p$-adic numbers $\mathbb{Q}_p$ was considered by Mariaule in [14] and [15].

**Theorem 1.4** (Mariaule [14], [15]). *Let $v_p$ be the $p$-adic valuation on $\mathbb{Q}_p$.*

*(i) If $\alpha \in \mathbb{Q}_p$ is an element satisfying $v_p(\alpha) > 0$, then $(\mathbb{Q}_p, +, \cdot, \alpha^{\mathbb{Z}})$ is decidable.*

*(ii) If $\alpha, \beta \in \mathbb{Q}_p$ are two elements with $v_p(\alpha), v_p(\beta) > 0$ and $\alpha^{\mathbb{Z}} \cap \beta^{\mathbb{Z}} = \{1\}$, then the theory of $(\mathbb{Q}_p, +, \cdot, \alpha^{\mathbb{Z}}, \beta^{\mathbb{Z}})$ is undecidable.*

For the field of formal Laurent series $\mathbb{F}_q(\!(t)\!)$, Pheidas proved the following undecidability result:

**Theorem 1.5** (Pheidas [20]). *Let $P = \{t^n \mid n \in \mathbb{Z}_{>0}\}$ be the set of positive powers of the indeterminate $t$. Then the existential theory of $(\mathbb{F}_q(\!(t)\!), 0, 1, +, \cdot, t, P)$ is undecidable.*

We will generalise these results, establishing undecidability for all non-archimedean local fields with enough predicates for discrete infinite cyclic subgroups.

**Theorem 1.6.** *Let $K$ be a $p$-adic field and $v$ the unique discrete valuation on $K$. Assume that $\alpha, \beta \in K$ are two elements with $v(\alpha), v(\beta) > 0$ and $\alpha^{\mathbb{Z}} \cap \beta^{\mathbb{Z}} = \{1\}$. Then $(K, +, \cdot, \alpha^{\mathbb{Z}}, \beta^{\mathbb{Z}})$ is undecidable.*

**Theorem 1.7.** *Let $\mathbb{F}_q(\!(t)\!)$ be a local field of characteristic $p$ and $v_t$ its $t$-adic valuation. Assume that $\alpha \in \mathbb{F}_q(\!(t)\!)$ is an element with $v_t(\alpha) > 0$. Then the existential theory of the structure $(\mathbb{F}_q(\!(t)\!), +, \cdot, \alpha, \alpha^{\mathbb{Z}})$ is undecidable. In particular, $(\mathbb{F}_q(\!(t)\!), +, \cdot, \alpha^{\mathbb{Z}})$ is undecidable.*

In our final section (Section 4) we will prove these two theorems, as well as Hieronymi's undecidability result for $(\mathbb{R}, +, \cdot, \alpha^{\mathbb{Z}}, \beta^{\mathbb{Z}})$ using various different techniques. It is the main theme of this thesis that although all types of local fields share topological and number theoretic properties[1], the way we approach decidability questions depends crucially on the

[1] E.g. they are locally compact topological fields, are complete with respect to their absolute value, and satisfy the same reciprocity laws in local class field theory.

specific arithmetic of the local field. Note that for $\mathbb{R}$ and $p$-adic fields $K$ we need two predicates for cyclic subgroups for undecidability to occur, whereas for $\mathbb{F}_q(\!(t)\!)$ we only need one. So in particular, the characteristic of the field plays an important role. We will use valuations for various proofs, but in each case in a different way: in the proof of Theorem 1.1, the natural valuation of an ordered field (introduced in Section 2.2) will make an appearance as a systematic way of thinking about infinitesimals, whereas in the proof of Theorem 1.7, we will use the $t$-adic valuation to show that certain Artin-Schreier polynomials do not have solutions in $\mathbb{F}_q(\!(t)\!)$.

The proof of Theorem 1.3 will be fairly analytic in nature. One constructs a particular sequence with definable range, to which the lemma on asymptotic extraction of groups (Lemma 4.1.2) can be applied. This way we can show that $\mathbb{Z}$ is definable in $(\mathbb{R}, +, \cdot, \alpha^{\mathbb{Z}}, \beta^{\mathbb{Z}})$ by a formula with one parameter, and undecidability of this structure can be reduced to the undecidability of $(\mathbb{Z}, +, \cdot)$. The proofs of Theorem 1.6 and Theorem 1.7 will, at the end, also invoke the undecidability of $(\mathbb{Z}, +, \cdot)$ or the negative solution to Hilbert's Tenth Problem. However, we will not prove that $\mathbb{Z}$ is definable in these structures. Instead, we will show that certain undecidable expansion of Presburger arithmetic $(\mathbb{N}, 0, 1, +)$ can be interpreted in $(K, +, \cdot, \alpha^{\mathbb{Z}}, \beta^{\mathbb{Z}})$, respectively $(\mathbb{F}_q(\!(t)\!), +, \cdot, \alpha, \alpha^{\mathbb{Z}})$. Thus we proceed in two steps: first, we prove that certain expansions of Presburger arithmetic are undecidable.

**Proposition.** *Let $p$ be a prime number. Let $v_p$ be the $p$-adic valuation on $\mathbb{N}_{>0}$, i.e., $v_p(n)$ is the largest $k \in \mathbb{N}$ such that $p^k \mid n$. Set $v_p(0) = 0$. Let $|_p$ be a binary relation on $\mathbb{N}$ defined by $n \,|_p\, m$ if and only if $\exists k \in \mathbb{N}\ m = p^k n$. Then the elementary theory of $(\mathbb{N}, +, v_p)$ and the existential theory of $(\mathbb{N}, 0, 1, +, |_p)$ are undecidable.*

In a second step, we show that $(\mathbb{N}, +, v_p)$, respectively $(\mathbb{N}, 0, 1, +, |_p)$, are interpretable in $(K, +, \cdot, \alpha^{\mathbb{Z}}, \beta^{\mathbb{Z}})$, respectively $(\mathbb{F}_q(\!(t)\!), +, \cdot, \alpha, \alpha^{\mathbb{Z}})$. Mariaule [15] and Pheidas [20] follow the same proof strategy. However, in the proof of Theorem 1.7, we need to modify Pheidas' interpretation of $(\mathbb{N}, 0, 1, +, |_p)$ in $(\mathbb{F}_q(\!(t)\!), +, \cdot, \alpha, \alpha^{\mathbb{Z}})$, which will not work for general $\alpha$. The proof changes insofar as that instead of analysing equations by their $t$-adic valuation, we will consider their $p^{\text{th}}$-power-omitting $t$-adic valuation (introduced in Definition 4.3.5).

*Acknowledgements.* I would like to thank Prof. Philipp Hieronymi for his guidance during the preparation of this thesis. I am particularly grateful for several helpful remarks, especially regarding the proof Theorem 4.1. I wish to extend my thanks to Margarete Ketelsen and Sebastian Meyer who offered valuable comments.

## 2. Preliminaries

The purpose of this section is to recall the necessary prerequisites for studying decidability questions in local fields.

**Note on notation.** The blackboard bold letter $\mathbb{N}$ stands for the non-negative integers.

We will use calligraphic letters $\mathcal{A}, \mathcal{M}, \mathcal{N}, \ldots$ etc. for structures and models of theories, and uppercase letters $A, M, N, \ldots$ etc. for their domains of definition. If $\mathcal{L}$ is a first-order language and $\mathcal{M}$ an $\mathcal{L}$-structure, then $\mathrm{Th}(\mathcal{M})$ resp. $\mathrm{Th}_\exists(\mathcal{M})$ is the set of $\mathcal{L}$-sentences resp. existential $\mathcal{L}$-sentences that are true in $\mathcal{M}$.

If $\mathcal{M} = (M, <, \ldots)$ is an ordered structure, then for any $x \in M$, we write

$$M_{>x} = \{y \in M \mid y > x\}$$
$$M_{\geq x} = \{y \in M \mid y \geq x\}.$$

### 2.1. Decidable and undecidable theories.

**Definition 2.1.1.** A subset $A$ of the set of natural numbers $\mathbb{N}$ is called *recursive* (or *computable*) if the characteristic function $\chi_A : \mathbb{N} \longrightarrow \{0, 1\}$

$$\chi_A(n) = \begin{cases} 1 & \text{if } n \in A \\ 0 & \text{if } n \notin A \end{cases}$$

is computable, i.e., there is a Turing machine that for inputs $n$ will output $\chi_A(n)$.

There are many other equivalent ways of defining computability, all of which have in common that they are descriptions of "effective methods" of computing functions (cf. Church-Turing thesis, see [5, Chap. 8]).

In logic, one is primarily concerned with formal symbols and formulas, not natural numbers. However, we can use the notion of computability in logic if we assign to each symbol, term, and formula a unique natural number called *Gödel number*. Such an assignment is called *Gödel numbering*. Thus we can call a first-order language or a set of formulas recursive, if the corresponding set of Gödel numbers is recursive (see [5, Chap. 15] for more details on Gödel numberings and its properties).

**Definition 2.1.2.** Let $\mathcal{L}$ be a countable recursive first-order language and $S_\mathcal{L}$ the set of all $\mathcal{L}$-sentences. An $\mathcal{L}$-theory $T$ is called *decidable* if there is an effective method (i.e. an algorithm) that determines for any given sentence $\varphi \in S_\mathcal{L}$, whether $\varphi \in T$ or $\varphi \notin T$. To be more precise, we say that $T$ is decidable if the set of Gödel numbers

$$\{\ulcorner \varphi \urcorner \mid \varphi \in T\} \subseteq \mathbb{N}$$

is recursive, where $\ulcorner \varphi \urcorner$ denotes the Gödel number of $\varphi$. We say that an $\mathcal{L}$-structure $\mathcal{M}$ is *decidable* if $\mathrm{Th}(\mathcal{M})$ is decidable, otherwise we say that $\mathcal{M}$ is *undecidable*.

We will be concerned with the question of whether a certain structure (or family of structures) is decidable or not. We will need a method of proof both for showing that a theory is decidable and that a theory is undecidable. The following theorem will be used to show decidability.

**Theorem 2.1.3.** *Let $\mathcal{L}$ be a countable recursive language and $\mathcal{M}$ an $\mathcal{L}$-structure. Let $\Sigma$ be a complete recursive axiomatisation for $\mathcal{M}$, i.e., $\mathcal{M} \models \Sigma$, $\Sigma \models \mathrm{Th}(\mathcal{M})$, and $\Sigma$ is recursive. Then $\mathcal{M}$ is decidable.*

We can give a short reasoning for why this theorem is true. Given $\varphi \in \mathrm{Th}(\mathcal{M})$, there must be a formal derivation of $\varphi$ from a finite subset $\Sigma_0$ of $\Sigma$ by Gödel's Completeness Theorem. One can contrive an algorithm, that after receiving an $\mathcal{L}$-sentence $\psi \in S_{\mathcal{L}}$ as input, goes one by one through all (countably many) derivations from finite subsets of $\Sigma$. After finitely many steps, it will find a formal derivation whose consequence is either $\psi$ or $\neg\psi$, because $\Sigma$ is complete. Then it will output 1 if $\psi$ is found to be consequence of $\Sigma$, and 0 if $\neg\psi$ is found to be a consequence of $\Sigma$. For a more precise proof of the above theorem, we refer to [5, 15.7].

**Example 2.1.4.** One of the first instances of a theory that was found to be decidable is *Presburger arithmetic*[2], the theory of $(\mathbb{Z}, 0, 1, +, -, <)$. This theory has quantifier elimination in an expanded language. Consider

$$\mathcal{L}_{\mathrm{Pres}} = \{0, 1, +, -, <\} \cup \{P_n\}_{n \geq 1},$$

where the $P_n$ are unary relation symbols that are to be interpreted as the multiples of $n$. Let $T_{\mathrm{Pres}}$ be the $\mathcal{L}_{\mathrm{Pres}}$-theory consisting of

(i) axioms for ordered abelian groups;

(ii) $0 < 1$;

(iii) $\forall x\,(x > 0 \to x \geq 1)$;

(iv) $\forall x\,(P_n(x) \leftrightarrow \exists y\; x = \underbrace{y + \ldots + y}_{n \text{ times}})$ for all $n \geq 1$;

(v) $\forall x \bigvee_{i=0}^{n-1} \left[ P_n(x + \underbrace{1 + \ldots + 1}_{i \text{ times}}) \wedge \bigwedge_{j \neq i} \neg P_n(x + \underbrace{1 + \ldots + 1}_{j \text{ times}}) \right]$ for all $n \geq 1$.

Clearly, $(\mathbb{Z}, 0, 1, +, -, <, \{n\mathbb{Z}\}_{n \geq 1})$ satisfies these axioms. If $\mathcal{Z}$ is another model of $T_{\mathrm{Pres}}$ with domain $Z$, then axiom (iii) says that there are no element in $Z$ between 0 and 1, (iv) says that $P_n^{\mathcal{Z}} = nZ$, and (v) says that $Z/nZ \cong \mathbb{Z}/n\mathbb{Z}$. It turns out that this theory has quantifier elimination and is in fact a complete axiomatisation for $(\mathbb{Z}, 0, 1, +, -, <, \{n\mathbb{Z}\}_{n \geq 1})$ (see [16, Cor. 3.1.21] for a proof of this statement). Looking at the list of axioms in $T_{\mathrm{Pres}}$, we see that it is recursive, so by Theorem 2.1.3 we have that $(\mathbb{Z}, 0, 1, +, -, <, \{n\mathbb{Z}\}_{n \geq 1})$ is decidable. In particular, $(\mathbb{Z}, 0, 1, +, -, <)$ is also decidable (its theory contains the same sentences, except those that use the symbols $P_n$). ⊣

We will later see another example of a decidable theory, the *theory of real closed fields* (see Theorem 2.3.7). Section 3.1 will contain a full proof of quantifier elimination for a certain theory, from which completeness and decidability can be inferred.

We will use the following basic example to show undecidability.

[2]The theory of $(\mathbb{N}, 0, 1, +)$ is also called Presburger arithmetic. One should note that these theories are mutually interpretable in each other.

**Example 2.1.5.** As mentioned in the introduction, the theory of $(\mathbb{Z}, +, \cdot)$ is undecidable by Gödel's Incompleteness Theorem. Moreover, Matiyasevich's negative solution to Hilbert's Tenth Problem implies that the existential theory of $(\mathbb{Z}, 0, 1, +, -, \cdot)$ is undecidable. ⊣

If we can show that theory of $(\mathbb{Z}, +, \cdot)$ or the existential theory of $(\mathbb{Z}, 0, 1, +, -, \cdot)$ can be effectively coded in a given theory $T$, then $T$ will be undecidable. This method of proof will be used in Section 4 to show undecidability of expansion of local fields.

## 2.2. **Valuations and local fields.**

§ 1. *Absolute value and valuation.* An absolute value on a field is a measure of distance. It is defined by three axioms.

**Definition 2.2.1.** A *valued field* $(K, |\cdot|)$ is a field $K$, together with a map $|\cdot| : K \longrightarrow \mathbb{R}_{\geq 0}$ satisfying

(i) $|x| = 0 \Longleftrightarrow x = 0$

(ii) $|xy| = |x| \cdot |y|$

(iii) $|x + y| \leq |x| + |y|$ (*triangle inequality*),

for all $x, y \in K$. We call $|\cdot|$ an *absolute value* on $K$. We say it is *non-archimedean* if it satisfies the strengthened axiom

(iii') $|x + y| \leq \max\{|x|, |y|\}$ (*ultrametric inequality*).

If this is not the case, we say that $|\cdot|$ is *archimedean.*

**Example 2.2.2.** If $|\cdot|_\infty$ is the Euclidean norm, then $(\mathbb{Q}, |\cdot|_\infty)$, $(\mathbb{R}, |\cdot|_\infty)$, and $(\mathbb{C}, |\cdot|_\infty)$ are archimedean valued fields. ⊣

Non-archimedean valued fields have an alternative description.

**Definition 2.2.3.** A *(rank 1) valuation*[3] on a field $K$ is a map

$$v : K \longrightarrow \mathbb{R} \cup \{\infty\}$$

satisfying the axioms

(i) $v(x) = \infty \Longleftrightarrow x = 0$

(ii) $v(xy) = v(x) + v(y)$

(iii) $v(x + y) \geq \min\{v(x), v(y)\}$,

for all $x, y \in K$. Here, we assume the conventions

$$x + \infty = \infty + x = \infty + \infty = \infty \qquad (2.2.1)$$
$$x < \infty$$

for all $x \in \mathbb{R}$. The image $v(K^\times)$ of $K^\times$ under $v$ is called *value group.*

[3]Rank 1 refers to the fact that the value group $v(K^\times)$ is a subgroup of the ordered group of reals.

The notions of non-archimedean absolute value and (rank 1) valuation are basically equivalent: if we fix $c \in (0,1)$, then $|x| = c^{v(x)}$ turns a valuation $v$ into a non-archimedean absolute value. Conversely, the definition $v(x) = \log_c |x|$ turns a non-archimedean absolute value into a valuation. Essentially, we are only switching between additive and multiplicative notation for the value group. We say that two valuations $v_1$ and $v_2$ are *equivalent* if there is a constant $C > 0$ such that $v_2 = C \cdot v_1$. Likewise, we say that two absolute values $|\cdot|_1$ and $|\cdot|_2$ are equivalent if $|\cdot|_2 = |\cdot|_1^C$ for some constant $C > 0$.

If we do not restrict ourselves to value groups $v(K^\times) \subseteq \mathbb{R}$, but instead allow arbitrary ordered groups, we get a more general notion.

**Definition 2.2.4.** Let $K$ be a field and $(\Gamma, \leq)$ a totally ordered abelian group. A *valuation* $v$ on $K$ with value group $\Gamma$ is a surjective map

$$v : K \longrightarrow\!\!\!\!\!\rightarrow \Gamma \cup \{\infty\}$$

satisfying the properties

(i) $v(x) = \infty \iff x = 0$

(ii) $v(xy) = v(x) + v(y)$

(iii) $v(x+y) \geq \min\{v(x), v(y)\}$,

for all $x, y \in K$. Again, we suppose that $\infty$ is subject to the relations (2.2.1). We say $v$ is *trivial* if it has trivial value group $\Gamma = 0$. We say that $v$ is *discrete* if it has value group isomorphic to $(\mathbb{Z}, \leq)$.

In many cases we actually have equality in (iii).

**Lemma 2.2.5.** *Let $K$ be a field with valuation $v : K \longrightarrow\!\!\!\!\!\rightarrow \Gamma \cup \{\infty\}$. If $x_1, \ldots, x_n \in K$ are elements of $K$ with pairwise distinct valuation, then*

$$v(x_1 + \ldots + x_n) = \min_{1 \leq i \leq n} v(x_i).$$

*Proof.* Consider the case $n = 2$. We can assume without loss of generality that $v(x_1) > v(x_2)$ and thus $v(x_1 + x_2) \geq v(x_2)$. If we had strict inequality $v(x_1 + x_2) > v(x_2)$, this would yield a contradiction:

$$v(x_2) = v((x_1 + x_2) - x_1) \geq \min\{v(x_1 + x_2),\, v(-x_1)\} > v(x_2).$$

Hence we have

$$v(x_1 + x_2) = \min\{v(x_1),\, v(x_2)\}.$$

The general case follows by induction. □

§ 2. *The p-adic valuation.* The most important example of a non-archimedean absolute value is the following.

**Definition 2.2.6.** Let $p$ be a prime number. Given $x \in \mathbb{Q}^\times$, written as $x = p^k \frac{a}{b}$ with $p \nmid a, b$, we define

$$|x|_p = p^{-k}.$$

The *p-adic valuation* $v_p$ on $\mathbb{Q}$ is given by

$$v(x) = k \in \mathbb{Z}.$$

Note that if we restrict ourselves to the positive integers $n \in \mathbb{Z}_{>0}$, then $v_p(n)$ is just the exponent of the prime $p$ in the prime factorisation of $n$.

It is a remarkable fact (see [19, Chap. II, (3.7)]) that this already describes all possible valuations on $\mathbb{Q}$.

**Theorem 2.2.7.** *Up to equivalence, the p-adic valuations $v_p$ are the only valuations on $\mathbb{Q}$.*

§ 3. *The t-adic valuation.* Consider the rational function field $k(t)$ over a field $k$ in one variable.

**Definition 2.2.8.** Let $k$ be any field. Given $x \in k(t)^\times$, written as

$$x = t^l \frac{f(t)}{g(t)},$$

where $f(t), g(t) \in k[t]$ have non-zero constant term, we define

$$v_t(x) = l \in \mathbb{Z}.$$

We call $v_t$ the *t-adic valuation* on $k(t)$.

§ 4. *Valuation ring, unit group, and residue field.* Essential to any valuation are the following algebraic objects associated to it.

**Definition/Remark 2.2.9.** Let $v : K \longrightarrow\!\!\!\!\!\rightarrow \Gamma \cup \{\infty\}$ be a valuation. The ring

$$\mathcal{O}_v = \{x \in K \mid v(x) \geq 0\}$$

is a local ring, called the *valuation ring*, with maximal ideal

$$\mathcal{M}_v = \{x \in K \mid v(x) > 0\}$$

and *unit group*

$$\mathcal{O}_v^\times = \mathcal{O}_v \setminus \mathcal{M}_v = \{x \in K \mid v(x) = 0\}.$$

The field

$$k_v = \mathcal{O}_v / \mathcal{M}_v$$

is called *residue field*. Note that the group homomorphism $v|_{K^\times}$ has kernel $\mathcal{O}_v^\times$, so the value group $\Gamma$ is isomorphic to $K^\times / \mathcal{O}_v^\times$. ⊣

The final remark indicates that from the valuation ring alone, one can recover the whole valuation. This will be illustrated by an explicit example in Remark 2.2.16.

**Example 2.2.10.** (1) Consider the $p$-adic valuation $v = v_p$ on $\mathbb{Q}$. Then

$$\begin{aligned}
\mathcal{O}_v &= \left\{ \tfrac{a}{b} \in \mathbb{Q} \;\middle|\; p \nmid b \right\} \\
\mathcal{M}_v &= \left\{ \tfrac{a}{b} \in \mathbb{Q} \;\middle|\; p \mid a,\, p \nmid b \right\} \\
\mathcal{O}_v^\times &= \left\{ \tfrac{a}{b} \in \mathbb{Q} \;\middle|\; p \nmid a,\, p \nmid b \right\} \\
k_v &= \mathcal{O}_v / p\mathcal{O}_v = \mathbb{F}_p.
\end{aligned}$$

(2) Given any field $k$, consider the $t$-adic valuation $v = v_t$ on $k(t)$. Then

$$\begin{aligned}
\mathcal{O}_v &= \left\{ \tfrac{f(t)}{g(t)} \in k(t) \;\middle|\; g(0) \neq 0 \right\} \\
\mathcal{M}_v &= \left\{ \tfrac{f(t)}{g(t)} \in k(t) \;\middle|\; f(0) = 0,\, g(0) \neq 0 \right\} \\
\mathcal{O}_v^\times &= \left\{ \tfrac{f(t)}{g(t)} \in k(t) \;\middle|\; f(0) \neq 0,\, g(0) \neq 0 \right\} \\
k_v &= \mathcal{O}_v / t\mathcal{O}_v = k.
\end{aligned}$$

⊣

§ 5. *Local fields.* A valued field $(K, |\cdot|)$ is a metric space with distance function

$$d(x, y) = |x - y|.$$

When we say that $(K, |\cdot|)$ is *complete*, we mean that the induced metric space is complete.

**Example 2.2.11.** The valued field $(\mathbb{Q}, |\cdot|_\infty)$ is not complete, but $(\mathbb{R}, |\cdot|_\infty)$ is. Also, the valued field $(\mathbb{Q}, |\cdot|_p)$ is not complete. For example,

$$a_n = \sum_{i=1}^{n} p^{i!}$$

defines a Cauchy sequence with respect to the $p$-adic metric. However, it cannot have a limit in $\mathbb{Q}$, because any $q \in \mathbb{Q}$ has periodic $p$-adic expansion. ⊣

Any valued field $(K, |\cdot|)$ can be extended to a complete valued field $(\widehat{K}, |\cdot|)$, called the *completion* of $K$, in a universal way (see [19, Chap. II, §4]). The absolute value on $\widehat{K}$ extends the absolute value on $K$, and $K$ is dense in $\widehat{K}$. The completion of $(K, |\cdot|)$ is unique up to unique value-preserving isomorphism fixing $K$. It is worth noting that when $|\cdot|$ is non-archimedean, the value group and residue field do not change after completion.

**Definition 2.2.12.** The field of *$p$-adic numbers* $\mathbb{Q}_p$ is the completion of $(\mathbb{Q}, |\cdot|_p)$. The field of *formal Laurent series over* $\mathbb{F}_q$, written $\mathbb{F}_q(\!(t)\!)$, is the completion of $\mathbb{F}_q(t)$ with respect to the $t$-adic valuation.

The valued fields $\mathbb{Q}_p$ and $\mathbb{F}_q(\!(t)\!)$ are basic examples of *local fields*. Often, it is useful to represent elements of $\mathbb{Q}_p$ and $\mathbb{F}_q(\!(t)\!)$ as infinite series. We can write

$$\begin{aligned}
\mathbb{Q}_p &= \left\{ \sum_{i=-n}^{\infty} a_i p^i \;\middle|\; a_i \in \{0, \ldots, p-1\},\ n \in \mathbb{Z} \right\} \\
\mathbb{F}_q(\!(t)\!) &= \left\{ \sum_{i=-n}^{\infty} a_i t^i \;\middle|\; a_i \in \mathbb{F}_q,\ n \in \mathbb{Z} \right\},
\end{aligned}$$

and both the $p$-adic and $t$-adic valuation are given by $\min\{i \mid a_i \neq 0\}$.

**Definition 2.2.13.** A *local field* is either a complete archimedean valued field, or a complete non-archimedean valued field with discrete valuation and finite residue field.

By Ostrowski's theorem [19, Chap. II, (4.2)], any complete archimedean valued field is isomorphic to $\mathbb{R}$ or $\mathbb{C}$, and its absolute value is equivalent to $|\cdot|_\infty$. Moreover, the absolute value on $\mathbb{Q}_p$ or $\mathbb{F}_p(\!(t)\!)$ extends uniquely to any finite extension of $\mathbb{Q}_p$ or $\mathbb{F}_p(\!(t)\!)$, respectively. This, in fact, already characterises all non-archimedean local fields.

**Theorem 2.2.14.** *Any non-archimedean local fields of characteristic* 0 *is a finite extension of* $\mathbb{Q}_p$ *for some prime* $p$*. Any non-archimedean local field of characteristic* $p$ *is isomorphic to* $\mathbb{F}_q(\!(t)\!)$ *for some finite field* $\mathbb{F}_q$*.*

*Proof.* See [19, Chap. II, (5.2)]. □

Finally, let us note that local fields arise as completions with respect to an absolute value on *global fields*. These are finite extensions of $\mathbb{Q}$ (algebraic number fields), or finite extensions of $\mathbb{F}_q(t)$ (global function fields). If $K$ is a global field with absolute value $|\cdot|$, then the completion of $(K, |\cdot|)$ will be a local field.

§ 6. *The natural valuation of an ordered field.* We can define a valuation that is quite different in nature in comparison to discrete valuations on local fields.

Let $(K, \leq)$ be an *ordered field*, that is, a field $K$ together with a total order $\leq$ satisfying the compatibility conditions

(i) $x \leq y \Longrightarrow x + z \leq y + z$

(ii) $0 < x, y \Longrightarrow 0 < x \cdot y$,

for all $x, y, z \in K$. Note that $K$ is necessarily of characteristic 0. To any ordered field $(K, \leq)$ we can assign a valuation in a natural way, as we now describe.

For $x \in K$, we write[4]

$$|x| = \max\{x, -x\}.$$

Given $x, y \in K$, we say that $x$ and $y$ are in the same *archimedean class*, in symbols $x \sim y$, if there is $N \in \mathbb{Z}_{>0}$ such that

$$\frac{1}{N}|x| \leq |y| \leq N|x|.$$

Clearly, $\sim$ defines an equivalence relation. Write $\infty = [0]$ for the equivalence class of 0, and $\Gamma \cup \{\infty\}$ for the whole set of equivalence classes $[x]$, $x \in K$. We can turn $\Gamma$ into a totally ordered abelian group by declaring

$$[x] + [y] \coloneqq [x + y]$$
$$[x] \leq [y] :\Longleftrightarrow \exists x' \in [x],\, y' \in [y]\ |x'| \geq |y'|$$

for all $[x], [y] \in \Gamma$. It is not difficult to verify that this is indeed a well-defined totally ordered abelian group with neutral element $[1]$ (the trivial archimedean class).

By construction, the assignment $x \longmapsto [x]$ satisfies axioms (i) and (ii) of a valuation. Moreover, we have

$$|x + y| \leq |2x| \quad \text{or} \quad |x + y| \leq |2y|,$$

[4]Unfortunately, the notation here is overloaded, as we already used $|\cdot|$ to denote absolute values in Definition 2.2.1. Moving forward, we will not use absolute values anymore, so there should be no ambiguity.

which implies

$$[x+y] \geq [2x] = [x] \quad \text{or} \quad [x+y] \geq [2y] = [y],$$

so $x \longmapsto [x]$ does in fact define a valuation.

**Definition 2.2.15.** Let $(K, \leq)$ be an ordered field. We call

$$v_{\text{nat}} : K \longrightarrow\!\!\!\!\!\rightarrow \Gamma \cup \{\infty\},\ x \longmapsto [x],$$

as defined above, the *natural valuation* of $(K, \leq)$.

**Remark 2.2.16.** We can give an alternative description of $v_{\text{nat}}$ by starting with its valuation ring (this can be done, in general, with any valuation). Let

$$\text{Fin}(K) = \{x \in K \mid \exists N \in \mathbb{Z}_{>0}\ |x| < N\}$$

be the ring of *finitely bounded elements* of $K$. This is a local ring with unique maximal ideal

$$\text{Inf}(K) = \left\{x \in K \mid \forall N \in \mathbb{Z}_{>0}\ |x| < \frac{1}{N}\right\}$$

of *infinitesimal elements* of $K$. The unit group of $\text{Fin}(K)$ is given by

$$\text{Fin}(K)^\times = \text{Fin}(K) \setminus \text{Inf}(K) = \left\{x \in K \mid \exists N \in \mathbb{Z}_{>0}\ \frac{1}{N} \leq |x| \leq N\right\} = [1].$$

Hence $K^\times / \text{Fin}(K)^\times$ is precisely the group of archimedean classes $\Gamma$ (we divide out the trivial archimedean class). The canonical projection

$$v : K^\times \longrightarrow\!\!\!\!\!\rightarrow K^\times / \text{Fin}(K)^\times = \Gamma,$$

together with the assignment $v(0) = \infty$ and ordering

$$v(x) \leq v(y) :\Longleftrightarrow \frac{y}{x} \in \text{Fin}(K)$$

of $K^\times / \text{Fin}(K)^\times$, give another description for $v_{\text{nat}}$. ⊣

**Example 2.2.17.** (1) Consider the ordered field $(\mathbb{R}, \leq)$. Its only archimedean classes are $\infty = [0]$ and $0 = [1]$, so $v_{\text{nat}}$ is the trivial valuation.

(2) Consider the field of formal Laurent series $\mathbb{R}(\!(t)\!)$ over $\mathbb{R}$ in one variable. We define a lexicographical order $\leq$ on $\mathbb{R}(\!(t)\!)$ by declaring

$$\sum_i a_i t^i \leq \sum_i b_i t^i :\Longleftrightarrow a_k \leq b_k, \text{ where } k = \min\{i \in \mathbb{Z} \mid a_i \neq b_i\}.$$

We then have

$$\text{Fin}(\mathbb{R}(\!(t)\!)) = \left\{\textstyle\sum_i a_i t^i \mid \forall i < 0\ a_i = 0\right\} = \mathbb{R}[\![t]\!]$$
$$\text{Inf}(\mathbb{R}(\!(t)\!)) = \left\{\textstyle\sum_i a_i t^i \mid \forall i \leq 0\ a_i = 0\right\} = t\mathbb{R}[\![t]\!].$$

Thus $v_{\text{nat}}$ is precisely the $t$-adic valuation $v_t$ with residue field $\mathbb{R}$ and value group $\mathbb{Z}$.

(3) Consider the field of formal Laurent series $\mathbb{R}(\!(t, T)\!)$ over $\mathbb{R}$ in two variables. We would like to define a total order on $\mathbb{R}(\!(t, T)\!)$ in such a way that $t$ and $T$ are infinitesimals, and $t$ is infinitesimally small compared to $T$. This is realised by

$$\sum_{i,j} a_{ij} t^i T^j \leq \sum_{i,j} b_{ij} t^i T^j :\Longleftrightarrow a_{kl} \leq b_{kl}, \text{ where } \begin{cases} k = \min\{i \in \mathbb{Z} \mid \exists j\ a_{ij} \neq b_{ij}\} \\ l = \min\{j \in \mathbb{Z} \mid a_{kj} \neq b_{kj}\}. \end{cases}$$

This valuation has residue field $\mathbb{R}$ and value group $\mathbb{Z} \times \mathbb{Z}$. ⊣

All three examples are actually special cases of *Hahn series fields*. However, we will not need this general notion in our study of decidability of local fields.

2.3. **Real closed fields.** The theory $(\mathbb{R}, 0, 1, +, -, \cdot)$ does not have quantifier elimination: the subset $\mathbb{R}_{\geq 0} \subseteq \mathbb{R}$ is definable, but not by a quantifier-free formula. This can be remedied by expanding the language by a relation symbol $\leq$ for the order on $\mathbb{R}$. To understand the first-order theory of $(\mathbb{R}, 0, 1, +, -, \cdot, \leq)$, one has to study the Artin-Schreier theory of formally real fields. Its starting point is a simple observation: $-1$ is not the sum of squares in $\mathbb{R}$.

In general, if we consider an ordered field $(K, \leq)$, then again $-1$ will not be the sum of squares. This leads to the following definition and characterisation (see [16, Cor. B.7]):

**Definition 2.3.1.** Let $K$ be a field. We call $K$ *formally real* if $-1$ is not the sum of squares in $K$.

**Proposition 2.3.2.** *Let $K$ be a field. Then $K$ is formally real if and only if it is orderable, i.e., there is an order $\leq$ on $K$ making it into an ordered field.*

In the context of ordered fields, the notion of a real closed field takes the place of algebraically closed fields.

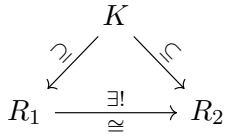
**Definition 2.3.3.** We say that a formally real field $K$ is *real closed* if there is no proper algebraic formally real extension of $K$.

Any real closed field $R$ has a unique ordering: these fields satisfy the property that for any $a \in R$, $a$ or $-a$ is a square in $R$, so that

$$x \leq y :\Longleftrightarrow \exists z \in R \; y = x + z^2$$

defines the unique ordering on $R$. In other words, the ordering on $R$ is already inherent to the algebra of the field. The *real closure* of an ordered field $(K, \leq)$ is a real closed field that is an algebraic extension of $K$ and whose unique ordering extends $\leq$ on $K$. In analogy to the existence and uniqueness of algebraic closures, we have the following theorem [16, Thm. B.14]:

**Theorem 2.3.4.** *Let $(K, \leq)$ be an ordered field. Then $(K, \leq)$ can be extended to a real closure $K^{\mathrm{rc}}$. Moreover, the real closure is unique up to unique isomorphism: if $R_1$ and $R_2$ are real closures of $K$, then there exists a unique isomorphism between $R_1$ and $R_2$ over $K$.*




Note however, that the real closure is not unique if we do not fix an ordering on $K$ beforehand. We can have non-isomorphic real closures if we start with different orderings on $K$.

Tarski showed that real closed fields are elementarily equivalent to the real field $\mathbb{R}$. To see that this actually gives us an axiomatisation of the first-order theory of $\mathbb{R}$, we will need an alternative description for real closed fields.

**Theorem 2.3.5.** *Let $(K, \leq)$ be an ordered field. Then the following are equivalent:*

*(i) $K$ is a real closed field.*

*(ii) The field extension $K(i)$ is algebraically closed, where $i^2 = -1$.*

*(iii) Any non-negative $x \in K$ has a square root and any polynomial $f(X) \in K[X]$ of odd degree has a solution in $K$.*

For proof, see [16, Cor. B.9, Thm B.12]. The last one of the three equivalent statements can be expressed by first-order sentences. Thus we define:

**Definition 2.3.6.** Let $\mathcal{L}_{\text{rcf}} = \{0, 1, +, -, \cdot, \leq\}$. The *$\mathcal{L}_{\text{rcf}}$-theory of real closed fields* $T_{\text{rcf}}$ consists of

(i) axioms for ordered fields;

(ii) $\forall x\,(x \geq 0 \to \exists y\; x = y^2)$;

(iii) $\forall a_0 \forall a_1 \ldots \forall a_{n-1} \exists x\,(x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0 = 0)$ for all odd $n$.

Thus we can formulate the main theorem of this section.

**Theorem 2.3.7.** *The theory $T_{\text{rcf}}$ is complete and has quantifier elimination. Consequently, $(\mathbb{R}, 0, 1, +, -, \cdot, \leq)$ is decidable.*

Clearly, $\mathbb{R} \models T_{\text{rcf}}$. For the proof of quantifier elimination, see [16, Thm. 3.3.15]. Quantifier elimination implies completeness, because $\mathbb{Q}^{\text{rc}}$ embeds into any real closed field (we will explain this type of argument in greater detail in the proof of Corollary 3.1.7). Decidability follows from Theorem 2.1.3, since $T_{\text{rcf}}$ is recursive.

We end this section with a lemma about valuations on real closed fields that will be of use in the next chapter.

**Lemma 2.3.8.** *Let $L/K$ be a field extension and $v : L \twoheadrightarrow \Gamma_L \cup \{\infty\}$ a valuation on $L$, that restricts to $v|_K : K \twoheadrightarrow \Gamma_K \cup \{\infty\}$ with value group $\Gamma_K \subseteq \Gamma_L$.*

*(i) If $L$ is real closed, then $\Gamma_L$ is divisible.*

*(ii) If $L$ is the the real closure of $K$ (with respect to some ordering), then $\Gamma_L$ is the divisible hull $\widetilde{\Gamma}_K$ of $\Gamma_K$.*[5]

*(iii) If $\widetilde{\Gamma}_K \subsetneq \Gamma_L$ and $x \in L^\times$ is such that $v(x) \notin \widetilde{\Gamma}_K$, then $x$ is transcendental over $K$.*

*Proof.* (i) Let $\gamma \in \Gamma_L$ be any element. Choose $x \in L$ with $v(x) = v(-x) = \gamma$. Since $L$ is real closed, we can find $y \in L$ such that $y^n = x$ or $y^n = -x$ for any $n \geq 1$. But then $n \cdot v(y) = \gamma$, so $\Gamma_L$ is divisible.

[5] The divisible hull of a torsion-free group $G$ is the smallest divisible group that contains $G$. It can be constructed by formally inverting all $n \in \mathbb{Z}_{>0}$.

(ii) We already know that $\Gamma_L$ is divisible. Thus we are left to show that for any $v(x) \in \Gamma_L$, there is $n \geq 1$ such that $n \cdot v(x) \in \Gamma_K$. Since $L/K$ is algebraic, we can find $a_0, \ldots, a_k \in K$ such that

$$a_k x^k + \ldots + a_1 x + a_0 = 0.$$

It cannot happen that all non-zero $a_i x^i$ have pairwise distinct valuation, because otherwise the left-hand side would have valuation $\neq \infty$ by Lemma 2.2.5. This mean that we can find $0 \leq i < j \leq k$ with $v(a_j x^j) = v(a_i x^i)$, implying

$$(j - i) \cdot v(x) = v(a_i) - v(a_j) \in \Gamma_K.$$

(iii) Follows from (ii). □

## 3. Decidable expansion of the real field

3.1. **The real field with a cyclic subgroup.** In [24], van den Dries shows that the theory of $(\mathbb{R}, 0, 1, +, -, \cdot, \leq, 2^{\mathbb{Z}})$, the real ordered field with a predicate for powers of two, is decidable. He does so by giving a complete and recursive axiomatisation of this structure. In turn, completeness follows from quantifier elimination in an expanded language and the observation that $\mathbb{Q}$ embeds into any structure satisfying the axiomatisation. At the end of the paper [24, p. 194], van den Dries remarks that his results, in particular quantifier elimination, generalise to the case when $2^{\mathbb{Z}}$ is replaced by any discrete cyclic subgroup $\alpha^{\mathbb{Z}}$, $\alpha \in \mathbb{R}_{>1}$. In this section we present his proof, while making the necessary modifications for general $\alpha \in \mathbb{R}_{>1}$ more explicit.

We start by fixing our language. Let $\mathcal{L}_{\mathrm{rcf}} \cup \{\underline{\alpha}, \underline{A}\}$ be the language of real closed fields

$$\mathcal{L}_{\mathrm{rcf}} = \{0, 1, +, -, \cdot, \leq\},$$

together with a constant symbol $\underline{\alpha}$ and unary relation symbol $\underline{A}$. For readability, we will omit 0, 1, +, −, and · from notation of structures in this language.

We propose the following complete axiomatisation for $\mathrm{Th}(\mathbb{R}, \leq, \alpha, \alpha^{\mathbb{Z}})$.

**Definition 3.1.1.** Let $T_{\mathrm{rcf}}(\alpha^{\mathbb{Z}})$ be the $\mathcal{L}_{\mathrm{rcf}} \cup \{\underline{\alpha}, \underline{A}\}$-theory consisting of the following sentences:

(R1) the axioms for ordered rings and $0 \neq 1$;

(R2) $\forall x \exists y\, (x \neq 0 \to x \cdot y = 1)$;

(R3) $\forall x \exists y\, (x > 0 \to x = y^2)$;

(R4) $\forall a_0 \forall a_1 \ldots \forall a_{n-1} \exists x\, (x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0 = 0)$ for all odd $n$;

(S1) $1 \in \underline{A}$, $\forall x \forall y\, (x \in \underline{A} \wedge y \in \underline{A} \to x \cdot y \in \underline{A})$, and $\forall x \forall y\, (x \cdot y = 1 \wedge x \in \underline{A} \to y \in \underline{A})$;

(S2) $\forall x\, (x \in \underline{A} \to x > 0)$;

(A1) $\underline{\alpha} \leq N$ and $N + 1 \leq N\underline{\alpha}$ for some fixed positive integer integer $N$;[6]

(A2) $\underline{\alpha} \in \underline{A}$ and $\forall x\, (1 < x < \underline{\alpha} \to x \notin \underline{A})$;

(A3) $\forall x \exists y \in \underline{A}\, (x > 0 \to y \leq x < \underline{\alpha} \cdot y)$.

If we are given a concrete $\alpha \in \mathbb{R}_{>1}$, then we obtain the $\mathcal{L}_{\mathrm{rcf}} \cup \{\underline{\alpha}, \underline{A}\}$-theory $T_{\mathrm{rcf}}(\alpha, \alpha^{\mathbb{Z}})$ by adding the sentences

(D) $m < n\underline{\alpha}$ for all $\frac{m}{n} \in \{q \in \mathbb{Q} \mid q < \alpha\}$, where $n > 0$, and
$m \geq n\underline{\alpha}$ for all $\frac{m}{n} \notin \{q \in \mathbb{Q} \mid q < \alpha\}$, where $n > 0$,

to the theory $T_{\mathrm{rcf}}(\alpha^{\mathbb{Z}})$, and if $\alpha$ is algebraic with minimal polynomial $p(X) \in \mathbb{Q}[X]$, a sentence for $p(\underline{\alpha}) = 0$.

[6] This axiom says that the interpretation of $\underline{\alpha}$ is bounded and bigger than 1 by at least $1/N$. Because of the Compactness Theorem, we have to specify this bound extrinsically. In particular, the theory $T_{\mathrm{rcf}}(\alpha^{\mathbb{Z}})$ thus defined depends on the constant $N$.

If $\mathcal{K} = (K, \leq, \alpha, A)$ is a model of $T_{\mathrm{rcf}}(\alpha, \alpha^{\mathbb{Z}})$, then (R1)–(R4) say that $K$ is a real closed field, (S1)–(S2) say that $A$ is a multiplicative subgroup of $K_{>0}$, (A2)–(A3) say that we can write $K_{>0}$ as the disjoint union

$$K_{>0} = \bigsqcup_{x \in A} [x, \alpha x),$$

and finally, (D) says that the Dedekind cut of $\alpha$ in $\mathbb{R}$ and $K$ coincides. Note that (D) implies (A1). Thus we do not need to specify $N \in \mathbb{Z}_{>0}$ for the theory $T_{\mathrm{rcf}}(\alpha, \alpha^{\mathbb{Z}})$.

We claim that these axioms suffice for an axiomatisation.

**Theorem 3.1.2.** *Let $\alpha \in \mathbb{R}_{>1}$ be a fixed constant. Then $T_{\mathrm{rcf}}(\alpha, \alpha^{\mathbb{Z}})$ is a complete axiomatisation of $(\mathbb{R}, \leq, \alpha, \alpha^{\mathbb{Z}})$. In particular, $(\mathbb{R}, \leq, \alpha, \alpha^{\mathbb{Z}})$ is decidable if and only if $\alpha$ is recursive.*

Recall that $\alpha \in \mathbb{R}_{>1}$ is recursive if there is an algorithm that can compute its decimal representation to any given degree of accuracy. This is equivalent to saying that the set of pairs $(m, n) \in \mathbb{N}^2$ satisfying $\frac{m}{n} < \alpha$ is recursive.

**Remark 3.1.3.** We see immediately that the second part of this theorem is a consequence of Theorem 2.1.3: the set of axioms (R1)–(R4), (S1)–(S2), (A1)–(A3) is recursive. If the same is true for (D), then $\mathrm{Th}(\mathbb{R}, \leq, \alpha, \alpha^{\mathbb{Z}})$ will be decidable. Conversely, this theory contains all sentences that express $q < \alpha$ for $q \in \mathbb{Q}$. This means that for "bad" choices of $\alpha$ (meaning that $\alpha$ is not recursive), $\mathrm{Th}(\mathbb{R}, \leq, \alpha, \alpha^{\mathbb{Z}})$ has no chance of being decidable. This explains the somewhat artificial condition on $\alpha$ and the subtlety which arises when passing from $(\mathbb{R}, \leq, 2^{\mathbb{Z}})$ to $(\mathbb{R}, \leq, \alpha, \alpha^{\mathbb{Z}})$. ⊣

As mentioned before, Theorem 3.1.2 will follow from quantifier elimination in an expanded language—which we now define—and the existence of a structure that embeds into any model of the extended theory.

**Definition 3.1.4.** For each positive integer $n$, let $\underline{P}_n$ be an unary relation symbol. Let $\underline{f}$ be an unary function symbol. We write $\mathcal{L}^* = \mathcal{L}_{\mathrm{rcf}} \cup \{\underline{\alpha}, \underline{A}, \{\underline{P}_n\}_{n \geq 1}, \underline{f}\}$ for the new expanded language. We obtain the $\mathcal{L}^*$-theory $T^* = T_{\mathrm{rcf}}(\alpha^{\mathbb{Z}}, \{P_n\}_{n \geq 1}, f)$ by adding the sentences

(P) $\forall x \, (x \in \underline{P}_n \leftrightarrow \exists y (y \in \underline{A} \wedge x = y^n))$;

(F) $\forall x \, (x \leq 0 \rightarrow \underline{f}(x) = 0)$, and

$\forall x \, (x > 0 \rightarrow (\underline{f}(x) \in \underline{A} \wedge \underline{f}(x) \leq x < \underline{\alpha} \cdot \underline{f}(x)))$

to the theory $T_{\mathrm{rcf}}(\alpha^{\mathbb{Z}})$.

In words: for a model $\mathcal{K} = (K, \leq, \alpha, A, \{P_n\}_{n \geq 1}, f)$ of $T^*$, we have that $P_n \subseteq A$ are the $n^{\mathrm{th}}$ powers in $A$, and $f|_{K_{>0}} : K_{>0} \longrightarrow A$ is the "floor function" that rounds positive $x \in K$ to the nearest element in $A$ below $x$.

**Example 3.1.5.** Our standard model $(\mathbb{R}, \leq, \alpha, \alpha^{\mathbb{Z}})$ of $T_{\mathrm{rcf}}(\alpha^{\mathbb{Z}})$ expands to a model of $T^*$ by setting $P_n = \alpha^{n\mathbb{Z}}$ and

$$f(x) = \alpha^{\lfloor \log_\alpha(x) \rfloor}$$

for $x \in \mathbb{R}_{>0}$. We denote this model by $\mathcal{R}$. ⊣

**Lemma 3.1.6.** *Let $\alpha \in \mathbb{R}_{>1}$. Let $(K, \leq)$ be an ordered field.*

*(i) Let $\beta \in K$ be an element of $K$ with the same Dedekind cut as $\alpha$, i.e.,*

$$\{q \in \mathbb{Q} \mid q < \alpha\} = \{q \in \mathbb{Q} \mid q < \beta\}.$$

*Furthermore, if $\alpha$ is algebraic with minimal polynomial $p(X) \in \mathbb{Q}[X]$, assume that $p(\beta) = 0$. Then the homomorphism*

$$\begin{array}{ccc} (\mathbb{Q}(\alpha), \leq) & \longrightarrow & (\mathbb{Q}(\beta), \leq) \\ \cap & & \cap \\ (\mathbb{R}, \leq) & & (K, \leq) \end{array}$$

*that sends $\alpha$ to $\beta$, defines an isomorphism of ordered fields.*

*(ii) $(\mathbb{Q}(\alpha), \leq)$ embeds into any model of $T_{\mathrm{rcf}}(\alpha, \alpha^{\mathbb{Z}})$. This embedding expands to an $\mathcal{L}^*$-embedding.*

*Proof.* (i) Consider any polynomial $f(X) = a_d X^d + \ldots + a_1 X + a_0 \in \mathbb{Q}[X]$. Let us show that

$$f(\alpha) > 0 \Longrightarrow f(\beta) > 0$$

in $(\mathbb{R}, \leq)$ resp. $(K, \leq)$. Choose $q_0, q_1, \ldots, q_d \in \mathbb{Q}_{>0}$ subject to the conditions

$$\begin{cases} q_i < \alpha & \text{if } a_i > 0 \\ q_i = 0 & \text{if } a_i = 0 \\ q_i > \alpha & \text{if } a_i < 0. \end{cases}$$

Set $Q = a_d q_d^d + \ldots + a_1 q_1 + a_0 \in \mathbb{Q}$. Then $f(\alpha) > Q$ and $f(\beta) > Q$. If $f(\alpha) > 0$, we can choose the $q_i$ sufficiently close to $\alpha$ (for all $a_i \neq 0$) so that $f(\alpha) > Q > 0$. But then $f(\beta) > Q > 0$. The same argument shows that

$$f(\alpha) < 0 \Longrightarrow f(\beta) < 0.$$

If $\alpha$ is transcendental, then $\beta$ must be transcendental as well. Hence $\mathbb{Q}(\alpha) \longrightarrow \mathbb{Q}(\beta)$, $\alpha \longmapsto \beta$, defines a field isomorphism that preserves order.

(ii) Let $\mathcal{A} = (\mathbb{Q}(\alpha), \leq, \alpha, \alpha^{\mathbb{Z}}, \{\alpha^{n\mathbb{Z}}\}_{n \geq 1}, x \mapsto \alpha^{\lfloor \log_\alpha(x) \rfloor})$ be the restriction of the standard model $\mathcal{R} \models T^*$ to the domain $\mathbb{Q}(\alpha)$. Let $\mathcal{K} = (K, \leq, \beta, A, \{P_n\}_{n \geq 1}, f)$ be the $\mathcal{L}^*$-expansion of a model of $T_{\mathrm{rcf}}(\alpha, \alpha^{\mathbb{Z}})$. By part (i), the inclusion

$$\iota : \mathbb{Q}(\alpha) \longrightarrow K, \ \alpha \longmapsto \beta,$$

is an embedding in the language $\mathcal{L}_{\mathrm{rcf}} \cup \{\underline{\alpha}\}$. We will now show that it is an $\mathcal{L}^*$-embedding as well. Note that for any positive $x \in \mathbb{Q}(\alpha)$,

$$\alpha^n \leq x < \alpha^{n+1} \Longrightarrow \beta^n \leq \iota(x) < \beta^{n+1}, \tag{3.1.1}$$

thus $f(\iota(x)) = \beta^n = \iota(\alpha^n) = \iota(f(x))$, so $\iota$ is compatible with $f$. Furthermore, $f(y) = y$ holds for any $y \in A$. Together with (3.1.1), this implies that for any $\iota(x) \in \iota(\mathbb{Q}(\alpha)) \cap A$, it follows that $\iota(x) = f(\iota(x)) \in \beta^{\mathbb{Z}} = \iota(\alpha^{\mathbb{Z}})$. Thus $\iota(\alpha^{\mathbb{Z}}) = \iota(\mathbb{Q}(\alpha)) \cap A$, and by the same argument, $\iota(\alpha^{n\mathbb{Z}}) = \iota(\mathbb{Q}(\alpha)) \cap P_n$ for all $n \geq 1$. □

**Corollary 3.1.7.** *If $T^*$ has quantifier elimination, then $T_{\mathrm{rcf}}(\alpha, \alpha^{\mathbb{Z}})$ is complete.*

*Proof.* This is a well-known argument (cf. [16, Prop. 3.1.14]). Let $\mathcal{K}_1$ and $\mathcal{K}_2$ be models of $T_{\mathrm{rcf}}(\alpha, \alpha^{\mathbb{Z}})$. Both expand to models of $T^*$. Let $\mathcal{A}$ be the $\mathcal{L}^*$-structure from the previous lemma that embeds into any model of $T^*$. Any $\mathcal{L}_{\mathrm{rcf}} \cup \{\underline{\alpha}, \underline{A}\}$-sentence $\varphi$ is equivalent to a quantifier-free $\mathcal{L}^*$-sentence $\psi$ under $T^*$. Thus we have

$$\mathcal{K}_1 \models \varphi \iff \mathcal{K}_1 \models \psi \iff \mathcal{A} \models \psi \iff \mathcal{K}_2 \models \psi \iff \mathcal{K}_2 \models \varphi,$$

which proves that $\mathcal{K}_1 \equiv \mathcal{K}_2$. □

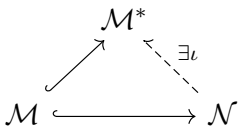
In other words: we are left to prove quantifier elimination for $T^*$, from which the main result (Theorem 3.1.2) follows by the above discussion. If we compare van den Dries' proof [24] with our exposition, we see that the only substantial difference is that for general $\alpha \in \mathbb{R}_{>1}$, we additionally need Lemma 3.1.6. For $\alpha = 2$ (or $\alpha \in \mathbb{Q}_{>1}$ for that matter) it is obsolete, because then $\mathbb{Q}$ is already an $\mathcal{L}^*$-structure that embeds into any model of $T^*$.

3.2. **Quantifier elimination in $T^*$.** We will use the following embedding test for quantifier elimination. It differs only marginally from the one used by van den Dries [24].

**Proposition 3.2.1** (Embedding test)**.** *Let $\mathcal{L}$ be a first-order language with at least one constant symbol. Let $\Sigma$ be an $\mathcal{L}$-theory. Then the following three statements are equivalent:*

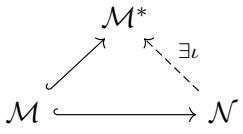
*(i)* *$\Sigma$ has quantifier elimination.*

*(ii)* *Given any $\mathcal{L}$-substructure $\mathcal{M} \subsetneq \mathcal{N} \models \Sigma$ and $|N|^+$-saturated model $\mathcal{M} \subseteq \mathcal{M}^* \models \Sigma$, the inclusion $\mathcal{M} \hookrightarrow \mathcal{M}^*$ can be extended to a partial $\mathcal{L}$-embedding $\iota : \mathcal{N} \longrightarrow \mathcal{M}^*$ with strictly bigger domain. Written diagrammatically:*




$\mathcal{N}, \mathcal{M}^* \models \Sigma,\ M \subsetneq \mathrm{dom}(\iota)$

*(iii)* *Given any $\mathcal{L}$-substructure $\mathcal{M} \subsetneq \mathcal{N} \models \Sigma$ and $|N|^+$-saturated model $\mathcal{M} \subseteq \mathcal{M}^* \models \Sigma$, the inclusion $\mathcal{M} \hookrightarrow \mathcal{M}^*$ can be extended to an $\mathcal{L}$-embedding $\iota : \mathcal{N} \hookrightarrow \mathcal{M}^*$. Written diagrammatically:*




$\mathcal{N}, \mathcal{M}^* \models \Sigma$

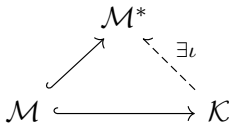
*Proof.* The proof of the equivalence of (i) and (iii) can be found in Marker's book (see [16, Prop. 4.3.28]). Clearly, (iii) implies (ii).

(ii) $\Longrightarrow$ (iii). Define a sequence of partial embeddings $\iota_\alpha : \mathcal{N} \longrightarrow \mathcal{M}^*$ indexed by ordinals $\alpha$. Let $\iota_0$ be the embedding $\mathcal{M} \hookrightarrow \mathcal{M}^*$. If we have defined $\iota_\alpha$ and $\mathrm{dom}(\iota_\alpha) \neq N$, let $\iota_{\alpha+1}$ be an extension of $\iota_\alpha$ obtained by an application of (ii). At limit stages $\lambda$, we let $\iota_\lambda$ be the union of all $\iota_\alpha$ constructed for $\alpha < \lambda$. This process terminates at some ordinal $\beta$ when we have $\mathrm{dom}(\iota_\beta) = N$, which will be the full embedding of $\mathcal{N}$ into $\mathcal{M}^*$. □

We are now going to apply this embedding test to the theory $T^* = T_{\mathrm{rcf}}(\alpha^{\mathbb{Z}}, \{P_n\}_{n\geq 1}, f)$. For this purpose, we fix $\mathcal{L}^*$-structures

$$\begin{aligned}\mathcal{M} &= (M, \leq, \alpha, A, \{P_n\}_{n\geq 1}, f|_M)\\ \mathcal{K} &= (K, \leq, \alpha, B, \{Q_n\}_{n\geq 1}, f)\\ \mathcal{M}^* &= (M^*, \leq, \alpha, A^*, \{P_n^*\}_{n\geq 1}, f^*)\end{aligned}$$

satisfying $\mathcal{M} \subsetneq \mathcal{K} \models T^*$, $\mathcal{M} \subseteq \mathcal{M}^* \models T^*$, and $\mathcal{M}^*$ is $|K|^+$-saturated. We need to show that we can extend the inclusion $\mathcal{M} \hookrightarrow \mathcal{M}^*$ to a partial embedding $\iota$ with $M \subsetneq \mathrm{dom}(\iota)$.




Before we can go further, we need to establish a few properties of models of $T^*$. This will give us some structural information that we can use to construct $\iota$.

**Remark 3.2.2.** $\mathcal{M}$ must not be a model of $T^*$, as it is merely a substructure of $\mathcal{K} \models T^*$. However, $\mathcal{M}$ will satisfy any universal sentence that is a consequence of $T^*$, including:

(1) $(M, \leq)$ satisfies axiom (R1) and $\forall x \forall y (x \neq 0 \wedge y \neq 0 \to xy \neq 0)$, so $(M, \leq)$ is an ordered integral domain.

(2) $\mathcal{M}$ still satisfies (S1)–(S2), so $A$ is a multiplicative subgroup of $M_{>0}$.

(3) $\mathcal{M}$ satisfies (F), and thus (A1)–(A3) as well.

Moreover, considering the natural valuation $v = v_{\mathrm{nat}}$ associated to the real closed field $(K, \leq)$, we know from Lemma 2.3.8 that its value group $\Gamma_K$ is divisible. ⊣

**Lemma 3.2.3.** *Let $v$ be the natural valuation associated to $(K, \leq)$ and $\Gamma_K$ its value group. The restriction $v|_B : B \longrightarrow \Gamma_K$ is surjective and has kernel $\alpha^{\mathbb{Z}}$, i.e.,*

$$B/\alpha^{\mathbb{Z}} \cong \Gamma_K.$$

*The same holds true for any other model of $T^*$.*

*Proof.* Consider any $\gamma \in \Gamma_K$. We can find $x > 0$ so that $v(x) = \gamma$. By (A1) and (F), we know that $x$ and $f(x)$ lie in the same archimedean class. Thus $v(f(x)) = \gamma$, where $f(x) \in B$.
Every element of $\alpha^{\mathbb{Z}}$ lies in the trivial archimedean class. If $v(x) = 0$ for some $x \in B$, then we can find $n \in \mathbb{Z}$ with $\alpha^n \leq x < \alpha^{n+1}$ by virtue of (A1). But then $x = f(x) = \alpha^n \in \alpha^{\mathbb{Z}}$, which proves that $\alpha^{\mathbb{Z}}$ is the kernel of $v|_B$. The same reasoning applies to any other model of $T^*$. □

**Lemma 3.2.4.** *The structure $(B, 1, \alpha, \cdot, \div, <, \{Q_n\}_{n\geq 1})$ is a model of Presburger arithmetic (as defined in Example 2.1.4). The same holds true for any other model of $T^*$.*

*Proof.* Note that because we are working with $\alpha^{\mathbb{Z}}$, we use multiplicative instead of additive notation. Properties (S1)–(S2), (A1)–(A2), and (P) imply properties (i)–(iv) of Presburger arithmetic. Since $\Gamma_K$ is divisible, we have

$$Q_n \alpha^{\mathbb{Z}}/\alpha^{\mathbb{Z}} \cong n\Gamma_K = \Gamma_K.$$

By several applications of the isomorphism theorems for groups, we get

$$(B/Q_n)/(Q_n\alpha^{\mathbb{Z}}/Q_n) \cong B/Q_n\alpha^{\mathbb{Z}} = (B/\alpha^{\mathbb{Z}})/(Q_n\alpha^{\mathbb{Z}}/\alpha^{\mathbb{Z}}) \cong \Gamma_K/\Gamma_K \cong \{0\}.$$

Combined with

$$Q_n\alpha^{\mathbb{Z}}/Q_n \cong \alpha^{\mathbb{Z}}/\alpha^{n\mathbb{Z}} \cong \mathbb{Z}/n\mathbb{Z},$$

this yields $B/Q_n \cong \mathbb{Z}/n\mathbb{Z}$, which implies (v), the last axiom of Presburger arithmetic. □

We are now ready for the construction of the extension $\iota$. We consider four cases.

*Case 1.* If $M$ is not a field, extend $\mathcal{M} \hookrightarrow \mathcal{M}^*$ to the field of fractions $F = \mathrm{Frac}(M) \subseteq K$.

*Case 2.* If $M$ is a field that is not real closed, extend $\mathcal{M} \hookrightarrow \mathcal{M}^*$ to the real closure $M^{\mathrm{rc}} \subseteq K$.

*Case 3.* If $M$ is a real closed field and $A = B$, we extend $\mathcal{M} \hookrightarrow \mathcal{M}^*$ to all of $K$.

*Case 4.* If $M$ is a real closed field and $A \neq B$, we extend $\mathcal{M} \hookrightarrow \mathcal{M}^*$ to a simple field extension $M(b) \subseteq K$, where $b \in B \setminus A$.

*Case 1. $M$ is not a field.* We know from property (1) of Remark 3.2.2 that $M$ is an integral domain, so it has a unique field of fractions inside $K$,

$$M \subsetneq F \coloneqq \mathrm{Frac}(M) = \left\{\tfrac{x}{y} \in K \mid x \in M,\ y \in M \setminus \{0\}\right\} \subseteq K.$$

The ordering on $F$ is uniquely determined by the ordering on $M$ via

$$\tfrac{x}{y} \geq 0 \iff xy \geq 0. \tag{3.2.1}$$

Consider any positive fraction $\frac{x}{y} \in F$ with $x, y > 0$. Let us determine $f\left(\frac{x}{y}\right) \in B$. We have

$$\begin{gathered} f(x) \leq x < \alpha f(x) \\ \alpha^{-1} f(y)^{-1} < y^{-1} \leq f(y)^{-1} \\ \implies \alpha^{-1} f(x) f(y)^{-1} < \tfrac{x}{y} < \alpha f(x) f(y)^{-1} \end{gathered}$$

from which we conclude

$$f\left(\tfrac{x}{y}\right) = \begin{cases} \alpha^{-1} f(x) f(y)^{-1} & \text{if } \alpha^{-1} f(x) f(y)^{-1} < \frac{x}{y} < f(x) f(y)^{-1} \\ f(x) f(y)^{-1} & \text{if } f(x) f(y)^{-1} \leq \frac{x}{y} < \alpha f(x) f(y)^{-1}. \end{cases} \tag{3.2.2}$$

This shows that $f\left(\frac{x}{y}\right) \in A$, with its precise value being uniquely determined by $f|_M$. If we combine this with the fact that $f|_B = \mathrm{id}_B$, we see that for any $z \in F \cap B$ we have $z = f(z) \in A$. Thus $F \cap B = A$ and $F \cap Q_n = P_n$ for all $n \geq 1$.

Combined, this shows that

$$(F, \leq, \alpha, A, \{P_n\}_{n\geq 1}, f|_F)$$

is an $\mathcal{L}^*$-substructure of $\mathcal{K}$. Repeating this reasoning inside $\mathcal{M}^*$ will allow us to extend $\mathcal{M}$ to the field of fractions $F' \coloneqq \mathrm{Frac}(M) \subseteq M^*$, so that

$$(F', \leq, \alpha, A, \{P_n\}_{n\geq 1}, f^*|_{F'})$$

is an $\mathcal{L}^*$-substructure of $\mathcal{M}^*$. But then, the unique field isomorphism

$$\begin{array}{ccc} F & \xrightarrow[\cong]{\iota} & F' \\ \cap & & \cap \\ K & & M^* \end{array}$$

that fixes $M$ will be an $\mathcal{L}^*$-embedding, because the ordering and floor function on $F$ and $F'$ are determined by (3.2.1) and (3.2.2).

*Case 2. $M$ is an ordered field that is not real closed.* We know that $K$ is a real closed field. Hence we can consider the real closure $M^{\mathrm{rc}} \subseteq K$ which will be a proper field extension of $M$. As in the previous case, we would like to determine $f(x)$ for any given positive $x \in M^{\mathrm{rc}}$. This is where valuation theory of ordered fields comes into play.

Let $v : M \longrightarrow\!\!\!\!\!\rightarrow \Gamma_M \cup \{\infty\}$ be the natural valuation of $(M, \leq)$. From Lemma 2.3.8, we know that this extends to a valuation

$$\bar{v} : M^{\mathrm{rc}} \longrightarrow\!\!\!\!\!\rightarrow \widetilde{\Gamma}_M \cup \{\infty\},$$

with value group $\widetilde{\Gamma}_M$ the divisible hull of $\Gamma_M$. Since $v(A) = \Gamma_M$, we can find $n \geq 1$ and $y \in A$ such that

$$\bar{v}(x) = \frac{1}{n}\, v(y) \in \widetilde{\Gamma}_M$$

Because of (A1), all elements

$$y,\ \alpha y,\ \alpha^2 y, \ldots,\ \alpha^{n-1} y$$

lie in the same archimedean class (and thus have the same valuation), and precisely one of them is an element of $P_n$. So without loss of generality, we may assume $y \in P_n$, and therefore $z = y^{1/n} \in A$. Then we can write $\bar{v}(x) = v(y^{1/n}) = v(z)$ (which in fact shows $\widetilde{\Gamma}_M = \Gamma_M$). Now that $x$ and $z$ lie in the same archimedean class, we can find a unique integer $k \in \mathbb{Z}$ such that

$$\alpha^k z \leq x < \alpha^{k+1} z. \tag{3.2.3}$$

This implies $f(x) = \alpha^k z \in A$. Like in the first case, we conclude $M^{\mathrm{rc}} \cap B = A$ and $M^{\mathrm{rc}} \cap Q_n = P_n$.

This proves that

$$(M^{\mathrm{rc}}, \leq, \alpha, A, \{P_n\}_{n\geq 1}, f|_{M^{\mathrm{rc}}})$$

is an $\mathcal{L}^*$-substructure of $\mathcal{K}$. Note that by the universal property of the real closure, there is a unique embedding

$$\iota : M^{\mathrm{rc}} \longhookrightarrow M^*$$

into the real closed field $M^*$ over $M$. This is an $\mathcal{L}_{\mathrm{rcf}} \cup \{\underline{\alpha}\}$-embedding. In particular, inequality (3.2.3) is preserved under $\iota$, so that $f^*(\iota(x)) = \iota(f(x)) = \alpha^k z$ for $x$ and $z$ as above. Hence $\iota$ is in fact an $\mathcal{L}^*$-embedding.

*Case 3. $M$ is a real closed field and $A = B$.* In this particular case, we have $P_n = Q_n$ for all $n \geq 1$. Moreover, Lemma 3.2.3 implies that $\Gamma_M = \Gamma_K$. This means that for any $x \in K_{>0}$, there is $y \in A$ in the same archimedean class as $x$. As in Case 2, we can find a unique integer $k \in \mathbb{Z}$ satisfying

$$\alpha^k y \leq x < \alpha^{k+1} y, \tag{3.2.4}$$

so that $f(x) = \alpha^k y \in A$.

The theory of real closed fields $T_{\mathrm{rcf}}$ has quantifier elimination (Theorem 2.3.7). Since $K$ and $M^*$ are real closed, we can extend $M \longhookrightarrow M^*$ to an $\mathcal{L}_{\mathrm{rcf}}$-embedding

$$\iota : K \longhookrightarrow M^*$$

by the implication (i) $\Longrightarrow$ (iii) of the embedding test (Proposition 3.2.1). From inequality (3.2.4), we see that $\iota$ is actually an $\mathcal{L}^*$-embedding by the same argument as in the previous case.

*Case 4. $M$ is a real closed field and $A \neq B$.* Choose any $b \in B \setminus A$ and consider $M(b) \subseteq K$, a simple field extension of $M$. Let $\gamma = v(b) \in \Gamma_K$. In view of Lemma 3.2.3, we have $\gamma \notin \Gamma_M$. By Lemma 2.3.8, $b$ must be transcendental over $M$. In particular, the value group of $M(b)$ is generated by $\Gamma_M$ and $\gamma$. If we combine this with the fact that $\Gamma_M$ is divisible (which implies $\Gamma_M \cap \gamma\mathbb{Z} = \{0\}$), we obtain the decomposition

$$v(M(b)^\times) = \Gamma_M \oplus \gamma\mathbb{Z} \subseteq \Gamma_K.$$

For any $n \geq 1$, $v(b^n) = n\gamma \notin \Gamma_M$ by divisibility of $\Gamma_M$. This implies $A \cap b^{\mathbb{Z}} = \{1\}$, and shows that we can decompose the subgroup $A\langle b\rangle \subseteq B$ generated by $A$ and $b$ as the direct product

$$A\langle b\rangle = A \times b^{\mathbb{Z}} \subseteq B.$$

By our usual argument, for any positive $x \in M(b)$, we can find $y \in A$, $b^l \in b^{\mathbb{Z}}$ with $v(x) = v(yb^l) \in \Gamma_M \oplus \gamma\mathbb{Z}$, and a unique integer $k \in \mathbb{Z}$ satisfying

$$\alpha^k yb^l \leq x < \alpha^{k+1} yb^l. \tag{3.2.5}$$

As usual, this implies $f(x) = \alpha^k yb^l \in A\langle b\rangle$ and thus $M(b) \cap B = A\langle b\rangle$, proving that

$$\mathcal{M}(b) = (M(b), \leq, \alpha, A\langle b\rangle, \{M(b) \cap Q_n\}_{n\geq 1}, f|_{M(b)})$$

is an $\mathcal{L}^*$-substructure of $\mathcal{K}$. In contrast to previous cases, we had to enlarge the multiplicative subgroup from $A$ to $A\langle b\rangle$. Hence we need the additional step of finding an explicit description for $M(b) \cap Q_n$ for each $n \geq 1$. First, note that

$$M(b) \cap Q_n \subseteq M(b) \cap B = A\langle b\rangle = A \times b^{\mathbb{Z}}.$$

Let $r_n \in \{0, 1, \ldots, n-1\}$ be the unique integer with $\alpha^{r_n} b \in Q_n$. For any $yb^l \in A \times b^{\mathbb{Z}}$ that lies in $Q_n$, we have $yb^l(\alpha^{r_n} b)^{-l} = y\alpha^{-r_n l} \in A \cap Q_n = P_n$, thus

$$M(b) \cap Q_n = \{y(\alpha^{r_n} b)^l \mid y \in P_n,\, l \in \mathbb{Z}\} = P_n \times (\alpha^{r_n} b)^{\mathbb{Z}},$$

giving us the desired explicit description.

Recall that in Lemma 3.2.4, we showed that $B$ and $A^*$ are models of Presburger arithmetic in multiplicative notation. Moreover, since $\mathcal{M}^*$ is $|K|^+$-saturated, $A^*$ will be $|B|^+$-saturated. Again, we can apply the embedding test (Proposition 3.2.1), but this time to the theory $T_{\text{Pres}}$ that has quantifier elimination (Example 2.1.4). It allows us to extend $A \hookrightarrow A^*$ to an elementary embedding $A\langle b\rangle \hookrightarrow A^*$. Let $b^* \in A^*$ be the image of $b$ under this embedding. By virtue of this map being elementary, we know that

(i) $b^* \notin A$;

(ii) $\alpha^{r_n} b^* \in P_n^*$ for all $n \geq 1$;

(iii) $b^*$ defines the same cut as $b$ in the ordering of $A$ and because of (F), in the ordering of $M$ as well.

By the same reasoning as for $b \in B$, (i) implies

(iv) $b^*$ is transcendental over $M$.

Now, we can construct the embedding $\iota : \mathcal{M}(b) \hookrightarrow \mathcal{M}^*$. By (iv), the homomorphism

$$\iota : M(b) \longrightarrow M(b^*) \subseteq M^*$$

that fixes $M$ and sends $b$ to $b^*$ is an isomorphism of fields. By (iii), $\iota$ preserves order. As usual, the inequality (3.2.5) shows that

$$f^*(\iota(x)) = \alpha^k y (b^*)^l = \iota(\alpha^k y b^l) = \iota(f(x)),$$

so $\iota$ is compatible with the floor function. Finally, by (i) and (ii), we obtain

$$M(b^*) \cap A^* = A \times (b^*)^{\mathbb{Z}}$$
$$M(b^*) \cap P_n^* = P_n \times (\alpha^{r_n} b^*)^{\mathbb{Z}}$$

by the same structural analysis as we did for $M(b) \cap B$ and $M(b) \cap Q_n$. Hence $\iota$ is indeed an $\mathcal{L}^*$-embedding. This completes the proof of quantifier elimination in $T^*$.

## 4. Undecidable expansions of local fields

We prove undecidability results for local fields $K$ extended by predicates for discrete infinite cyclic subgroups of the multiplicative group $K^\times$. We will separately study different types of local fields, namely,

- the real field $\mathbb{R}$;
- the $p$-adic fields $K$ (finite extensions of the field of $p$-adic numbers $\mathbb{Q}_p$);
- the fields $\mathbb{F}_q(\!(t)\!)$ of formal Laurent series over fields with $q = p^r$ elements.

Note that there is a unique discrete valuation $v$ on $K$ extending the $p$-adic valuation on $\mathbb{Q}_p$, whereas the field $\mathbb{F}_q(\!(t)\!)$ is endowed with the $t$-adic valuation $v_t$.

We will prove the following three theorems:

**Theorem 4.1.** *Let $\alpha, \beta \in \mathbb{R}_{>1}$ be two real numbers satisfying $\alpha^{\mathbb{Z}} \cap \beta^{\mathbb{Z}} = \{1\}$. Then the theory of the structure $(\mathbb{R}, +, \cdot, \alpha^{\mathbb{Z}}, \beta^{\mathbb{Z}})$ is undecidable.*

**Theorem 4.2.** *Let $K$ be a $p$-adic field and $\alpha, \beta \in K$ two elements with $v(\alpha), v(\beta) > 0$. Assume that $\alpha^{\mathbb{Z}} \cap \beta^{\mathbb{Z}} = \{1\}$. Then the theory of the structure $(K, +, \cdot, \alpha^{\mathbb{Z}}, \beta^{\mathbb{Z}})$ is undecidable.*

**Theorem 4.3.** *Let $\alpha \in \mathbb{F}_q(\!(t)\!)$ be an element with $v_t(\alpha) > 0$. Then the existential theory of the structure $(\mathbb{F}_q(\!(t)\!), +, \cdot, \alpha, \alpha^{\mathbb{Z}})$ is undecidable.*

Theorem 4.1 is due to Hieronymi [9]. The idea of the proof is to define $\mathbb{Z}$ from the range of a sequence $(a_n)_{n\in\mathbb{N}}$ with converging differences $(a_{n+1} - a_n)$. Thereupon, one can invoke the undecidability of $(\mathbb{Z}, +, \cdot)$.

As explained in the introduction, the proofs of Theorem 4.2 and Theorem 4.3 will proceed by showing that certain undecidable expansion of Presburger arithmetic, namely $(\mathbb{N}, +, v_p)$ and $(\mathbb{N}, 0, 1, +, |_p)$, can be interpreted in our structures of interest. First, we will prove in Section 4.2 that multiplication in $\mathbb{N}$ can be defined in both expansion of Presburger arithmetic. In Section 4.3 we will then explain how these expansion of Presburger arithmetic can be interpreted in $(K, +, \cdot, \alpha^{\mathbb{Z}}, \beta^{\mathbb{Z}})$, respectively $(\mathbb{F}_q(\!(t)\!), +, \cdot, \alpha, \alpha^{\mathbb{Z}})$, which will complete our proofs.

For Theorem 4.2, the special case $K = \mathbb{Q}_p$ is due to Mariaule [15]. Theorem 4.3 for $\alpha = t$ and $\alpha^{\mathbb{Z}_{>0}}$ instead of $\alpha^{\mathbb{Z}}$ is due to Pheidas [20]. We will comment on the changes made for the general cases when discussing the proofs.

### 4.1. The real field with two cyclic subgroups.

In this section we will present the proof of Theorem 4.1. This is a corollary of a more general result by Hieronymi [9, Thm. 1.1].

**Theorem 4.1.1.** *Let $D \subseteq \mathbb{R}$ be a closed and discrete set and $f : D^n \longrightarrow \mathbb{R}$ a function such that $f(D^n)$ is somewhere dense. Then $\mathbb{Z}$ can be defined (with parameters) in $(\mathbb{R}, +, \cdot, f)$.*

Indeed, the set $D = \alpha^{\mathbb{N}} \cup \beta^{\mathbb{N}}$ is closed and discrete, and

$$f : D^2 \longrightarrow \mathbb{R}, \quad (x, y) \longmapsto \frac{x}{y},$$

has dense image in $\mathbb{R}_{>0}$. Thus $(\mathbb{R}, +, \cdot, \alpha^{\mathbb{Z}}, \beta^{\mathbb{Z}})$ defines $\mathbb{Z}$. We will present Hieronymi's proof specialised to our case of interest $D = \alpha^{\mathbb{N}} \cup \beta^{\mathbb{N}}$. This will give a definition of $\mathbb{Z}$ in $(\mathbb{R}, +, \cdot, \alpha^{\mathbb{Z}}, \beta^{\mathbb{Z}})$ with one parameter, from which we can deduce undecidability.

**Lemma 4.1.2.** *An expansion of $(\mathbb{R}, +, \cdot)$ defines $\mathbb{Z}$ if and only if it defines the range of a sequence $(a_n)_{n\in\mathbb{N}}$ such that*

$$\lim_{n\to\infty} (a_{n+1} - a_n) \in \mathbb{R}_{>0}.$$

*Proof.* This is Miller's lemma on asymptotic extraction of groups, see [18]. If we can define $\mathbb{Z}$, then we can also define $\mathbb{N}$, which is the range of the sequence $a_n = n$. Conversely, assume that $A$ is the definable range of a sequence $(a_n)_{n\in\mathbb{N}}$ with

$$\lim_{n\to\infty} (a_{n+1} - a_n) = c > 0.$$

Observe that we can define

$$c\mathbb{Z} = \{r \in \mathbb{R} \mid \forall \varepsilon, N > 0 \; \exists x, y > N \, (x, y \in A \wedge |x - y - r| < \varepsilon)\}.$$

From this we can define $c$ as the smallest positive element of $c\mathbb{Z}$. Thus, $\mathbb{Z}$ is definable. □

**Lemma 4.1.3.** *Let $D = \alpha^{\mathbb{N}} \cup \beta^{\mathbb{N}}$. There is a definable bijection*

$$f : D^2 \longrightarrow F$$

*in $(\mathbb{R}, +, \cdot, \alpha^{\mathbb{Z}}, \beta^{\mathbb{Z}})$, where $F \subseteq \mathbb{R}$ is a closed and discrete subset satisfying $|a - b| \geq 1$ for all distinct $a, b \in F$.*

*Proof.* First, let $g : D^2 \longrightarrow \mathbb{R}_{>0}$ be the function that maps

$$(\gamma^n, \delta^m) \longmapsto \begin{cases} \alpha^{2n}\beta^{2m} & \text{if } \gamma^n \in \alpha^{\mathbb{N}} \text{ and } \delta^m \in \alpha^{\mathbb{N}}, \\ \alpha^{2n}\beta^{2m+1} & \text{if } \gamma^n \in \alpha^{\mathbb{N}} \text{ and } \delta^m \in \beta^{\mathbb{N}} \setminus \{1\}, \\ \alpha^{2n+1}\beta^{2m} & \text{if } \gamma^n \in \beta^{\mathbb{N}} \setminus \{1\} \text{ and } \delta^m \in \alpha^{\mathbb{N}}, \\ \alpha^{2n+1}\beta^{2m+1} & \text{if } \gamma^n \in \beta^{\mathbb{N}} \setminus \{1\} \text{ and } \delta^m \in \beta^{\mathbb{N}} \setminus \{1\}. \end{cases}$$

By construction, $g$ is injective and definable. Let $E = g(D^2)$. Since $\alpha, \beta > 1$, we see that $E$ is a closed and discrete subset of $\mathbb{R}_{>0}$. Let $s : E \longrightarrow E$ be the successor function that maps $x \in E$ to the smallest element of $E$ lying above $x$. Then define $h : E \longrightarrow \mathbb{R}_{>0}$ by

$$x \longmapsto x \cdot \max\left(\{(s(y) - y)^{-1} \mid x > y \in E\} \cup \{1\}\right).$$

By construction, $h$ is injective and definable. Thus $f = h \circ g$ is definable. It is a bijection onto $F = h(E)$, where $F$ is closed, discrete, and satisfies $|a - b| \geq 1$ for all distinct $a, b \in F$. □

Note that we have modified the first step in the proof of [9, Lem. 2.1], which uses parameters to define $g$ in the general case.

**Lemma 4.1.4.** *In the structure $(\mathbb{R}, +, \cdot, \alpha^{\mathbb{Z}}, \beta^{\mathbb{Z}})$ we can define $\mathbb{Z}$ by a formula with one parameter.*

*Proof.* By Lemma 4.1.3, we can assume that we have a definable function $f : D \longrightarrow \mathbb{R}_{>0}$, where $D \subseteq \mathbb{R}$ is a definable, closed, and discrete set satisfying $|a - b| \geq 1$ for all distinct $a, b \in D$ that has dense image in $\mathbb{R}_{>0}$. After shrinking $D$, we can assume that $D \subseteq \mathbb{R}_{\geq 1}$ has dense image $f(D) \subseteq (1, 2)$, where $f : D \longrightarrow (1, 2)$ is now a definable function.

We would like to find a sequence $(e_n)_{n\geq 2}$ with definable range, satisfying $e_n \in \left(n, n + \frac{1}{n}\right)$, so that we can apply the lemma on asymptotic extraction of groups. To do so, we first need to construct an auxiliary sequence $(d_n)_{n\geq 1}$. Define, by induction, a sequence $(d_n)_{n\geq 1}$ satisfying

(i) for all $n > m \geq 1$,

$$f(d_m)\left(1 + \frac{d_m^{-2}}{m + \frac{1}{m}}\right) < f(d_n)\left(1 + \frac{d_n^{-2}}{n + \frac{1}{n}}\right)$$
$$f(d_n)\left(1 + \frac{d_n^{-2}}{n}\right) < f(d_m)\left(1 + \frac{d_m^{-2}}{m}\right) < 2;$$

(ii) for all $d \in D$ and $d_1 \leq d_{n-1}^7 < d < d_n$, $n > 1$,

$$f(d)(1 + d^{-2}) < f(d_n) \quad \text{or} \quad f(d_n)(1 + d_n^{-2}) < f(d);$$

(iii) $d_1 > 4$ and $d_n > \max\{4, 2n, d_{n-1}^{49}\}$ for all $n > 1$.

For $n = 1$, choose $d_1 \in D$ with $d_1 > 4$ and $f(d_1)(1 + d_1^{-2}) < 2$. Assume we have already constructed $d_1, \ldots, d_n$ satisfying the above properties. We will now define $d_{n+1}$. A small calculation (see [9, p. 2166]) shows that the set

$$S \coloneqq \left(f(d_n)\left(1 + \frac{d_n^{-2}}{n + \frac{1}{n}}\right), f(d_n)\left(1 + \frac{d_n^{-2}}{n}\right)\right) \setminus \bigcup_{\substack{d\in D \\ d\geq d_n^7}} [f(d), f(d)(1 + d^{-2})]$$

has positive Lebesgue measure. By the Steinhaus theorem, one can find elements in $S$ arbitrarily close together. In particular, we can find $s_1, s_2 \in S$, $s_1 < s_2$, such that the smallest $d \in D$ with $s_1 < f(d) < s_2$ satisfies $d > \max\{4, 2n, d_n^{49}\}$. Then define

$$d_{n+1} = \min\{d \in D \mid s_1 < f(d) < s_2\}.$$

One can easily verify that $d_{n+1}$ satisfies (i)–(iii) by construction (see [9, p. 2167]).

We can now define the sequence $(e_n)_{n\geq 2}$. Let

$$c \coloneqq \lim_{n\to\infty} f(d_n)\left(1 + \frac{d_n^{-2}}{n}\right)$$

be a fixed constant. Define

$$e_n = \frac{d_n^{-2} f(d_n)}{c - f(d_n)}$$

for all $n \geq 2$. Note that (i) implies

$$f(d_n)\left(1 + \frac{d_n^{-2}}{n + \frac{1}{n}}\right) < c < f(d_n)\left(1 + \frac{d_n^{-2}}{n}\right), \tag{4.1.1}$$

which is equivalent to $e_n \in \left(n, n+\frac{1}{n}\right)$. By Lemma 4.1.2, we are left to prove that the range $C = \{d_n\}_{n\geq 2}$ of the sequence $(d_n)_{n\geq 2}$ is definable. If we let $\varphi(x)$ be the formula

$$\forall y \in D\,(f(y) < c < f(y)(1+y^{-2}) \to (y < x^{1/7} \vee x \leq y)),$$

we claim that

$$C = \{d \in D \mid f(d) < c < f(d)(1+d^{-2}) \wedge d_2 \leq d \wedge \varphi(d)\}. \tag{4.1.2}$$

Consider any $n \geq 2$. Then (4.1.1) implies that $f(d_n) < c < f(d_n)(1+d^{-2})$, so assume that $\varphi(d_n)$ does not hold, i.e., there is $d \in D$ with

$$d_n^{1/7} \leq d < d_n \quad \text{and} \quad f(d) < c < f(d)(1+d^{-2}).$$

Using that $d_{n-1}^{49} < d_n$ implies $d_{n-1}^7 < d < d_n$, we see that (ii) implies

$$c < f(d)(1+d^{-2}) < f(d_n) \quad \text{or} \quad f(d_n)(1+d_n^{-2}) < f(d) < c,$$

which contradicts $f(d) < c < f(d)(1+d^{-2})$. Thus $\varphi(d_n)$ holds.

Conversely, assume that there is $d \in D$, $d_{n-1} < d < d_n$, satisfying $f(d) < c < f(d)(1+d^{-2})$ and $\varphi(d)$. If we apply $\varphi(d)$ to $d_{n-1}$, we get $d_{n-1}^7 < d < d_n$. This yields the same contradiction as above. Hence (4.1.2) holds true, which defines $C$ by a formula with one parameter. □

**Proof of Theorem 4.1.** Assume towards a contradiction that there is an algorithm that decides for each sentence $\varphi$, whether $(\mathbb{R}, +, \cdot, \alpha^{\mathbb{Z}}, \beta^{\mathbb{Z}}) \models \varphi$ or not. We claim that this implies a positive solution to Hilbert's Tenth Problem.

By Lemma 4.1.4, there is a formula $\zeta(x, y)$ with

$$\mathbb{Z} = \{r \in \mathbb{R} \mid \mathbb{R} \models \zeta(r, c)\},$$

where $c$ is the constant defined in the lemma. A polynomial $p(X_1, \ldots, X_n) \in \mathbb{Z}[X_1, \ldots, X_n]$ has a solution in $\mathbb{Z}$ if and only if

$$\exists y \exists x_1 \ldots \exists x_n [\zeta(0, y) \wedge (\forall z\,(\zeta(z, y) \wedge z > 0) \to z \geq 1) \wedge (\forall z\ \zeta(z, y) \leftrightarrow \zeta(z+1, y))]$$
$$\wedge [\zeta(x_1, y) \wedge \ldots \wedge \zeta(x_n, y) \wedge p(x_1, \ldots, x_n) = 0]$$

holds in $\mathbb{R}$. Thus, given a polynomial $p(X_1, \ldots, X_n)$ with integer coefficients, we can apply the decision algorithm on this sentence to determine whether or not $p(X_1, \ldots, X_n)$ has a solution in $\mathbb{Z}$, in contradiction to Matiyasevich's negative answer to Hilbert's Tenth Problem. □

The same relativisation argument can be used to reduce the undecidability of $(\mathbb{R}, +, \cdot, \alpha^{\mathbb{Z}}, \beta^{\mathbb{Z}})$ to the undecidability of $(\mathbb{Z}, +, \cdot)$, instead of Hilbert's Tenth Problem.

4.2. **Expansions of Presburger arithmetic by $p$-adic operations.** The expansions of Presburger arithmetic of interest to us, are obtained by expanding $(\mathbb{N}, +)$ by certain $p$-adic operations. Specifically, we consider the following functions and relations on $\mathbb{N}$.

**Definition 4.2.1.** Fix some prime number $p$. We use the following notation for functions/relations on $\mathbb{N}$:

| | |
|---|---|
| $v_p$ | is the $p$-adic valuation[7] on $\mathbb{N}$; |
| $\mathcal{V}_p$ | is a function that maps $n$ to the largest power of $p$ dividing $n$, which is $p^{v_p(n)}$; |
| $p^{\square}$ | is the base $p$ power function that maps $n$ to $p^n$; |
| $\mid_p$ | is a binary relation given by $n \mid_p m \iff \exists k \in \mathbb{N}\ m = p^k n$. |

**Example 4.2.2.** The symbol $|_p$ is somewhat unusual and may take some getting used to. For example, we have

$$1 \mid_2 8,\ 2 \mid_3 18,\ 10 \mid_5 50,$$

but also

$$3 \nmid_2 5,\ 1 \nmid_3 8,\ 2 \nmid_3 12.$$

However, it is precisely this relation that will show up in our study of $\mathbb{F}_q(\!(t)\!)$. ⊣

§ 1. *Expansion of Presburger arithmetic by $v_p$.* We will show that $(\mathbb{N}, +, \mathcal{V}_p, p^{\square})$ is undecidable and, as a corollary, that the same is true for $(\mathbb{N}, +, v_p)$. For this purpose, it will suffice to prove that the multiplication operation is definable in these structures. Although not stated in this form, the fact that $(\mathbb{N}, +, \mathcal{V}_p, p^{\square})$ is undecidable goes back to Elgot and Rabin [7]. In [6], Cherlin and Point give a direct argument for the undecidability of $(\mathbb{N}, +, \mathcal{V}_2, 2^{\square})$.

First, we need a criterion for undecidability. The next proposition says that if finite binary relations $A \subseteq \mathbb{N}^2$ can be coded by a natural number, such that there is a formula that recognises this coding, then multiplication can be defined from addition. Our proof is adapted from [7, p. 171].

**Proposition 4.2.3.** *Let $\mathcal{N}$ be an $\mathcal{L}$-structure that expands $(\mathbb{N}, +)$ by finitely many new symbols. Assume that there is an $\mathcal{L}$-formula $\mathrm{Rel}(x, y, c)$ with the following property: for any finite binary relation $A \subseteq \mathbb{N}^2$, there is an element $C \in \mathbb{N}$ such that for all $m, n \in \mathbb{N}$,*

$$(m, n) \in A \quad \textit{if and only if} \quad \mathrm{Rel}(m, n, C).$$

*Then $\mathcal{N}$ is undecidable.*

*Proof.* If suffices to show that we can define multiplication of natural numbers in $\mathcal{N}$. We write $x \leq y$ to abbreviate $\exists d\ (y = x + d)$. The constants 0 and 1 can also be defined in $(\mathbb{N}, +)$. Let $\mathrm{Fcn}(b, c)$ denote the formula

$$\forall x\,(x \leq b \to \exists! y\ \mathrm{Rel}(x, y, c)).$$

For any $B, C \in \mathbb{N}$, the formula $\mathrm{Fcn}(B, C)$ states that for the code $C$, $\mathrm{Rel}(x, y, C)$ defines a function for values $x \leq B$. But then, $x \cdot y = z$ can be defined by the $\mathcal{L}$-formula

$$\exists c\ [\mathrm{Fcn}(y, c) \wedge \mathrm{Rel}(0, 0, c) \wedge [\forall u \forall w(u < x \wedge \mathrm{Rel}(u, w, c)) \to \mathrm{Rel}(u + 1, w + x, c)] \wedge \mathrm{Rel}(y, z, c)],$$

which simulates a finite recursion up to $y$. If $\mathcal{N}$ is decidable, then so must be $(\mathbb{N}, +, \cdot)$ (construct an algorithm that transforms a $\{+, \cdot\}$-sentence into an equivalent $\mathcal{L}$-sentence and then applies a decision routine to the later). However, $(\mathbb{N}, +, \cdot)$ is undecidable, so $\mathcal{N}$ must be undecidable as well. □

Using a concrete coding for finite binary relations over the language $\{+, \mathcal{V}_p, p^{\square}\}$ (slightly different from the one used in [6, p. 21]), the preceding proposition implies:

[7] For $n = 0$ we may take $v_p(0)$ to be any natural number, say $v_p(0) = 0$ (in contrast to the usual convention $v_p(0) = \infty$). We also set $\mathcal{V}_p(0) = 1$.

**Theorem 4.2.4.** *The theory of the structure* $(\mathbb{N}, +, \mathcal{V}_p, p^{\square})$ *is undecidable.*

*Proof.* Given a finite binary relation $A \subseteq \mathbb{N}^2$, define the code

$$C = \sum_{(m,n)\in A} p^{m+p^{m+n}}.$$

Note that for any two pairs $(m_1, n_1), (m_2, n_2) \in \mathbb{N}^2$, we have

$$m_1 + p^{m_1+n_1} = m_2 + p^{m_2+n_2} \iff (m_1, n_1) = (m_2, n_2).$$

In other words, we code a pair $(m, n) \in A$ as a 1-digit at position $m + p^{m+n}$ in the $p$-adic expansion of $C$. Using $\mathcal{V}$ and $p^{\square}$ this process can be reversed, that is, we can extract $(m, n)$ from $C$. Let $\mathrm{Rel}(x, y, c)$ be the formula

$$\exists s_1 \exists s_2 \exists s_3 \, (s_1 + s_2 + s_3 = c \wedge s_1 < s_2 \wedge s_2 = p^{x+p^{x+y}} \wedge (s_2 < \mathcal{V}_p(s_3) \vee s_3 = 0)).$$

This formula satisfies the defining property in Proposition 4.2.3. Hence $(\mathbb{N}, +, \mathcal{V}_p, p^{\square})$ is undecidable. □

**Corollary 4.2.5.** *The theory of the structure* $(\mathbb{N}, +, v_p)$ *is undecidable.*

*Proof.* The relation $p^x = y$ can be defined by

$$y \neq 0 \wedge v_p(y) = x \wedge (\forall z > 0 \, (v_p(z) = x \to y \leq z)),$$

and $\mathcal{V}(x) = y$ by $y = p^{v_p(x)}$. Thus by the previous theorem, $(\mathbb{N}, +, v_p)$ is undecidable. □

§ 2. *Expansion of Presburger arithmetic by* $|_p$. The following theorem is due to Pheidas [20, Thm. 1].

**Theorem 4.2.6.** *The existential theory of the structure* $(\mathbb{N}, 0, 1, +, |_p)$ *is undecidable.*

We will reproduce the proof from [20]. Again, we would like to define multiplication in $\mathbb{N}$ from $+$ and $|_p$ (by an existential formula). This time though, we will need a few elementary number theoretic lemmas.

**Lemma 4.2.7.** *Assume that for* $a, b, c, d \in \mathbb{Z}_{>0}$, *we have*

$$(p^a - 1)(p^b - 1) = (p^c - 1)(p^d - 1).$$

*Then* $\{a, b\} = \{c, d\}$.

*Proof.* Without loss of generality we may assume $a \geq b$, $c \geq d$, and $b \geq d$. Note that this implies $c \geq a$. We obtain the equation

$$p^{a+b} - p^a - p^b = p^{c+d} - p^c - p^d,$$

and after cancellation,

$$p^{a+b-d} - p^{a-d} - p^{b-d} = p^c - p^{c-d} - 1.$$

All powers of $p$ that occur in the above equation are divisible by $p^{b-d}$ (since $c \geq a \geq b$). In particular, $p^{b-d}$ divides 1, so we have $b = d$ and $a = c$. □

**Lemma 4.2.8.** *Let $m, n \in \mathbb{Z}_{>0}$ and $a \in \mathbb{N}$. Then*

$$m = p^a n \quad \textit{iff} \quad n \mid_p m,\ (n+1) \mid_p m + p^a,\ \textit{and}\ (n+p) \mid_p m + p^{a+1}.$$

*Proof.* One direction is obvious. So assume that

$$\begin{aligned} m &= np^b \\ m + p^a &= (n+1)p^c \\ m + p^{a+1} &= (n+p)p^d, \end{aligned}$$

where $b, c, d \in \mathbb{N}$. We need to show $a = b$. From the above system of equations, we get

$$\begin{aligned} n(p^b - p^c) &= p^c - p^a \\ n(p^b - p^d) &= p^{d+1} - p^{a+1}, \end{aligned}$$

and thus

$$(p^c - p^a)(p^b - p^d) = (p^b - p^c)(p^{d+1} - p^{a+1}). \tag{4.2.1}$$

Any one of $a = c$, $a = d$, $b = c$, or $b = d$, implies $a = b$. So assume towards a contradiction that $a \neq c, d$ and $b \neq c, d$. Depending on the order of $a$, $b$, $c$, $d$, we can further rewrite (4.2.1).

If $b > c, d$ and $c, d > a$, then

$$(p^{c-a} - 1)(p^{b-d} - 1)p^{a+d} = (p^{b-c} - 1)(p^{d-a} - 1)p^{c+a+1}.$$

This implies $a + d = c + a + 1$ (i.e. $d = c + 1$), and by Lemma 4.2.7, $c - a = b - c$ and $b - d = d - a$, or, $c - a = d - a$ and $b - d = b - c$ (both of which imply $c = d$). Thus we get a contradiction in this case.

For other orders of $a$, $b$, $c$, $d$, we do the same: factor out the biggest power of $p$ on both sides of (4.2.1) and apply Lemma 4.2.7. It is straightforward to check the remaining cases (see [20, Lem. 2]). □

**Lemma 4.2.9.** *Let $m, n \in \mathbb{Z}_{>0}$. Then $n \mid m$ if and only if $p^n - 1 \mid p^m - 1$. Moreover, if $m = nk$ with $k \in \mathbb{Z}_{>0}$, then*

$$\frac{p^m - 1}{p^n - 1} \equiv k \pmod{p^n - 1}.$$

*Proof.* If $n \mid m$, then

$$p^m = (p^n)^{\frac{m}{n}} \equiv 1^{\frac{m}{n}} = 1 \pmod{p^n - 1}.$$

Conversely, if $p^n - 1 \mid p^m - 1$, write $m = qn + r$, where $q \in \mathbb{N}$ and $0 \leq r < n$. But then $p^n - 1 \mid p^m - p^{qn}$, which implies $p^n - 1 \mid p^r - 1$ and thus $r = 0$.

If we can write $m = nk$, then

$$\frac{p^m - 1}{p^n - 1} = (p^n)^{k-1} + \ldots + p^n + 1 \equiv 1^{k-1} + \ldots + 1^1 + 1 = k \pmod{p^n - 1}.$$ □

**Lemma 4.2.10.** *Let $m, n \in \mathbb{N}$. Then*

$$m = n^2 \quad \textit{iff} \quad \exists a, b \in \mathbb{N} \begin{cases} n < p^a - 1, \ m < p^{2a} - 1, \\ p^{2a} - 1 \mid p^b - 1, \\ \frac{p^b-1}{p^{2a}-1} \equiv n \pmod{p^{2a} - 1}, \ \textit{and} \\ \left(\frac{p^b-1}{p^{2a}-1}\right)^2 \equiv m \pmod{p^{2a} - 1}. \end{cases} \tag{4.2.2}$$

*Proof.* Assume $m = n^2$. For $n = 0$, we can take $a = 1$ and $b = 2(p^2 - 1)$. For $n \neq 0$, choose $a \in \mathbb{Z}_{>0}$ so that $n < p^a - 1$, $m < p^{2a-1}$, and let $b = 2an \in \mathbb{Z}_{>0}$. The properties then hold by Lemma 4.2.9.

Conversely, assume that the right-hand side holds for some $a, b \in \mathbb{N}$. We have

$$m \equiv \left(\frac{p^b - 1}{p^{2a} - 1}\right)^2 \equiv n^2 \pmod{p^{2a} - 1}.$$

Note that $n < p^a - 1$ implies $n^2 < p^{2a} - 1$, so we must have $m = n^2$. □

**Proposition 4.2.11.** *The relation $m = n \cdot k$ in $\mathbb{N}$ can be defined by an existential formula in the language $\{0, 1, +, |_p\}$.*

*Proof.* It suffices to have an existential definition for $m = n^2$, since

$$m = n \cdot k \quad \text{iff} \quad \exists r, s \ (r = n^2 \wedge s = k^2 \wedge (n + k)^2 = r + m + m + s).$$

Thus we are left to prove that the conditions in (4.2.2) can be expressed by existential formulas in the language $\{0, 1, +, |_p\}$. The definition for $m = n^2$ will begin with

$$\exists P, Q, R \ [1 \mid_p P \wedge 1 \mid_p R \wedge P \mid_p Q \wedge (P + 1) \mid_p (Q + P) \wedge (P + p) \mid_p (Q + pP)] \ldots$$

which expresses the fact $P$ and $R$ are powers of $p$ (think: $p^a$ and $p^b$), and $Q = P^2$ (think: $p^{2a}$) by Lemma 4.2.8. Instead of $n < p^a - 1$ and $m < p^{2a} - 1$, we can write

$$\exists d \ P = (n + 2) + d \quad \text{and} \quad \exists e \ Q = (m + 2) + e.$$

The condition $p^{2a} - 1 \mid p^b - 1$ is equivalent to

$$\exists c \ (c + 1)Q = R + c,$$

which by Lemma 4.2.8 can be further converted to

$$\exists c \ [(c + 1) \mid_p (R + c) \wedge (c + 2) \mid_p (R + c + Q) \wedge (c + 1 + p) \mid_p (R + c + pQ)].$$

The first equivalence relation in (4.2.2) is equivalent to

$$\begin{aligned} &\exists f \ \frac{R - 1}{Q - 1} = n + f(Q - 1) \\ \longleftrightarrow \ &\exists f \ R + 2fQ + n = fQ^2 + nQ + f + 1. \end{aligned}$$

Now with several applications of Lemma 4.2.8, this can be rewritten as an existential formula in the language $\{0, 1, +, |_p\}$ (certainly occupying more than two lines of text). The same can be done for the second equivalence relation in (4.2.2). □

Now that multiplication in $\mathbb{N}$ can be defined in terms of $+$ and $|_p$ by an existential formula, we can easily see that $\mathrm{Th}_\exists(\mathbb{N}, 0, 1, +, |_p)$ is undecidable:

**Proof of Theorem 4.2.6.** The existential theory of $(\mathbb{N}, 0, 1, +, \cdot)$ can be effectively coded in the existential theory of $(\mathbb{N}, 0, 1, +, |_p)$. If $\mathrm{Th}_\exists(\mathbb{N}, 0, 1, +, |_p)$ is decidable, then so must be $\mathrm{Th}_\exists(\mathbb{N}, 0, 1, +, \cdot)$ (construct an algorithm that translates an existential $\{0, 1, +, \cdot\}$-sentence into an existential $\{0, 1, +, |_p\}$-sentence and then applies a decision routine to the later). By the negative answer to Hilbert's Tenth Problem, however, $\mathrm{Th}_\exists(\mathbb{N}, 0, 1, +, \cdot)$ is undecidable. Hence $\mathrm{Th}_\exists(\mathbb{N}, 0, 1, +, |_p)$ is undecidable as well. □

4.3. **Undecidable expansions of non-archimedean local fields.** We will use the fact that $(\mathbb{N}, +, v_p)$ is undecidable (Corollary 4.2.5) to prove Theorem 4.2. Similarly, we will use the fact that the existential theory of $(\mathbb{N}, 0, 1, +, |_p)$ is undecidable (Theorem 4.2.6) to prove Theorem 4.3.

§ 1. *Elementary theory of expansions of p-adic fields.* Let us repeat the statement of the theorem we would like to prove.

**Theorem.** *Let $K$ be a p-adic field and $\alpha, \beta \in K$ two elements with $v(\alpha), v(\beta) > 0$. Assume that $\alpha^{\mathbb{Z}} \cap \beta^{\mathbb{Z}} = \{1\}$. Then the theory of the structure $(K, +, \cdot, \alpha^{\mathbb{Z}}, \beta^{\mathbb{Z}})$ is undecidable.*

*Proof.* Write $\mathcal{O}$ for the valuation ring of $K$, and let $\pi$ be a uniformiser for the maximal ideal $\mathcal{M}$ of $\mathcal{O}$, i.e., $\mathcal{M} = \pi\mathcal{O}$. Let $e \geq 1$ be the ramification degree of $K/\mathbb{Q}_p$. Thus $\frac{1}{e}\mathbb{Z}$ is the value group of $K$, since $v$ extends the $p$-adic valuation $v_p$ on $\mathbb{Q}_p$.

We may assume without loss of generality, that $v(\alpha) = v(\beta) \in \mathbb{Z}_{>0}$ by replacing $\alpha$ and $\beta$ with one of their powers (note that all subgroups of $\alpha^{\mathbb{Z}}$ and $\beta^{\mathbb{Z}}$ are definable in our given structure). Hence $\alpha/\beta \in \mathcal{O}^\times$. Again, by replacing $\alpha$ and $\beta$ with suitable powers if necessary, we may assume $\alpha/\beta = 1 + \gamma$, $\gamma \in \pi^{e+1}\mathcal{O}$, since $\mathcal{O}^\times/(1 + \pi^{e+1}\mathcal{O})$ is a finite quotient. From $\alpha^{\mathbb{Z}} \cap \beta^{\mathbb{Z}} = \{1\}$ we know that $\gamma \neq 0$. The $p$-adic logarithm

$$\log(1 + x) = x - \frac{x^2}{2} + \frac{x^3}{3} - \dots$$

converges on $1 + \pi^k\mathcal{O}$ for $k > \frac{e}{p-1}$, and satisfies $v(\log(1 + x)) = v(x)$. In particular, we have $v(\log(1 + \gamma)) = v(\gamma)$ and hence

$$v((1 + \gamma)^n - 1) = v(\log((1 + \gamma)^n)) = v(n \log(1 + \gamma)) = v_p(n) + v(\gamma) \tag{4.3.1}$$

for all $n \geq 1$. Using this identity, we will now show that the function $\alpha^{\mathbb{N}} \longrightarrow \alpha^{\mathbb{N}}$, $\alpha^n \longmapsto \alpha^{v_p(n)}$, is definable in our structure.

First, note that $\mathcal{O}$ and hence the formula $v(x) = v(y)$ are definable. Thus the functions $\alpha^{\mathbb{Z}} \longrightarrow \beta^{\mathbb{Z}}$, $\alpha^n \longmapsto \beta^n$, and $\alpha^{\mathbb{Z}} \longrightarrow (1+\gamma)^{\mathbb{Z}}$, $\alpha^n \longmapsto (1+\gamma)^n$ are definable in $(K, +, \cdot, \alpha^{\mathbb{Z}}, \beta^{\mathbb{Z}})$. Furthermore, there are unique integers $0 \leq q$, $0 \leq r < v(\alpha)$ with

$$v_p(n) = q \cdot v(\alpha) + r = v(\alpha^q) + r,$$

where both $\alpha^q$ and $r$ are definable from $(1 + \gamma)^n$ via (4.3.1). Hence

$$\alpha^{\mathbb{N}} \longrightarrow \alpha^{\mathbb{N}}, \quad \alpha^n \longmapsto \left(\alpha^q\right)^{v(\alpha)} \cdot \alpha^r = \alpha^{v_p(n)},$$

is definable. This shows that we can interpret $(\mathbb{N}, +, v_p)$ in $(K, +, \cdot, \alpha^{\mathbb{Z}}, \beta^{\mathbb{Z}})$ via the monoid $\alpha^{\mathbb{N}}$. Since the theory of $(\mathbb{N}, +, v_p)$ is undecidable, the theory of $(K, +, \cdot, \alpha^{\mathbb{Z}}, \beta^{\mathbb{Z}})$ must also be undecidable. □

§ 2. *Existential theory of expansions of* $\mathbb{F}_q(\!(t)\!)$. We consider local fields of characteristic $p$ with a discrete subgroup generated by an element $\alpha \in \mathbb{F}_q(\!(t)\!)$ of positive $t$-adic valuation. In [20], Pheidas proved Theorem 1.5 from the introduction by

- showing that the relation $n \mid_p m$ can be effectively coded in $\mathbb{F}_q(\!(t)\!)$ by an existential formula via $\alpha^{\mathbb{Z}_{>0}}$, and
- using the fact that $\mathrm{Th}_\exists(\mathbb{N}, 0, 1, +, \mid_p)$ is undecidable (Theorem 4.2.6).

Generalising from $\alpha = t$ to any $\alpha$ of positive valuation, we follow the same strategy. However, in contrast to [20], we will have to treat the case when $p$ divides $v_t(\alpha)$ separately. Essential to the coding is the unique arithmetic of $\mathbb{F}_q(\!(t)\!)$.

**Remark 4.3.1.** 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-bijective endomorphism on $\mathbb{F}_q(\!(t)\!)$ with image

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

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

**Lemma 4.3.2.** *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 $m, n \in \mathbb{Z}_{>0}$ as follows:*

$$n \mid_p m \quad \textit{iff} \quad m \geq n \wedge \exists a \in \mathbb{F}_q(\!(t)\!)\ \alpha^{-m} - \alpha^{-n} = a^p - a. \tag{4.3.2}$$

*Proof.* The proof of [20, Lem. 1], which covers the case $\alpha = t$, will work here as well. We repeat it here.

Assume $n \mid_p m$ holds and write $m = np^k$ for some $k \in \mathbb{N}$. Then the element

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

witnesses that the right-hand side of the equivalence holds. Conversely, assume that for positive integers $m \geq n$ there is $a \in \mathbb{F}_q(\!(t)\!)$ satisfying

$$\alpha^{-m} - \alpha^{-n} = a^p - a.$$

We want to show $n \mid_p m$. Write $m = m_0 p^{v_p(m)}$ and $n = n_0 p^{v_p(n)}$, where both $m_0, n_0 \in \mathbb{Z}_{>0}$ are not divisible by $p$. By the first part of the proof, we can find $b, c \in \mathbb{F}_q(\!(t)\!)$ with

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

If we set $d = a - b + c$, we can combine the above three equations to

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

Now if $m_0 = n_0$, we are done since $m \geq n$. So assume $m_0 \neq n_0$. In that case,

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

At the same time, we know that $v_t(d) < 0$ implies that $v_t(d^p - d)$ is divisible by $p$, contradicting our assumption that $v_t(\alpha)$, $m_0$, $n_0$ are not divisible by $p$. □

**Remark 4.3.3.** Note that (4.3.2) still holds true in the case where we can write $\alpha = \beta^{p^k}$, $k \geq 1$, with $v_t(\beta)$ not divisible by $p$. Indeed, for $m \geq n$, we have that

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

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

The characterisation of $\mid_p$ given by (4.3.2) will not, however, work for all possible values of $\alpha$, as the following example shows.

**Example 4.3.4.** Consider $p = q = 3$, and thus the local field $\mathbb{F}_3(\!(t)\!)$. Take

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

with $v_t(\alpha) = 3$ divisible by $p = 3$. Then

$$\alpha^{-2} - \alpha^{-1} = a^3 - a$$

has a solution in $\mathbb{F}_3(\!(t)\!)$, namely,

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

as can be seen by direct calculation:

$$\alpha^{-2} - \alpha^{-1} = t^{-6} + t^{-3} + 2t^{-2} + 2t^{-1} + t + 2t^2 + 2t^3 + t^4 = a^3 - a.$$

But note that the relation $1 \mid_3 2$ does not hold. ⊣

When $p$ divides $v_t(\alpha)$, it is hence necessary to change our characterisation of $\mid_p$ in (4.3.2) to include such $\alpha$ as in the example. For this purpose, we need the following definition:

**Definition 4.3.5.** Given $x \in \mathbb{F}_q(\!(t)\!)$, written as a Laurent series

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

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 $x \in \mathbb{F}_q(\!(t^p)\!)$.

One could call $\hat{v}_t$ the "$p^{\text{th}}$-power-omitting $t$-adic valuation".[8] It will be of use to us, because we can capture its behaviour under exponentiation in some important instances.

**Lemma 4.3.6.** *Assume that $\alpha \in \mathbb{F}_q(\!(t)\!)$ is not a $p^{th}$ power, but $p \mid v_t(\alpha)$. Let $N \in \mathbb{Z}_{>0}$ be not divisible by $p$. Then*

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

[8] 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 not a group homomorphism.

*Proof.* Decompose $\alpha$ as $\alpha = \beta + \gamma$, where $\beta$ contains all monomials with exponent divisible by $p$ and $\gamma$ contains all monomials with exponent not divisible by $p$. By assumption,

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

If we consider the binomial theorem for $(\beta + \gamma)^n$, we see 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 4.3.7.** *Fix an element $\alpha \in \mathbb{F}_q(\!(t)\!)$ with valuation $v_t(\alpha) = C > 0$ divisible by $p$. Assume in addition that $\alpha$ is not a $p^{th}$ power, so that $\hat{v}_t(\alpha^{-1}) = D \in \mathbb{Z}$. Then for any choice of $N \in \mathbb{Z}_{>0}$ satisfying*

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

*we have 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 $m, n \in \mathbb{Z}_{>0}$.*

*Proof.* If $n \mid_p m$ holds, we can virtually take the same witness for $a \in \mathbb{F}_q(\!(t)\!)$ as before. For the converse, consider integers $m \geq n$ such that there is $a \in \mathbb{F}_q(\!(t)\!)$ with

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

As in the previous proof, we write $m = m_0 p^{v_p(m)}$ and $n = n_0 p^{v_p(n)}$, and can find $b, c \in \mathbb{F}_q(\!(t)\!)$ with

$$\alpha^{-mN} - \alpha^{-m_0 N} = b^p - b$$
$$\alpha^{-nN} - \alpha^{-n_0 N} = c^p - c.$$

If we set $d = a - b + c$, this yields

$$\alpha^{-m_0 N} - \alpha^{-n_0 N} = d^p - d. \tag{4.3.3}$$

We are done if $m_0 = n_0$. Thus assume without loss of generality that $m_0 > n_0 \geq 1$. Instead of taking the $t$-adic valuation on both sides of equation (4.3.3) to arrive at a contradiction, as we did before, we look at the $p^{\text{th}}$-power-omitting $t$-adic valuation. By Lemma 4.3.6 and the fact that $p \nmid m_0 N$, we have

$$\hat{v}_t(\alpha^{-m_0 N} - \alpha^{-n_0 N}) = -(m_0 N - 1)C + D. \tag{4.3.4}$$

If we evaluate the right-hand side of (4.3.3), we get

$$\hat{v}_t(d^p - d) = \hat{v}_t(d) \geq v_t(d). \tag{4.3.5}$$

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

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

together with (4.3.3), (4.3.4), and (4.3.5), to obtain the inequality

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

After rearranging, we have

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

contradicting our choice of $N$. □

**Example 4.3.8.** Consider $\alpha = (t^{-3} + 1 + t + t^2)^{-1} \in \mathbb{F}_3(\!(t)\!)$ from our previous example. We have $v_t(\alpha) = C = 3$ and $\hat{v}_t(\alpha^{-1}) = D = 1$. Hence we can take $N = 2$ in the preceding lemma. In particular, the lemma says that the equation

$$\alpha^{-4} - \alpha^{-2} = a^3 - a$$

has no solution $a \in \mathbb{F}_3(\!(t)\!)$, whereas

$$\alpha^{-2} - \alpha^{-1} = a^3 - a$$

does have one. ⊣

By combining Lemma 4.3.2 and Lemma 4.3.7, we complete our coding of $|_p$ inside $\mathbb{F}_q(\!(t)\!)$ for arbitrary $\alpha$.

**Corollary 4.3.9.** *Fix an element $\alpha \in \mathbb{F}_q(\!(t)\!)$ with valuation $v_t(\alpha) > 0$. There exists a parameter $N \in \mathbb{Z}_{>0}$, depending on $\alpha$, 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 $m, n \in \mathbb{Z}_{>0}$.*

*Proof.* Write $\alpha = \beta^{p^k}$, $k \geq 0$, such that $\beta$ is not a $p^{\text{th}}$ power in $\mathbb{F}_q(\!(t)\!)$. We consider two cases:

*Case 1. $p$ does not divide $v_t(\beta)$.* By Lemma 4.3.2 and Remark 4.3.3, we can choose $N = 1$.

*Case 2. $p$ divides $v_t(\beta)$.* By Lemma 4.3.7 and the idea of Remark 4.3.3, we can choose $N$ to be the smallest natural number not divisible by $p$ bigger than $\frac{\hat{v}_t(\beta^{-1})}{v_t(\beta)} + 1$. □

From this, we can conclude our main theorem (Theorem 4.3) about the undecidability of the existential theory of local fields of characteristic $p$ with a discrete infinite cyclic subgroup.

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

*Proof.* First, we need to identify $\alpha^{\mathbb{N}}$ in this structure. Because $v_t(\alpha) > 0$, we know that

$$\alpha^{\mathbb{N}} = \alpha^{\mathbb{Z}} \cap \mathbb{F}_q[\![t]\!].$$

In [2], 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 $\alpha^{\mathbb{N}}$ in $(\mathbb{F}_q(\!(t)\!), +, \cdot, \alpha, \alpha^{\mathbb{Z}})$. By Corollary 4.3.9, we can interpret $(\mathbb{N}, 0, 1, +, |_p)$ in $(\mathbb{F}_q(\!(t)\!), +, \cdot, \alpha, \alpha^{\mathbb{Z}})$ using existential formulas. Since the existential theory of $(\mathbb{N}, 0, 1, +, |_p)$ is undecidable, the existential theory of $(\mathbb{F}_q(\!(t)\!), +, \cdot, \alpha, \alpha^{\mathbb{Z}})$ must also be undecidable. □

## References


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

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

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

[4] James Ax and Simon B. Kochen. Diophantine problems over local fields II. A complete set of axioms for $p$-adic number theory. *American Journal of Mathematics*, 87(3):631–648, 1965.

[5] George S. Boolos, John P. Burgess, and Richard C. Jeffrey. *Computability and Logic*. Cambridge University Press, 2007.

[6] Gregory Cherlin and Françoise Point. On extensions of presburger arithmetic. *Proceedings of the 4th Easter conference on model theory (Gross Köris)*, Seminarberichte 86:17–34, 1986.

[7] Calvin C. Elgot and Michael O. Rabin. Decidability and undecidability of extensions of second (first) order theory of (generalized) successor. *Journal of Symbolic Logic*, 31(2):169–181, 1966.

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

[13] Angus Macintyre and Alex J. Wilkie. On the decidability of the real exponential field. In Piergiorgio Odifreddi, editor, *Kreisel 70th Birthday Volume*, pages 441–467. CLSI, 1995.

[14] Nathanaël Mariaule. Model theory of the field of $p$-adic numbers expanded by a multiplicative subgroup. Preprint, 2018. 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] David Marker. *Model Theory: An Introduction*, volume 217 of *Graduate Texts in Mathematics*. Springer-Verlag, 2002.

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

[18] Chris Miller. Avoiding the projective hierarchy in expansions of the real field by sequences. *Proceedings of the American Mathematical Society*, 134(5):1483–1493, 2005.

[19] Jürgen Neukirch. *Algebraic Number Theory*. Springer Berlin Heidelberg, 1999.

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

[21] Alexander Prestel and Peter Roquette. *Formally p-adic Fields*, volume 1050 of *Lecture Notes in Mathematics*. Springer Berlin Heidelberg, 1984.

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

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

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

[25] Lou van den Dries. *Tame Topology and O-minimal Structures*, volume 248 of *London Mathematical Society Lecture Note Series*. Cambridge University Press, 1998.

[26] Lou van den Dries and Ayhan Günaydin. The fields of real and complex numbers with a small multiplicative group. *Proceedings of the London Mathematical Society*, 93(1):43–81, 2006.